kaspersky

Космические системы как цель и средство кибератак

Семен Корт, Александр Николаев, Екатерина Рудина

16.07.2026 Версия 1.0

Оглавление

Вступление

В ноябре 2019 года в Брюсселе лидеры стран – членов НАТО официально признали космос «новой оперативной средой» (наряду с сушей, морем, воздухом и киберпространством).

В статье рассматриваются вопросы информационной безопасности и атак в космическом пространстве. При этом в фокусе – не только целенаправленные атаки на цифровые инфраструктуры космических систем, но и более широкий спектр инцидентов, включая программные сбои, отказы и непреднамеренные человеческие ошибки. Ретроспективный анализ этих происшествий дает важную информацию для выявления скрытых уязвимостей и повышения устойчивости космической инфраструктуры. Без учета ошибок и сбоев невозможно построить эффективную стратегию кибербезопасности в космосе – именно это утверждение лежит в основе представленного исследования.

Космическая система – это предельно удаленная и сложно контролируемая автоматизированная система. Для описания различных атак на космические системы представим схему, включающую основные подсистемы и каналы коммуникаций.

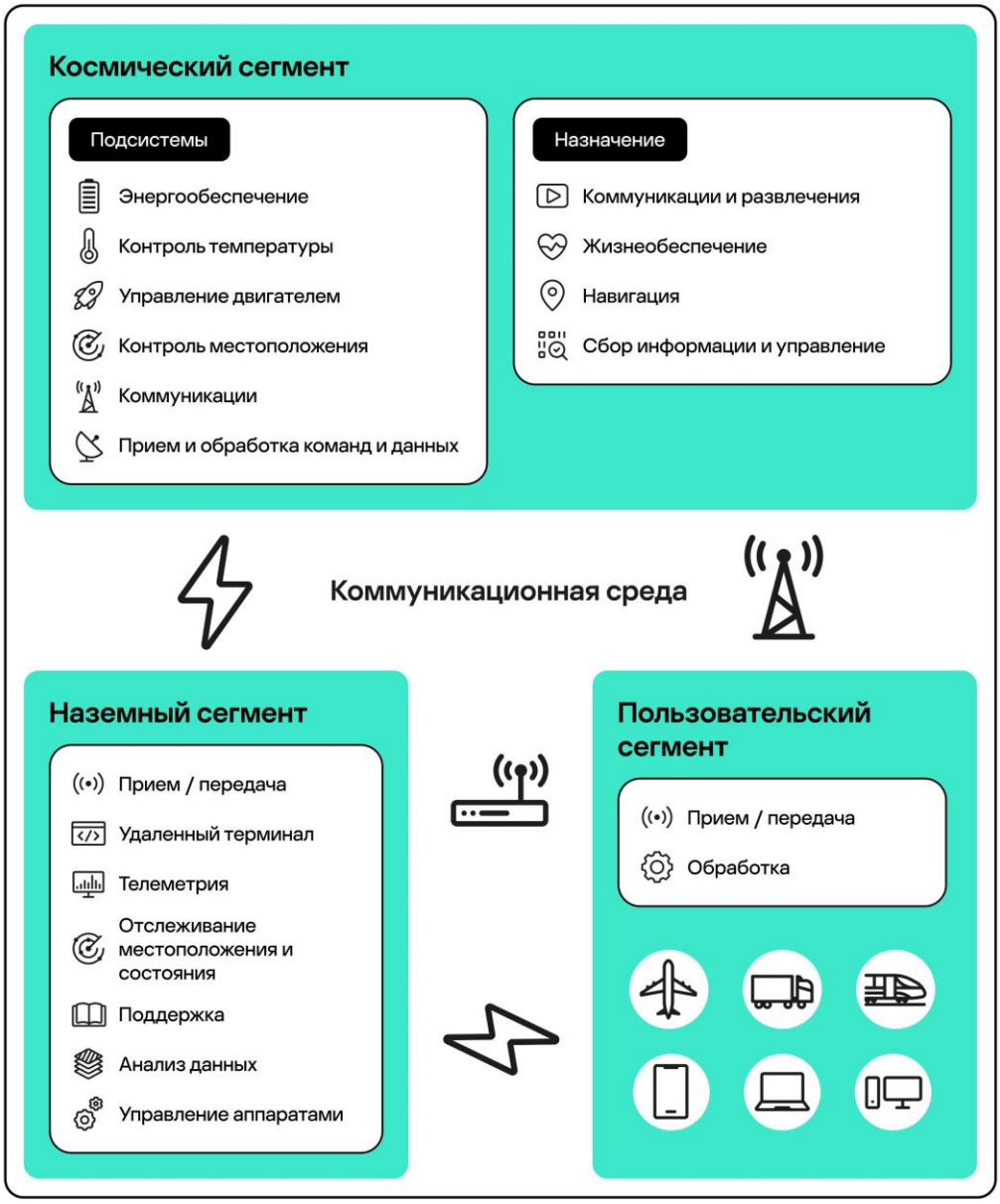

Рисунок 1. Космическая система

Космический сегмент состоит из выведенных на орбиту аппаратов, от взаимного расположения которых и параметров передаваемых сигналов зависят точность позиционирования и стабильность функционирования системы. Наземный сегмент (сегмент управления) включает в себя сеть наземных станций для управления космическими аппаратами и обновления информации. Пользовательский (абонентский) сегмент состоит из приемного оборудования всех пользователей системы – военных служб, коммерческих организаций или частных лиц. В некоторых случаях

(например, непосредственное спутниковое вещание) наземный сегмент отсутствует – сигнал идет сразу в пользовательский сегмент.

Представим последствия, которые влечет за собой нарушение безопасности космической системы.

- Получение злоумышленником управления космическим аппаратом, наземным сегментом, пользовательским устройством.
- Отказ в обслуживании устройств.
- Кража технологий.
- Перехват и внедрение информации, в том числе распространение сообщений в широком публичном поле.
- Репутационный ущерб для производителя атакованной системы, компрометация в публичном поле организаций, которые эту систему используют.

Современные космические системы, в основном спутниковые, являются частью критической инфраструктуры: от их функционирования зависят многие процессы, непосредственно влияющие на повседневную жизнь. Перечислим возможные последствия полного отключения спутниковых систем.

- Сбои в работе связи. Спутники являются ключевым компонентом глобальных систем связи. Вывод из строя компонентов спутниковой системы влечет серьезные нарушения в работе всех видов коммуникаций, включая телефонную связь, интернет и телевизионные сети. Деградация связи приводит к массовым сбоям в работе предприятий, отключениям электроэнергии, невозможности работы служб экстренной помощи и в конечном счете – к негативному влиянию на общественную безопасность и благополучие населения.
- Проблемы навигации. Приемники глобальной навигационной спутниковой системы (ГНСС) обеспечивают предоставление точной информации о местоположении. Безусловно, самолеты летали и пароходы ходили задолго до появления спутниковой навигации. Морские суда по-прежнему оснащены картами и навигационными приборами, а самолеты способны достигать пункта назначения под руководством авиадиспетчеров. Однако экипажи привыкли к современным средствам навигации – работать без ГНСС существенно сложнее, безопасность при этом страдает. Возникают проблемы и у дорожного транспорта – сегодня сложно представить поездку без навигатора. Помимо этого, оказывается затруднено отслеживание и перемещение грузов, поскольку логистические компании и таможенные службы используют навигационные маячки.

- Сложности с прогнозированием погоды. Спутники играют важнейшую роль в мониторинге погодных условий и сборе данных, которые используются для метеорологических прогнозов. Без спутников возможность прогнозировать и своевременно готовиться к таким суровым погодным явлениям, как ураганы, торнадо и тайфуны, значительно снизится.
- Ограничение возможностей для научных изысканий. Спутники широко применяются в исследовательских проектах для мониторинга окружающей среды, изучения изменения климата, отслеживания океанских течений. Без этого ученые были бы ограничены в своих возможностях получать данные и расширять научные знания.
- Угроза национальной безопасности. Многие страны используют спутники в военных целях, в частности для наблюдения и рекогносцировки. Потеря спутников может иметь серьезные последствия для национальной и общемировой безопасности: негативно повлиять на сбор разведывательной информации, разрушить стратегический баланс сил, привести к военным столкновениям или усугубить их.

Все это объясняет, почему космические и, в частности, спутниковые системы являются значимым объектом для атак и привлекают внимание злоумышленников.

Атаки на космические системы

По информации из открытых источников, с 1957 года до начала 2020-х годов было зафиксировано немногим более сотни атак на космические системы. Исследователи расходятся во мнениях относительно того, что именно следует считать кибератакой на космическую систему – относить ли к таковой глушение или подмену сигнала от наземной станции, прослушивание трафика, использование злоумышленниками инфраструктуры пользовательского сегмента с целью сокрытия вредоносной деятельности. Согласно различным источникам, количество инцидентов в новейшее время составляет тысячи и десятки тысяч атак в год, однако эта цифра напрямую зависит от интерпретации понятий «космическая система» и «кибератака».

Открытость информации о космических инцидентах (тех, которые удалось обнаружить) повышалась со временем – от слухов об атаках в начале использования космических технологий до подробного описания некоторых инцидентов в наше время.

Учитывая это, рассмотрим примеры инцидентов и проследим эволюцию атак на космические системы. Даты в хронологии приблизительные: они соответствуют этапу развития систем, на каждом этапе различаются причины инцидентов, их последствия, мотивация действующих лиц. С течением времени эти факторы менялись, именно эти изменения являются предметом нашего исследования.

1957–1979. Начало автоматизации космических систем

Когда в 1957 году СССР запустил первый в мире искусственный спутник Земли – «Спутник-1», никто не знал и даже не задумывался о таком понятии как кибербезопасность. Системы были аналоговые. Максимум, что можно было сделать с точки зрения обеспечения защиты данных, – физическая защита. Использовались закрытые «военные» частоты, шифрование, ограничение доступа персонала к данным проектов. «Модель угроз» включала разведку, наблюдение или попытки воздействия на радиоволновые коммуникации, однако ни одно подозрение в воздействии такого рода не получило подтверждения. Зато в раскрытых документах ЦРУ упоминаются, например, мониторинг со стороны США первой автоматической стыковки беспилотных кораблей «Космос-186» и «Космос-188» в 1967 году, а также активность радиоразведывательных станций НАТО в Норвегии.

До середины 1970-х годов все космические аппараты были полностью аналоговыми, но ошибки при компьютеризированных расчетах иногда приводили к проблемам. В 1965 году в ходе миссий «Джемини-3» и «Джемини-5» были допущены ошибочные расчеты точки приземления. В обоих случаях отклонение составило около сотни километров: в первом – из-за ошибки в расчетах аэродинамических характеристик капсулы, а во втором – из-за того, что программист указал суточное вращение Земли равным 360°, тогда как на самом деле оно составляет 360,98°. И в том и в другом случае экипаж скорректировал курс, насколько это было возможно, а вот для беспилотных аппаратов исправление подобных ошибок требует удаленного управления (да и пилотируемым оно пригодится).

Во второй половине 1970-х цифровые системы начали постепенно внедряться в космические аппараты. И хотя до намеренных атак на эти системы было еще далеко, о возможных проблемах можно судить по инцидентам, связанным со сбоями в их работе. Проблемы программного обеспечения и систем управления, ошибки при обновлении ПО и недостаточная компетентность персонала сопровождали как миссии NASA, так и советскую космическую программу. Особенно примечательна

роль человеческого фактора. Во время миссии «Аполлон-8» непреднамеренно введенная космонавтом команда привела к удалению содержимого памяти компьютера, в результате чего компьютер посчитал, что инерциальный блок указывает на неправильную ориентацию аппарата. Ситуацию исправили вручную. В ходе миссии «Аполлон-10» (считающейся «репетицией» перед высадкой на Луне) система аварийного наведения лунного модуля была по ошибке переключена из режима удержания положения в режим автоматического управления, что спровоцировало неожиданное вращение модуля и тоже потребовало вмешательства для стабилизации.

Были и необратимые ошибки, особенно в более поздние годы, когда цели космических исследований стали более удаленными и разнообразными, а механизмы защиты от сбоя все еще не были безупречными. Поэтому мы приведем следующие примеры именно в этой главе. В 1982 году при обновлении программного обеспечения спускаемой на поверхность Марса части американского аппарата «Викинг-1» оператор ошибся в последовательности команд, что привело к опусканию антенны на аппарате и потере связи с ним навсегда.

Советская автоматическая межпланетная станция «Фобос-1» 1 сентября 1988 года не ответила при запросе запланированного сеанса связи. Позднее выяснилось, что тремя днями ранее оператор в Центре управления полетами в Евпатории непреднамеренно пропустил один дефис в одной из команд. Все команды перед передачей должны были проходить проверку на компьютере, но в тот день он оказался неисправен. Оператор нарушил процедуру и отправил команду, не дожидаясь устранения неисправности. Это незначительное изменение в коде команды активировало неиспользуемый тестовый код и отключило двигатели ориентации, что привело к потере слежения за Солнцем и, следовательно, к разрядке батарей. Аппарат был потерян.

Буквально на следующей неделе, 5 сентября 1988 года, пилотируемый корабль «Союз ТМ-5» едва не потерпел катастрофу. Причиной стала устаревшая версия программы стыковки со станцией «Мир», загруженная в бортовой компьютер: она предназначалась для предыдущей миссии. После отстыковки от станции тормозные двигатели включились на семь минут позже запланированного из-за неправильной работы программного обеспечения с инфракрасным датчиком горизонта, – и космонавты были вынуждены их отключить. Повторное включение, предпринятое через три часа, продолжалось только шесть секунд. Компьютерное управление не позволяло вручную свести корабль с орбиты из-за первого отключения двигателя. Двигатели удалось запустить только после того, как командир

корабля прямо в полете перепрограммировал модуль управления для игнорирования первого неуспешного тормозного импульса. Затем выполнение программы было вручную прервано во избежание сброса приборно-агрегатного отсека: без него космонавты не смогли бы выжить – спуск затянулся бы, и им не хватило бы воздуха и электричества. Пристыковаться обратно к станции тоже было нельзя, так как стыковочная система была уже сброшена. Фактически взламывая компьютерную систему корабля и заставляя его подчиняться ручному управлению, космонавты провели на орбите еще одни сутки и 7 сентября, с третьей попытки, сошли с орбиты и приземлились.

Таким образом, причиной большинства известных инцидентов являлся человеческий фактор: отсутствие проверок, резервирования или игнорирование процедур. Но были и чисто компьютерные баги. В 1981 году первый испытательный полет многоразового транспортного космического корабля – шаттла STS-1 – был отменен за несколько минут до старта. В присутствии президента США Рональда Рейгана и в прямом телевизионном эфире. Причиной стала рассинхронизация при обмене данными между основным и резервным компьютерами. Дело было в трудноуловимой на поздних этапах ошибке. Программы были написаны и отлажены, однако в процессе разработки сложного ПО управления шаттлом, включавшего резервирование и восстановление, в стандартную платформу бортового компьютера были внесены изменения, связанные с использованием таймера очереди операционной системы основного компьютера. Из-за этих изменений – в частности, из-за запуска некоторых подпрограмм до первого процесса основного компьютера – планируемый запуск первого процесса иногда оказывался в прошлом и переносился операционной системой на цикл в соответствии с алгоритмом планировщика. С вероятностью 1/67 это приводило к рассинхронизации основного и резервного компьютеров: таймер очереди основного использовался всеми процессами всех компьютеров как часы, тогда как процессы на разных компьютерах выполнялись в разное время относительно этого таймера. При интеграционном тестировании проблему не выявили, и она дала о себе знать в день старта шаттла.

Таким образом, ранний этап автоматизации космических систем характеризуется следующими положениями:

- даже небольшая ошибка в системе цифрового управления способна повлечь катастрофические последствия;
- инциденты чаще связаны не с ошибками в коде, а с человеческим фактором (отсутствие или возможность обхода или игнорирование процедур проверки) – и последствия таких инцидентов тяжелее;

- инциденты показали, что резервирование и возможность автоматического восстановления существенны для автономных систем;
- возможность гибкой настройки, экстренного и надежного обновления как пилотируемых, так и беспилотных объектов важна, когда речь идет о действиях в непредвиденных обстоятельствах.

1980–1989. Коммерциализация космических технологий

В 1980-е годы в повседневную жизнь пришли персональные компьютеры и спутниковое телевидение, спутники стали использовать в интересах гражданского сектора. Круг потребителей космических технологий расширился. Космические системы к тому времени стали преимущественно автоматизированными и компьютеризированными, что сделало их доступным объектом для угроз информационной безопасности, а неизбежная коммерциализация технологий создала повод к атакам.

В этом разделе рассмотрим атаки на наземный и пользовательский сегменты космических систем США. Эти атаки обусловлены в том числе конфликтом интересов коммерческих компаний и пользователей технологий. Основная цель этих атак – огласка самого факта взлома, публичная передача сообщения. Они схожи, например, с появившимися позднее атаками типа дефейс веб-сайтов в интернете и были спровоцированы тем, что законодательство США менялось вслед за развитием технологий, обеспечивая интересы коммерческих компаний, что, с точки зрения потребителей, было несправедливо.

Вместе с тем описанные атаки – не единственный вид инцидентов в 1980-е годы. Атаки, направленные на перехват, подавление и подделку информации появились одновременно со спутниковой передачей информации. По данным из открытых источников, в 1986 году Индонезия стала первым государством, обвиненным в нарушении правил спутникового прослушивания, а в 1996 года она же первой намеренно использовала спутник для подавления сигнала другого спутника. Впрочем, инциденты, относящиеся к сфере государственной радиоэлектронной разведки, радиоэлектронной борьбы и космической гонке государств, выходят за рамки этой статьи, поскольку в публичных материалах на эту тему зачастую невозможно отделить достоверные факты от предположений и спекуляций. Поэтому мы ограничимся рассказом исключительно об атаках на коммерческие системы гражданского применения.

Атака Капитана Полночь на спутниковую трансляцию компании Home Box Office (HBO), вероятно, является одним из первых актов хактивизма, получивших широкую известность. Чтобы понять цель этой атаки, нужно обратиться к истории развития технологий спутникового телевидения в 1970-1980-е годы. Системы спутникового телевещания с конца 1960-х – начала 1970-х годов были рассчитаны на прием спутникового сигнала исключительно с помощью приемных станций кабельных операторов, которые, в свою очередь, продавали подписку на каналы своим абонентам. Однако в 1976 году бывший сотрудник NASA Генри Тейлор Говард из интереса собрал в своем гараже комплект оборудования, позволивший напрямую принимать со спутника сигнал, предназначенный для приемных станций операторов телевидения (позднее эта технология получила название Direct-to-Home, DTH). Он опробовал новый способ и даже отправил компании HBO чек за полученный контент, однако ни чек, ни само изобретение компанию не заинтересовали. Тогда Генри Тейлор Говард вместе с Робертом Таггартом в 1980 году основал компанию Chapparal Communication по производству и продаже оборудования для просмотра спутникового телевидения. Это оборудование позволяло смотреть множество каналов сразу нескольких поставщиков без абонентской платы, а качество изображения было выше, чем при передаче по кабельным сетям. Более того, его можно было использовать в отдаленных районах, где кабельные операторы не работали. Поэтому, несмотря на высокую стоимость оборудования, дела компании быстро пошли на лад. В начале 1980-х годов большинство зрителей смотрели спутниковые телеканалы, не оплачивая услуги поставщика. Дилеры по продаже антенн-приемников спутникового ТВ появились по всей стране – это был весьма прибыльный бизнес. Одним их таких дилеров и был Джон Макдугалл, позднее прославившийся как Капитан Полночь.

Основанная в 1972 году и являвшаяся пионером в области спутникового формата телевещания компания HBO упустила технологию DTH из виду, однако не намеревалась мириться с потерей той части абонентов, которые перестали платить за просмотр. Вместе с другими компаниями HBO добилась принятия в 1984 году «Акта о политике в сфере кабельных коммуникаций» (Cable Communications Policy Act of 1984), закрепившего за кабельными операторами право на кодирование передаваемого сигнала. Уже через два года HBO реализовала кодирование сигнала, после чего продажи оборудования для нелегального просмотра платных спутниковых каналов резко упали, а Джон Макдугалл, как и многие другие дилеры, лишился дохода. Параллельно он устроился работать инженером по эксплуатации в компанию Central Florida Teleport, занимавшуюся передачей данных на спутники. Около полуночи 27 апреля 1986 года, после

окончания своей смены, в течение которой Джон Макдугалл поддерживал трансляцию фильма для компании People's Choice, он, следуя инструкции, развернул антенну. И она якобы по случайности оказалась направлена на спутник, один из транспондеров которого осуществлял трансляцию для HBO. Координаты спутника и частоты для передачи были известны Джону из общедоступных руководств и журналов для энтузиастов. Действуя, по его словам, импульсивно, он настроил телевизионную картинку – сообщение для HBO, придумал себе псевдоним Капитан Полночь (Captain Midnight) и включил передачу на высокой мощности. Джон перебил трансляцию фильма сообщением: «Добрый вечер, HBO, от Капитана Полночь! 12,95 долларов в месяц? Ни за что! (Showtime/киноканалы, берегитесь!)». Аудитория HBO в районе прерванной трансляции составляла около 14,6 миллионов человек.

Рисунок 2. Сообщение, которое зрители канала HBO увидели во время просмотра триллера «Агенты Сокол и Снеговик» поздно вечером 27 апреля 1986 года

На протяжении одной-двух минут Джон Макдугалл и инженер HBO соревновались в наращивании мощности сигнала, однако инженер сдался, испугавшись повредить спутник, после чего Джон прекратил трансляцию.

Версию о спонтанности этого акта опровергает тот факт, что неделей ранее Джон Макдугалл уже вмешивался в трансляцию HBO – правда, без

какого-либо сообщения, просто передав настроечную таблицу. 22 июля 1986 года он предстал перед федеральным судом, который назначил ему год условно и оштрафовал на 5000 долларов.

В глазах многих продавцов спутниковых антенн и спутникового телевидения Джон Макдугалл стал героем. В его поддержку была создана «Народная коалиция имени Капитана Полночь», представитель которой Дональд Кохран заявил: «Есть те, кто считает Капитана Полночь преступником за его несанкционированные трансляции, но существует и другая группа – владельцы домашних спутниковых антенн, представители малого бизнеса и бунтари, которые поддерживают его действия как ненасильственный и неразрушительный протест в лучших американских традициях».

Джона Макдугалла осудили по статье 47 U.S.C. §301 «Лицензия на радиовещание и передачу энергии» (License for radio communication or transmission of energy), хотя применение этой статьи в данном случае выглядело юридически сомнительным. Представители спутниковой индустрии, обеспокоенные возможностью усиления помех и риском повреждения спутников из-за перегрузок на входе, призвали Конгресс принять новый уголовный закон, который стал статьей 18 U.S.C. §1367 «Вмешательство в работу спутника» (Interference with the operation of a satellite). По этой статье год спустя осудили и приговорили к условному сроку Томаса Хейни – техника станции спутниковой связи Христианской вещательной сети (CBN) в Вирджиния-Бич. В сентябре 1987 года он перебил трансляцию телеканалов American Exxxtasy Channel и Playboy TV текстовыми сообщениями, призывавшими зрителей покаяться и обратиться к Иисусу. Хактивисты не особенно скрывались: максимальная огласка только помогала им добиваться большего эффекта.

Наряду с идейно мотивированными акциями случались и откровенно хулиганские акты. К их числу относится инцидент Макса Хэдрума – перехват сигнала телевидения в Чикаго 22 ноября 1987 года. В отличие от предшественников, хакер транслировал не текстовые сообщения, а видеозапись, на которой он появился в маске Макса Хэдрума – персонажа одноименного фильма 1985 года. Инцидент включал два эпизода. Первый произошел на канале WGN-TV в 21:14 – во время трансляции спортивного блока новостей сигнал внезапно пропал, а спустя девять секунд на экране появился человек в маске Макса Хэдрума и черных очках, дергавшийся в разные стороны. Второй эпизод случился в тот же вечер на телеканале WTTW, в 23:15, во время показа сериала «Доктор Кто». Злоумышленник в течение полутора минут транслировал эпатажное видео, вызвавшее у зрителей смешанную реакцию: одних оно расстроило и даже напугало,

других – рассмешило. Установить, кто стоял за атакой, правоохранительным органам так и не удалось. Вскоре после этого инцидента чикагский канал WMAQ-TV специально включил скандальную видеозапись во время трансляции спортивных новостей и получил шквал сообщений с вопросами о взломе. Это обеспечило каналу то, что сегодня назвали бы вирусной рекламой.

В череду описанных инцидентов органично вписывается происшествие, о котором стало известно из публикации в New York Times от 16 сентября 1987 года. В заметке сообщалось, что группа западногерманских компьютерных энтузиастов взломала международную компьютерную сеть NASA и, прежде чем их обнаружили, беспрепятственно копалась в данных как минимум три месяца. Организация из Гамбурга Chaos Computer Club, утверждавшая, что выступает от имени анонимной группы, взломавшей сеть, заявила: злоумышленники установили троянскую программу, которая позволила им обойти процедуры безопасности и получить доступ к 135 компьютерам сети. Речь шла о сети Space Physics Analysis Network, предназначенной главным образом для предоставления авторизованным ученым и организациям доступа к данным NASA. Систему безопасности сети обеспечивала американская компания Digital Equipment Corp. И пользователи, и официальные представители NASA заявили, что сеть широко использовалась учеными в США, Великобритании, Западной Германии, Японии и других странах и не передавала секретную информацию. В NASA пояснили, что цель сети – обеспечить легкий доступ к несекретным данным, и любое физическое или юридическое лицо, занимающееся исследованиями, связанными с NASA, может подать заявку на доступ. Потенциальный ущерб от действий злоумышленников мог быть связан с модификацией или уничтожением информации, однако представитель Chaos Computer Club Бау Холланд опроверг информацию о какой-либо модификации данных, назвав подобные действия противоречащими хакерской этике. Следует оговориться, что в те времена слово «хакер» обозначало компьютерного энтузиаста-любителя, а не злоумышленника, причиняющего ущерб.

Таким образом, в 1980-х годах атаковать космические системы начали обычные злоумышленники. Мотивами в тот период служили самоутверждение, пропаганда, пиратство в относительно благородном понимании этого слова. Впрочем, извлечение выгоды из намеренного причинения ущерба было лишь вопросом времени.

1990–1999. Компьютеризация космических систем

В 1990-е годы злоумышленники, стремившиеся получить доступ к телевизионным трансляциям, окончательно сфокусировались на декодировании сигнала спутниковых каналов телевидения. Хотя подобные атаки можно отнести к атакам на пользовательский сегмент космических систем, выраженной «космической» специфики они не имели. Основной вектор атаки заключался в установке на приемнике телесигнала декодера, который, к примеру, мог подменять официальную смарт-карту поставщика с актуальными ключами для просмотра телеканалов или подключаться к компьютеру для динамической расшифровки сигнала записанной телетрансляции. Один из пионеров взлома – Маркус Гюнтер Кун, известный как изобретатель декодирующего устройства Season7, получившего широкое распространение в начале 1990-х годов. В открытом письме от 23 мая 1996 года, адресованном комиссии Европейского Союза, где 6 марта того же года прошли слушания на тему «Правовая защита зашифрованных сервисов на внутреннем рынке. Консультации о необходимости действий сообщества» (Legal Protection for Encrypted Services in the Internal Market – Consultation on the Need for Community Action), Маркус Гюнтер Кун утверждал, что использовал свой декодер не в коммерческих целях и не для просмотра платного контента, а исключительно для просмотра телеканалов, которые официальный немецкий поставщик не декодировал: эти каналы не были запрещены, но оставались недоступны для просмотра. Список публикаций Маркуса Гюнтера Куна подтверждает, что он в действительности исследователь и ученый. Разумеется, пираты вовсю использовали как его наработки, так и результаты работ других исследователей для получения собственной коммерческой выгоды.

Атаки на системы наземного сегмента могут иметь и другие задачи: получение несанкционированного доступа к информации, исходному коду и функциям управления с целью вымогательства или даже попытки влияния на космические миссии. Именно это направление интересно широкой публике. Однако далеко не все утверждения о фактах взлома или их последствиях получают однозначное подтверждение.

Спекуляции на тему хакерского взлома системы управления рентгеновской обсерватории ROSAT широко распространились в интернете и до сих пор публикуются как подтвержденные факты. Спутник, запущенный в 1990 году, был оснащен рентгеновским телескопом немецкого производства, американским прибором получения изображений высокого разрешения и английским телескопом для наблюдений в диапазоне экстремального ультрафиолета. Комбинация

такого оборудования давала широкие возможности по наблюдению и изучению всей небесной сферы.

Изначально международная миссия была рассчитана на 18 месяцев, однако активная работа продолжалась более восьми лет, в течение которых система обнаружила свыше 150 000 преимущественно неизвестных источников рентгеновского излучения. Отказ астронавигационного датчика в 1998 году заставил телескоп «смотреть» прямо на Солнце, что привело к серьезным повреждениям (вероятнее всего, к отказу солнечных батарей). Последнее астрономическое наблюдение спутник ROSAT провел 17 декабря 1998 года, 12 февраля 1999 года он был выключен, а 23 октября 2011 года – выведен с орбиты. В 2008 году в новостях и блоге известного специалиста по кибербезопасности Брюса Шнайера появилась версия о том, что упомянутый сбой датчика был вызван кибератакой на Центр космических полетов Годдарда: якобы злоумышленники, получив доступ к коду, сумели перенаправить солнечные панели таким образом, что они вышли из строя. Впоследствии эксперты NASA опровергли эту версию, хотя сам факт неправомерного доступа в сеть Годдарда в 1998 году подтвердили. Приведем цитату: «Компьютеры в этой сети содержали исходный код программного обеспечения для управления полетами нескольких спутников NASA, и нельзя исключать, что кто-то мог использовать знание этого кода для управления спутником с помощью собственной наземной станции или же взломать наземную станцию NASA. Однако с ROSAT этого просто не могло произойти, поскольку в Годдарде были только копии переданных данных, а все манипуляции с обсерваторией проводились из Германии. В 1999 году ROSAT был уже устаревшим спутником, его основная миссия к тому времени уже давно завершилась. Так что его отказ не является неожиданным и вполне поддается объяснению».

При этом остается неясным, имеем ли мы дело со спекуляциями на тему «русских хакеров» (именно их обвиняли в сбое ROSAT) или же с сокрытием последствий атаки на цепочку поставок. Ответ на этот вопрос мы вряд ли узнаем, хотя инцидент до сих пор остается на слуху. Столь же часто фигурирует и инцидент с захватом британского спутника сети Skynet. Она обеспечивает поддержку стратегических и тактических ядерных сил, а также военно-морских, воздушных и сухопутных сил Великобритании. Министерство обороны страны называет эту сеть «необходимой для поддержки всех аспектов современных военных операций». В начале 1999 года британские аэрокосмические власти заметили несоответствие в положении военного спутника связи, одного из четырех аппаратов в семействе Skynet. Вскоре они получили анонимное сообщение с требованием выкупа в обмен на возврат контроля над системами

наведения спутника. Этот случай во многих источниках называют важным ранним примером космического терроризма и взлома спутников.

Министерство обороны Великобритании не признало факт инцидента. Более того, аналитик издательства, специализирующегося на военной тематике, опроверг техническую осуществимость взлома канала управления. Он заявил, что для атаки путем подавления сигнала управления более мощным (jamming-атаки, как в деле Капитана Полночь) злоумышленникам потребовался бы «очень, очень мощный передатчик, и кто-то это наверняка заметил бы». Атака «человек посередине» тоже затруднительна: в отличие от радиоволн, которые распространяются во всех направлениях, используемые микроволны формируют «узкий» луч, распространяющийся всего на три сантиметра на каждые 10 000 км пути. А расположение передающих станций таково, что для перехвата и изменения сигналов потребовалось бы возвести вышку на юго-западе Лондона. Остается теоретическая возможность атаки непосредственно на системы управления, но аналитик утверждал, что «атака невозможна, если не находиться в одном из передающих пунктов Министерства обороны, при этом единственный способ проникнуть внутрь – через американскую систему в военное время, но сейчас не война» и что «британская система намного лучше <американской>, поскольку она полностью автономна». В этих высказываниях очевидно много спекуляции и эмоционально окрашенного отрицания самой возможности атаки. Тем не менее, не следует исключать допустимые варианты атаки инсайдера и неабсолютной изолированности систем управления, которая могла привести к их компрометации. Впрочем, об этом широкой публике вряд ли расскажут.

Выходит, что атаки на космические системы в 1990-е годы не могут быть ни подтверждены, ни опровергнуты на основе имеющейся информации. Вместе с тем определенные вещи можно утверждать наверняка.

Атаки на пользовательский сегмент, особенно в сфере спутникового телевидения, начали приносить злоумышленникам финансовую выгоду. Это дало импульс развитию средств криптографической защиты для коммерческого использования, хотя и весьма умеренному: сдерживающими факторами оставались необходимость обеспечивать обратную совместимость технологий и следовать законодательным, в том числе экспортным ограничениям, а также требования к масштабируемости решений.

Атаки на наземный сегмент проводились и имели успех, однако фактические последствия и ущерб, как и сами инциденты, при

возможности замалчивались. Тем не менее некоторые инциденты впоследствии стали поводом для политических спекуляций.

Угроза кибератак в космической отрасли стала набирать вес, однако обеспечение кибербезопасности в ней все еще не было приоритетной задачей: сама отрасль и состояние космической гонки не всегда оставляли ресурсов и времени для поиска и устранения уязвимостей в системах.

2000–2009. Политизация атак

В нулевые частой целью атак стало распространение политических заявлений, вмешательство в каналы информации и пропаганды. Кроме того, впервые были предприняты попытки вмешательства в работу беспилотных систем и атаки на системы управления космическими объектами, подключенные к интернету.

Как и в 1980-е годы, произошли сразу несколько эпизодов jamming-атак на спутниковое телевидение – тоже хактивистских, но на этот раз с политической мотивацией. В 2002 году политические и религиозные активисты (некоторые связанные с ними организации признаны в РФ нежелательными и экстремистскими) неоднократно перехватывали сигнал спутника SinoSat и прерывали вещание Центрального телевидения Китая и Китайского образовательного телеканала и демонстрировали в эфире оппозиционные видеоролики и сообщения. Китайские власти сообщили, что предполагаемый источник сигнала располагался на территории Тайваня, правительство Тайваня не сразу отреагировало на это обвинение. За инцидентами последовали массовые задержания сторонников активистов. Десятки человек, осужденных за различные эпизоды перехвата телевизионного сигнала с целью показа видеороликов, были приговорены к лишению свободы сроком до 20 лет.

Схожий инцидент произошел в начале 2007 года в Шри-Ланке. Организация «Тигры освобождения Тамил-Илама» (ТОТИ), признанная многими государствами террористической, использовала один из транспондеров спутника крупного оператора связи Intelsat для несанкционированной теле- и радиотрансляции в США и Европе. Урегулирование инцидента потребовало межгосударственного взаимодействия: посол Шри-Ланки был вынужден обратиться к официальным лицам США. К концу апреля 2007 года компания Intelsat подтвердила, что ей удалось успешно лишить «Тамильских тигров» возможности использовать свои объекты, и тем самым сорвала пропагандистскую деятельность группировки. Эта акция была частью более масштабной кампании по борьбе с логистикой ТОТИ на

заключительном этапе гражданской войны в Шри-Ланке, часто называемой «Четвертой Иламской войной».

Вмешательство в вещание (jamming-атаки) практиковали не только повстанцы, но и официальные власти. В 2009 году во время выборов в Иране правительство страны не только запретило деятельность телерадиослужбы BBC на персидском языке, но и приняло активные технические меры, в частности мощное подавление спутникового сигнала BBC Persian и BBC World News, а также блокировку сайта bbcpersian.com.

Подобные атаки не отличаются технической сложностью – для их проведения достаточно иметь доступ к оборудованию. Вообще в нулевые годы проблема устойчивости и информационной безопасности не относилась к числу приоритетных, если только речь не шла о прямой коммерческой выгоде от вещания. Наглядным свидетельством тому служит следующий пример.

В 2009 году в Ираке повстанцы использовали программное обеспечение для перехвата в реальном времени видеопотоков, передаваемых со спутников на американские беспилотники Predator (и, по некоторым сведениям, Reaper). Это давало им возможность получать информацию, необходимую для уклонения от военных ударов США или для наблюдения. Условно-бесплатное ПО SkyGrabber, цена лицензии на которое составляла 26 долларов США, широко использовалось в конце нулевых для перехвата в пассивном режиме данных со спутников, включая фильмы, музыку, изображения и прочего контента, загружаемого другими пользователями. По своей сути это был анализатор и сборщик сетевых пакетов: программа получала доступ к незашифрованному каналу передачи данных между спутником и наземной станцией, так что такой перехват даже взломом назвать сложно.

Факт перехвата обнаружили военнослужащие США в Ираке, когда задержали шиитского боевика, на ноутбуке которого оказались файлы видеопотоков с беспилотников. Несколько месяцев спустя аналогичные файлы были найдены на ноутбуках других повстанцев, что позволило сделать вывод о систематическом характере перехвата данных боевыми группировками. Отсутствие шифрования при передаче данных с военных беспилотников впоследствии объясняли ограниченным временем введения дронов в эксплуатацию, а также тем, что производитель запатентовал некоторые коммуникационные технологии, поэтому распространенные системы шифрования оказались несовместимы с ними. По словам некоторых официальных лиц, правительство США было в курсе этой уязвимости еще со времен американской кампании в Боснии в 1990-х годах, но Пентагон предполагал, что противники не сумеют ее

эксплуатировать. Тем не менее, проблему признали уязвимостью и впоследствии устранили.

При этом нельзя сказать, что проблема безопасности космических систем игнорировалась. В публикации от 28 октября 2011 года агентство Bloomberg News, ссылаясь на проект доклада Комиссии по контролю американо-китайских отношений в области экономики и безопасности, сообщает, что в 2007–2008 годах наземная станция NASA в Норвегии несколько раз фиксировала продолжительные помехи в работе спутников дистанционного зондирования Земли Landsat-7 и Terra AM-1. «В октябре 2007 года и июле 2008 года система спутников дистанционного зондирования Земли Landsat-7 подвергалась помехам в течение 12 и более минут. Хакеры дважды создавали помехи спутнику дистанционного зондирования Земли Terra AM-1: в течение двух минут в июне и девяти минут в октябре 2008 года», – говорится в проекте документа со ссылкой на закрытый брифинг ВВС США. В итоговом докладе конкретные инциденты уже не упоминаются, но сообщается, что «Китай расширил свои возможности для ведения кибервойны и уничтожения спутников наблюдения в рамках тактического арсенала асимметричной войны. Из-за высокой зависимости от систем командования, управления, связи, компьютеров, разведки, наблюдения и рекогносцировки (C4ISR) американские вооруженные силы в значительной мере уязвимы для подобных атак». Китайские официальные лица опровергли эти сведения, заявив, что «данное сообщение не соответствует действительности и преследует скрытые мотивы».

Вместе с тем далеко не все инциденты имели политическую подоплеку или являлись результатом целевых атак. Активное распространение вредоносных программ в нулевые затронуло и случайные системы, которые затем оказались в космосе. Например, ноутбуки, доставленные на Международную космическую станцию (МКС) в июле 2008 года, оказались заражены компьютерным червем W32.Gammima.AG. Космонавты использовали эти ноутбуки для электронной переписки, и какие-либо защитные средства на них отсутствовали. Вредонос, скорее всего, занесенный с зараженного носителя, был предназначен для кражи паролей от онлайн-игр и не наносил ущерба системам МКС. Согласно заявлению NASA, вредоносные программы «отправлялись» в космос и прежде, хоть такое и происходило нечасто.

2010–2019. Дальнейший рост и усложнение атак

В 2010-е годы атаки на беспилотники с использованием вектора атаки на спутниковый канал связи получили дальнейшее развитие. В 2011 году

американский беспилотник RQ-170 Sentinel был посажен в Иране, а не на американской базе в Афганистане. Иранский инженер, занимавшийся обратным проектированием взломанного беспилотника, заявил, что иранской стороне удалось использовать известную GPS-уязвимость для изменения точки приземления: Sentinel принял место в Иране за свою базу в Афганистане.

Примечательно, что только в апреле 2011 года Научно-консультативный совет ВВС США опубликовал «Отчет об эксплуатации беспилотных летательных аппаратов нового поколения для ведения нерегулярных боевых действий», содержавший оценку надежности канала связи между дроном и наземной станцией управления. Согласно документу, американские беспилотники подвергаются следующим угрозам (выдержка).

- Глушение каналов коммерческой спутниковой связи (SATCOM). Это широко распространенная технология, которая может служить эффективным инструментом противодействия каналам передачи данных или средством блокирования управления и контроля.
- Оперативная необходимость может потребовать использовать незашифрованные каналы передачи данных для обеспечения информирования наземных войск, не имеющих допуска к секретным данным. Перехват таких каналов – известная уязвимость, доступная противникам за крайне низкую цену.
- Подмена или перехват ссылок, которые могут привести к ущербу миссии или даже к потере платформы.

В документе, посвященном противодействию угрозам для позиционирования, навигации и управления, подчеркивается: «Существует широкий спектр методов, которые целеустремленный противник может использовать для атаки на системы наведения и навигации беспилотных летательных аппаратов.

- Небольшие и простые устройства подавления GPS шумом могут быть легко сконструированы и использованы даже неискушенным противником; при этом они будут эффективны в ограниченной зоне действия беспилотных летательных аппаратов.
- Также существуют GPS-ретрансляторы, специально разработанные для нарушения навигации беспилотных летательных аппаратов.
- Киберугрозы представляют собой серьезную проблему для будущих операций с беспилотными летательными аппаратами. Кибератаки могут затрагивать как бортовые, так и наземные системы, а используемые методы могут варьироваться от асимметричных атак на центральные военно-морские силы до

высокотехнологичных атак на электронные системы и программное обеспечение».

Кибербезопасности спутниковых систем стали уделять гораздо больше внимания. Так, в 2013 году в США был инициирован внутренний аудит ИТ-безопасности Национального управления океанических и атмосферных исследований, в ведении которого находится Объединенная полярная спутниковая система (JPSS). В меморандуме от 2014 года сообщается о многочисленных уязвимостях системы безопасности, классифицированных как «высокорисковые», в наземной системе JPSS. Более 9100 уязвимостей были связаны с устаревшим или настроенным не должным образом ПО. Было выявлено более 3600 несоответствий политике безопасности, включая проблемы с паролями. Отдельно было отмечено, что три уязвимости, выявленные еще в ходе тестирования на проникновение в 2012 году, к 2014 году по-прежнему оставались не устранены. Впрочем, в ответном письме ведомство сообщило о принятых мерах и подтвердило, что была устранена даже уязвимость Heartbleed, о которой стало известно только в апреле 2014 года.

Атаки на операторов спутниковой связи реализовались в рамках многих кампаний по кибершпионажу. В качестве примера можно привести Icefog, запущенную как минимум в 2011 году, жертвами которой стали правительственные организации, военные ведомства, предприятия оборонно-промышленного комплекса, судостроительные фирмы, операторы телефонной и спутниковой связи, промышленные и высокотехнологичные компании, а также средства массовой информации преимущественно в Южной Корее и Японии.

Количественный рост и качественное усложнение атак в 2010-е годы закономерно затронули и сферу спутниковых технологий, которые все активнее стали использоваться в интересах киберпреступников.

Так, некоторые продвинутые APT-группы решили проблему, связанную с отключением и изъятием доменов и командных серверов вредоносного ПО, перейдя на спутниковые интернет-каналы для маскировки своих кампаний. На IP-адресах спутникового интернета были замечены командные серверы APT-групп HackingTeam, Xumuxu, Rocket Kitten. Но самой интересной и необычной из них была группа Turla. Она взломала нескольких провайдеров спутникового интернета стандарта DVB-S, которые в большинстве своем предоставляли нисходящие интернет-каналы для Ближнего Востока и Африки. Для реализации подобных атак требуется относительно доступное оборудование: спутниковая тарелка, размер которой зависит от географического положения и конкретного спутника, спутниковый конвертер (LNB), специальный спутниковый DVB-S

тюнер (плата PCIe) и компьютер под управлением ОС Linux. В отличие от дуплексного спутникового интернета, нисходящие интернет-каналы используют для ускорения скачивания: они отличаются дешевизной и простотой установки, не предусматривают шифрования. Это создает возможности для их злонамеренного использования.

Злоумышленники прослушивали передаваемый в открытом виде трафик через нисходящий спутниковый канал, чтобы определить активно используемые IP-адреса. Эти IP-адреса указывались в конфигурации вредоносного ПО, поэтому после успешного заражения все данные жертвы направлялись на них. При обнаружении в трафике вызова от вредоносного ПО C2-сервер отправлял по обычным (дешевым наземным) коммуникациям ответ с поддельным IP-адресом. Фактически это была атака «человек посередине», причем во многих случаях подавлять ответ действительного обладателя IP-адреса не требовалось, поскольку пакет, пришедший на закрытый порт, вероятнее всего, был бы отброшен межсетевым экраном (такова рекомендация для медленных каналов).

Исследователи отмечали, что описанный метод отличается простотой реализации и обеспечивает более высокий уровень анонимности по сравнению с обычными способами, такими как аренда виртуального выделенного сервера или взлом легального сервера. Единственное ограничение – необходимость располагаться в зоне покрытия провайдера спутникового интернета. Исследователи опасались, что метод могут взять на вооружение финансово мотивированные киберпреступники, но, видимо, это ограничение оказалось существенным сдерживающим фактором (либо такие случаи остались необнаруженными).

В 2017 году была описана деятельность другой APT-группы, получившей название Whitebear и имевшей отношение к группе Turla. Как и в случае с Turla, для построения инфраструктуры использовались скомпрометированные веб-сайты и перехваченные спутниковые соединения.

В 2018 году аналитики Symantec сообщили об обнаружении кибершпионской атаки группы Thrip на спутниковые, телекоммуникационные и оборонные организации. В блоге компании отмечалось, что «группа злоумышленников проявляла особый интерес к деятельности оператора спутниковой связи, выискивая и заражая компьютеры, на которых работало программное обеспечение для мониторинга и управления спутниками». Это навело исследователей на мысль, что мотивы атакующих выходили за рамки шпионажа и могли включать в себя намеренное нарушение работоспособности систем. Еще одной мишенью Thrip стала организация, занимающаяся

геопространственной обработкой изображений и картографированием. Атаке подверглись компьютеры под управлением программного обеспечения MapXtreme Geographic Information System, предназначенного для разработки пользовательских геопространственных приложений и интеграции данных о местоположении в другие приложения. Также целью были компьютеры под управлением Google Earth Server и программного обеспечения для обработки изображений Garmin. Технические подробности атаки, немедленно подхваченные информационными агентствами, позволили исследователям сделать вывод, что за ней стояли злоумышленники из Китая.

В исследовании, датированном 2019 годом, аналитики Symantec сообщили о продолжающихся атаках этой предположительно китайской группировки на операторов спутниковой связи в Юго-Восточной Азии.

В целом, 2010-е годы характеризовались ростом количества атак, в том числе на космические системы. Усилилась тенденция к поддержанию ИТ-инфраструктуры в безопасном состоянии, особенно в государственном секторе. Тем не менее, квалифицированные злоумышленники продолжали находить и вектора атак на системы, и способы эксплуатации технологий для своей выгоды.

2020–2024. Современные атаки

В начале 2020-х годов космические системы стали еще более популярными у киберпреступников. Развитие атак происходило в соответствии с общими трендами: атаки на цепочки поставок, шпионаж и кибервымогательство в пользовательском сегменте космических систем, атаки подавления и подмены сигнала, внедрение в каналы связи наземного сегмента спутниковых систем. Атаки могут быть очень узконаправленными. Так, в 2024 году исследователи из компании Proofpoint выявили целенаправленную кампанию по рассылке электронных писем, мишенями которой стали менее пяти организаций – клиентов Proofpoint в Объединенных Арабских Эмиратах, связанных с авиацией и спутниковой связью, а также критически важной транспортной инфраструктурой.

Вредоносные сообщения рассылались с адреса скомпрометированной организации, находящейся в доверительных деловых отношениях с целевыми объектами, при этом для каждой жертвы использовались индивидуально разработанные приманки. В ходе исследования этой кампании был обнаружен новый бэкдор, получивший название Sosano.

В пользовательском сегменте кибератаки затрагивали и непосредственных потребителей услуг. Примечательно, что атаки на устройства в пользовательском сегменте могут быть напрямую не связаны с космическими технологиями. Например, уязвимость Wi-Fi-роутеров Starlink к CSRF-атаке, получившая идентификатор CVE-2023-52235 с рейтингом CVSS 8.8, в равной степени может существовать и в сетевом оборудовании, не связанном с технологиями спутниковой связи. Тем не менее, ущерб от атак с использованием таких уязвимостей может быть выше, чем в сетях, подключенных к интернету с помощью других технологий. Спутниковый интернет дорог и, как правило, используется там, где альтернатив немного или вовсе нет. Поэтому отказ или злонамеренное переконфигурирование устройств спутниковой связи сопряжено с повышенными рисками – в первую очередь с недоступностью или длительными простоями изолированных систем и инфраструктур.

Наглядным примером служит инцидент, случившийся в начале 2022 года, когда от кибератаки пострадали более 5800 ветряных электростанций общей мощностью свыше 11 гигаватт. Компания Enercon уведомила немецкий регулятор в сфере кибербезопасности BSI об инциденте и обратилась к провайдерам спутниковой связи для устранения сбоя, затронувшего, по ее данным, около 30 000 спутниковых терминалов, используемых организациями из различных секторов по всей Европе. Регулятор публично подтвердил факт неисправности оборудования у одного из операторов спутниковой связи, ограничившей возможность проведения технического обслуживания некоторых ветряных турбин, однако никаких подробностей не раскрыл. Позднее стало известно, что причиной сбоя стала кибератака на оператора спутниковой связи VIASAT, обеспечивающего широкополосный доступ для частных пользователей на Украине и во многих европейских странах.

Выяснилось, что первоначальным вектором атаки было неправильно настроенное VPN-устройство, которое злоумышленники использовали для получения удаленного доступа к сети KA-SAT. После перемещения по сети атакующие использовали уязвимости домашних модемов, по заявлению оператора, «переписав часть данных во флеш-памяти и сделав модемы неспособными получить доступ к сети, но не полностью непригодными для использования». Сеть оставалась в автономном режиме в течение нескольких дней. Аналитики компании Sentinel выдвинули гипотезу, якобы злоумышленники использовали механизм управления KA-SAT посредством атаки на цепочку поставок, чтобы распространить программу для удаления данных, предназначенную для модемов и маршрутизаторов. Подобное вредоносное ПО перезаписывает ключевые данные во флеш-памяти модема, не делая его при этом полностью неработоспособным и

требующим замены. Атака и вредонос получили название AcidRain. В 2024 году было опубликовано исследование следующего поколения этого вредоноса – деструктивного ПО AcidPour. В отличие от своего предшественника, нацеленного на определенные модели модемов спутниковой связи, AcidPour ориентирован на более широкий спектр устройств, в том числе на маршрутизаторы и спутниковые интернет-модемы на базе Linux, и массивов хранения данных. AcidPour связывают с APT-группой Sandworm.

Широкое распространение в пользовательском сегменте получили атаки на приемники глобальной навигационной спутниковой системы. ГНСС – это обобщающий термин, обозначающий любую спутниковую систему определения местоположения, навигации и времени, которая предоставляет соответствующую информацию приемникам. ГНСС соответствует представленной в начале статьи схеме и тоже состоит из трех сегментов: космический (спутниковые группировки), наземный (наземные станции управления, станции мониторинга и наземные антенны для передачи данных) и пользовательский (потребительские устройства – от смартфонов до приемников на самолетах и морских судах).

В 2023 году международная группа по обмену информацией об инцидентах и событиях в гражданской авиации OpsGroup сообщила, что в районе Черного моря резко выросло количество инцидентов подмены сигналов ГНСС, что в ряде случаев поставило под угрозу навигацию самолетов. В отчетах упоминались ложные и заглушенные сигналы ГНСС, которые воздействовали на гражданские сигналы GPS, – в результате навигационные системы самолетов показывали неточную информацию о местоположении или не показывали никакой информации вовсе. В худших случаях последствия оказались крайне серьезными: полная потеря бортовой навигации, отказ инерциальной системы отсчета и незаметное отклонение от курса в сторону опасных зон и враждебного воздушного пространства.

Одним из таких векторов атак является эксплуатация наземных ГНСС-приемников, доступных через интернет и содержащих известные или новые уязвимости. В исследовании «Лаборатории Касперского» рассматриваются основные предпосылки и примеры атак на ГНСС-приемники с доступом через интернет. В 2023 году такие атаки провели минимум две группы хактивистов. В мае хактивистская киберпреступная группа SiegedSec получила доступ к спутниковым приемникам в Колумбии в ответ на арест хакера властями страны. А в середине 2023 года эта же группа атаковала устройства нескольких организаций в США и заявила о получении доступа к спутниковым приемникам в Румынии. Еще одной

группой, активно атаковавшей спутниковые приемники в 2023 году, была GhostSec. В течение года она атаковала множество ГНСС-приемников в разных странах, включая Россию и Израиль. Злоумышленники утверждали, что в ходе некоторых атак они не только получили доступ, но и удалили данные со скомпрометированных спутниковых приемников, что дает представление о потенциальном ущербе от таких инцидентов. Исследователи «Лаборатории Касперского» провели анализ данных об уязвимых ГНСС-приемниках с участием 70 поставщиков приемников, используемых по всему миру. Выяснилось что более 3000 приемников уязвимы для атак через интернет.

Атаки на наземный сегмент ГНСС ставят транспорт, который зависит от данных и сервисов ГНСС, в сложное положение. Невозможность определить местоположение самолета затрудняет эшелонирование и обеспечение положения в небе, экипажу становится сложнее планировать полет и принимать решения. Использование нескольких спутниковых систем (GPS, Galileo, ГЛОНАСС) может помочь при спуфинге одной из них, но не спасет при глушении сигнала.

Подводя итог, можно сказать, что в последнее десятилетие в киберпространстве, отвечающем за функционирование космических систем, развернулось многостороннее противостояние. В него вовлечены как хакерские группировки, спонсируемые государствами, так и отдельные хактивисты. Сложные цепочки поставок создают дополнительные риски и затрудняют распределение организационной ответственности за обеспечение безопасности.

Заключение

Рассматривая инциденты в начале космической эры, стоит говорить не о кибератаках, а о технических происшествиях с космическими системами. Уже в то время было очевидно, что незначительный баг способен вызвать серьезнейшие последствия, человеческий фактор является причиной многих печальных инцидентов, а налаженные процессы и контроль за ними – не прихоть, а необходимость для предотвращения и снижения негативного влияния ошибок и упущений при разработке и эксплуатации систем.

Использование космических систем в гражданском секторе – прежде всего для обеспечения коммуникационных и развлекательных сервисов – привело к появлению первых злоумышленников. Поначалу атаки носили характер хактивизма, а немногим позднее коммерциализировались. Говорить о каком-либо существенном разнообразии в тот период не

приходится, однако уже в противостоянии операторов спутникового телевидения и пиратов проявились многие проблемы, актуальные для современного инфобеза: отрицание и замалчивание инцидентов, стремление решить техническую проблему в правовом и организационном поле, возникновение уязвимостей коммерческих технологий из-за желания побыстрее продать продукт или услугу, «гонка вооружений» в сфере кодирования сигнала и взлома кодов.

Кибератаки на космические системы, появившиеся вместе с интернет-технологиями, развивались параллельно с ними. На сегодняшний день космические системы во многих случаях превратились в точку отказа для критически важных систем и инфраструктур. Прогосударственные APT-группы давно проявляют интерес к спутниковым системам, как в части вмешательства в их работу, так и в части использования в собственных целях. Распространение космических технологий делает их привлекательными в том числе и для финансово мотивированных киберпреступников.

В сфере кибербезопасности космических систем по-прежнему практически отсутствует нормативно-правовая база, что вызывает неопределенность в отношении применимых мер и средств контроля. Единого всеобъемлющего договора, посвященного кибербезопасности в космическом пространстве, не существует. Вместо этого действует комплекс принципов, извлеченных из общего международного космического права, резолюций ООН и норм, регулирующих киберпространство на Земле. Таким образом, международное законодательство в области защиты информации в космосе представляет собой «лоскутное одеяло», сотканное из принципов общего космического права, применяемых норм международного киберправа и формирующегося «мягкого права». Основная работа в настоящее время ведется не по созданию нового договора, а по конкретизации и консенсусному принятию норм ответственного поведения, которые призваны снизить риски киберконфликтов в космосе, но вряд ли станут препятствием для заинтересованных злоумышленников.

***

Информация из этой статьи частично была представлена на лекциях «Истории космических миссий через призму информационной безопасности» и «Безопасность систем спутниковой связи» в Музее космонавтики в рамках партнерского соглашения музея и «Лаборатории Касперского».

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com