УДК 341.1/8 **DOI: 10.34670/AR.2020.91.11.018**

Обеспечение кибербезопасности в космическом пространстве

Розенцвайг Анна Игоревна

Кандидат юридических наук,
доцент кафедры теории и истории государства
и права и международного права,
Самарский национальный исследовательский
университет им. академика С.П. Королева,
443086, Российская Федерация, Самара, ш. Московское, 34;
e-mail: lawyeranna@mail.ru

Коныгин Руслан Анатольевич

Магистрант,
Самарский национальный исследовательский
университет им. академика С.П. Королева,
443086, Российская Федерация, Самара, ш. Московское, 34;
e-mail: ru.konygin@gmail.com

Аннотация

В статье проанализировано понятие космических систем как активов, которые существуют либо в суборбитальных, либо в наземных системах управления, включая и средства запуска. Сделан вывод о существовании незначительно развитой инфраструктуры для повышения безопасности космических активов, такой как космические стандарты или организации по обмену информацией о космических системах. Космические активы испытывают значительные проблемы в части кибербезопасности, аналогичные и другим отраслям. Они сталкиваются с уникальным сочетанием угроз, существенно усложняющих возможности снижения рисков для обеспечения кибербезопасности. Рассмотрены проблемы кибербезопасности космических систем, различные атаки на космические системы и современные методы их смягчения, применяемые рядом организаций. Приведены примеры основных угроз для космических систем, выявлены потенциальные мотивы необходимости усиления организациями, государствами уровня защиты космических систем, повышения степени заинтересованности в реализации соответствующих мероприятий. Авторами предложен ряд рекомендаций, способствующих повышению базового уровня кибербезопасности космических активов по сравнению с сегодняшним днем, что может способствовать укреплению барьера для кибератак в этой области.

Для цитирования в научных исследованиях

Розенцвайг А.И., Коныгин Р.А. Обеспечение кибербезопасности в космическом пространстве // Вопросы российского и международного права. 2019. Том 9. № 11А. С. 170-178. DOI: 10.34670/AR.2020.91.11.018

Ключевые слова

Космические системы, космические активы, космическое пространство, кибербезопасность, международное право.

Введение

В настоящее время новыми участниками «космического» рынка предлагается все: космические отели, транспортные системы, управляемые человеком лаборатории космического производства, сбор энергии, добыча ресурсов на астероидах, снимки Земли, небольшие интернет-службы на основе спутниковых сетей, и этот список можно продолжить. Чтобы не отставать, традиционные космические компании также вводят новшества, используя многолетний опыт, пользуясь широким интересом, возникшим вокруг космоса. Очевидно, что не каждый проект или идея будут успешными, и многие, вероятно, будут недооценивать риски, как финансовые, так и технологические. Однако импульс человеческой экспансии выводит нас на новый уровень.

В связи с этим возникает вопрос о том, как управлять развитием столь разнообразной, динамичной экосистемы космических отношений для достижения коллективных целей. К традиционному космическому сообществу инженеров, ученых, техников и правительственных агентов мы должны добавить юристов, предпринимателей, инвесторов, страховые компании, организации по стандартизации, преподавателей университетов и их студентов, представителей малого бизнеса, художников, артистов и др.

В прошлом космическую сферу «обвиняли» в том, что она «разговаривает сама с собой», и теперь мы должны научиться взаимодействовать с гораздо более разнообразным сообществом с множеством различных планов, проблем и мотивов. Усложняет ситуацию тот факт, что обсуждаемый здесь переход происходит в глобальном масштабе. Таким образом, потребность в постоянном международном общении и открытой беседе становится жизненно важной.

Основная часть

Существует множество тем, требующих обсуждения, координации и обучения в растущей космической экосистеме, в том числе определение надлежащих норм и стандартов, установление ответственности и применимых принципов космического права, разработка бизнес-планов и обеспечение финансирования, управление космической средой. Стоит отметить и необходимость определения правил поведения на орбите как для людей, так и для машин, интеграции воздушного и космического движения в управляемую глобальную систему, а также учета динамики спроса и предложения в пограничной среде. Вышеперечисленные проблемы переплетены и не могут быть легко решены изолированно друг от друга.

Настало время для платформы, которая объединяет всю глобальную экосистему, а не только аэрокосмическую отрасль, с целью облегчения необходимых переговоров, нацеливания на результаты и отслеживания решения критических вопросов. Если работать вместе, последовательно, как широкое сообщество интересов в космосе, то можно добиться успеха.

Говоря о критически важной инфраструктуре, следует отметить электрические и водопроводные сети, транспортные системы, оборонную отрасль и финансовый сектор. Однако

редко приходится задумываться о том, где находятся базовые системы, обеспечивающие функциональные возможности технологий в этих секторах, кто разработал технологию и кто может получить доступ к данной технологии и управлять ею.

Большая часть критической инфраструктуры государств опирается на космические системы. Космические системы можно определить как активы, которые существуют либо в суборбитальных, либо в наземных системах управления, включая средства запуска для этих активов. Организации космических активов – это организации, которые строят, эксплуатируют, обслуживают или владеют космическими системами. Некоторые примеры критической зависимости инфраструктуры от космических систем – зависимость агробизнеса от метеорологических и климатических спутников, зависимость вооруженных сил от разведывательных спутников, зависимость различных транспортных отраслей от спутников глобальной системы позиционирования (GPS). Несколько критических секторов инфраструктуры также полагаются на космические системы для глобальной связи. Мы также используем космические системы для научных открытий, которые часто требуют высокоспециализированного и современного оборудования. Такое оборудование, изначально разработанное для научных открытий, впоследствии используется в значимых секторах инфраструктуры после дальнейшего тестирования и коммерциализации интеллектуальной собственности.

Несмотря на усилия по улучшению кибербезопасности столь важной инфраструктуры, кибербезопасности космических систем уделяется мало внимания. Хотя стандартов безопасности зачастую технически достаточно для сдерживания многих атак, их по-прежнему сложно реализовать из-за нехватки времени и ресурсов [Trends…, www]. Однако с точки зрения развития технологий и управления ими космические системы являются более сложными, чем критическая инфраструктура.

Сначала рассмотрим некоторые из основных угроз кибербезопасности для космических систем и потенциальные мотивы того, почему киберпреступники или государства будут заинтересованы в защите космических систем. Проанализируем некоторые проблемы управления кибербезопасностью космической системы, а затем попытаемся оценить шаги, предпринимаемые в настоящее время компаниями и правительственными учреждениями для защиты этих систем.

Почему космические системы являются привлекательной целью? Космические системы имеют важнейшее значение для критически важной инфраструктуры, которая обеспечивает нашу глобальную экономику и оборону, и лежат в ее основе, а также служат центральной точкой отказа для различных отраслей промышленности. Цель скрытного киберзлоумышленника, как правило, заключается в сведении к минимуму воздействия и максимизации влияния. Кто-то может подумать, что хакер, пытающийся подорвать торговлю в США, сначала попытается помешать таким компаниям электронной коммерции, как Amazon.com, нарушить работу интернет-платежей через PayPal. Тем не менее эти компании вкладывают значительные средства в кибербезопасность и постоянно отслеживают свои сети на предмет мошеннической и вредной деятельности. Кроме того, существует несколько систем, которые необходимо было бы взломать одновременно, чтобы вызвать сбой инфраструктуры, которая позволяет работать каждому из этих столпов торговли. С точки зрения киберзлоумышленника, возможно, более простой путь к компрометации торговли в США будет заключаться в нацеливании на спутники

связи, которые обеспечивают подключение к системам кредитных карт в точках продаж, управление запасами и даже услугами видеоконференций. Еще более ценным может быть нацеливание на оператора серии спутников, которые обеспечивают такие услуги.

Спутники и связанные с ними наземные системы управления, обеспечивающие базовую инфраструктурную поддержку, являются центральной точкой отказа для торговли и других отраслей. Без космических систем многие отрасли не могут эффективно функционировать. Например, компании, занимающиеся распределением природного газа, используют спутники для связи с удаленными трубопроводами, чтобы понять состояние своих систем. Хакеры, взломавшие спутник связи, могут вызвать взрывы труб, если они запрещают вызовы на техобслуживание из этих удаленных труб в командный центр распределителя природного газа.

Есть разные пути атаки для подавления центральной точки отказа космической системы, двумя из которых являются производитель оборудования для космических средств и оператор или управляющая компания космических систем. Способность воздействовать на несколько систем путем компрометации центральной точки отказа делает космические системы привлекательными целями.

Космические системы, такие как спутники и средства управления ими, как правило, представляют собой сложное оборудование с учетом их требований к связи, радиационной стойкости и вычислительным возможностям. Несмотря на это, стандарты кибербезопасности для космических активов не регулируются каким-либо руководящим органом, а отсутствие регулирования означает, что спутники не имеют общих стандартов кибербезопасности и могут использоваться для кибератак с безнаказанностью и анонимностью. Это не похоже на другие отрасли, такие как электрические системы, регулируемые Федеральной комиссией по регулированию энергетики (FERC).

На самом деле, регулирование спутников достаточно слабое. Международный союз электросвязи (МСЭ), учреждение ООН, регулирует частоты спутниковой связи для предотвращения помех связи и регистрирует орбиты спутников, но за пределами этих областей существует несколько стандартов. На данный момент нет учреждений, ограничивающих использование спутников, и нет руководящего органа, который контролирует использование спутников. Из-за этого правового вакуума возможно использование некоторых спутников в качестве базы для запуска кибероперациий или для других противоправных киберцелей.

Хотя отсутствие стандартов для таких критически важных систем является проблемой, сложность цепочки поставок, необходимой для создания этих систем, также делает их привлекательными для хакеров. Для некоторых систем потребуются несколько производителей с различными специальностями для разработки технологий и системный интегратор для компиляции всех компонентов, чтобы они функционировали как единое целое. Несколько поставщиков должны предоставить хакеру различные точки доступа для получения доступа к спутнику. Каждый дополнительный поставщик предоставляет дополнительную возможность скомпрометировать спутник. Для наиболее сложных систем существуют строгие протоколы безопасности. Однако не все спутники настолько сложны. Недавняя тенденция включает в себя запуск на орбиту недорогих спутников, использующих готовую коммерческую технологию (COTS). Кубсаты имеют довольно низкий барьер для входа в разработку с технической точки зрения и находятся в рамках бюджета любой крупной компании (или состоятельного любителя) для запуска (как правило, менее 100 000 долларов США).

Принимая во внимание природу спутника COTS, отметим, что вполне вероятно, что такие компоненты, как операционные системы с открытым исходным кодом, изобилующие уязвимостями безопасности, являются центральными для функции этих спутников. Существуют серьезные проблемы безопасности для этих систем, поскольку:

– широкое распространение продуктов COTS означает, что многие люди имеют доступ к устройствам, поэтому хакер может тщательно проанализировать устройство на наличие уязвимостей;
– продукты COTS необходимо активно поддерживать и обновлять для исправления пробелов в системе безопасности, что часто не применяется;
– возможность внести свой «вклад» в код, лежащий в основе технологии с открытым исходным кодом, означает, что уязвимости или бэкдоры программного обеспечения могут быть преднамеренно установлены злоумышленниками.

По состоянию на 2017 г. на орбите находилось примерно 700 кубов [David, www]. Для компании вполне возможно запустить кубсат для оптимизации операций на Земле и тем самым внести уязвимости в свою ИТ-систему. Известно, что правительственные агентства арендуют полосу пропускания на коммерческих спутниках, и это может привести к уязвимостям в военных или других ИТ-системах государственных учреждений, если кубсат не обеспечен надлежащей защитой.

Маловероятно, что злоумышленник выберет путь отключения спутника. Он может взломать малый спутник с помощью движителя и направить его на столкновение с другими спутниками. Столкновение кубсатов – достаточно распространенное явление. В одном случае Европейское космическое агентство заметило, что кубсат прорезал дыру в солнечной панели для своего спутника Sentinel 1-A [Pultarova, www]. Это был непреднамеренный несчастный случай, но можно предположить, что хакер мог причинить больший вред. Космические системы являются привлекательными целями из-за своей способности служить центральной точкой отказа для массивных систем, отсутствия у них мер безопасности и наличия обширной площадки для атаки. Так как большая часть критически важной инфраструктуры (например, США) зависит от космических систем, для хакеров была бы логичной попытка скомпрометировать критическую инфраструктуру с помощью этих средств. Космические системы не нуждаются в существенно отличающихся системах безопасности от другой критически важной инфраструктуры; однако они требуют особого внимания с точки зрения безопасности, поскольку действуют как базовая инфраструктура для критических систем. Они не обязательно считаются частью критических систем и, следовательно, не подпадают под те же стандарты безопасности. Кроме того, как более подробно обсуждается ниже, ответственность за кибербезопасность для космических систем чрезвычайно сложна по сравнению с другими отраслями, что оставляет место для неопределенности относительно того, кто должен защищать эти жизненно важные системы и как они должны быть защищены.

Космические активы уже были скомпрометированы государствами и преступными организациями. Наиболее часто упоминавшиеся атаки были направлены против правительственных и корпоративных космических активов. Эти атаки демонстрируют, что даже хорошо финансируемые космические проекты не имеют соответствующей системы кибербезопасности для защиты от хакеров. Лаборатории Касперского обнаружили, что базирующаяся в России группа кибершпионажа Turla взломала провайдер спутникового

Интернета, чтобы скрыть операции кибершпионажа против стран бывшего Восточного блока от США.

Используя наземную антенну, Turla может обнаруживать IP-адреса пользователей спутникового Интернета, а затем инициировать соединение TCP/IP с украденного IP-адреса. Turla может запутать свои действия, используя похищенный IP-адрес спутника. Обнаружить атаку сложно, поскольку шпионская операция не должна заметно влиять на производительность рядового пользователя; это зависит от того, используют ли хакер и законный пользователь одновременно IP-адрес. Поскольку компьютеры жертвы и злоумышленника будут иметь один и тот же IP-адрес, атака будет скрытой и вряд ли будет помечена системами обнаружения вторжений. Независимо от того, насколько скрытными могут быть космические кибератаки, они могут нанести серьезный ущерб операциям конечного пользователя. Хакеры гипотетически могут использовать технику Turla, к примеру, для нацеливания на удаленную электрическую подстанцию. Злоумышленник может перехватывать пакеты восходящей или нисходящей линии с IP-адреса жертвы или вводить данные в пользовательскую систему, подключенную к IP-адресу. Такой ввод ложных данных в автономный беспилотник может привести к переопределению системы или даже к падению самолета.

Другая космическая кибератака скомпрометировала системы GPS, которые полагаются на спутники для триангуляции определенных положений на Земле. Введение шума в спектр приемника спутника GPS может привести к тому, что приемник GPS на земле не сможет обеспечить считывание. Это техника, известная как глушение. Россия установила глушители GPS на более чем 250 000 вышек сотовой связи, чтобы нарушить навигацию ракет, поступающих из США [Dalton, www]. Хотя в прошлом были использованы «глушилки» GPS, которые необязательно считаются кибератаками, спуфинг GPS является кибератакой из-за манипуляций с сигналом GPS. Подмена GPS намного более опасна, чем глушение, потому что кажется, что GPS работает так, как задумано.

Есть несколько способов обмануть спутник GPS. Одним из механизмов для этого являются компрометация спутникового приемника и изменение выходного сигнала со спутника. Другой возможностью является атака с использованием ложных данных, когда злоумышленник использует имитатор сигнала GPS (чей успех будет ограничен, поскольку он не всегда может обмануть приемник) или программный спуфер. Программно-определенные спуферы более надежны. Они работают, вставляя едва заметный поддельный сигнал за истинным сигналом. Постепенно мощность фальшивого сигнала увеличивается до такой степени, что приемник считает, что фальшивый сигнал действительно является реальным сигналом [Gatherer, www]. Система, которая может выполнить программную атаку с использованием фальсификации, стоит всего лишь около 1000-2000 долларов, что продемонстрировано профессором Тоддом Хамфрисом из Техасского университета.

Многие полагают, что иранцы использовали еще одну атаку такого типа для захвата американского беспилотника в США в декабре 2011 г. [Vaas, www]. В сентябре 2011 г. иранцы заявили, что они освоили новую технику для компрометации самолетов с помощью подмены GPS. Эта техника была продемонстрирована, когда они успешно захватили американский беспилотный аппарат RQ-170 Sentinel, перенастроив координаты GPS-сигнала, чтобы дрон приземлился в Иране, а не на своей базе в Афганистане [Peterson, www]. Американские военные обвинили захват в сбое, но были не в состоянии объяснить, как иранцы получили беспилотник

без изменений.

Эти инциденты представляют собой небольшую выборку среди многих других зарегистрированных кибератак на космических активах [Byrne et al., 2014, www]. Помимо реальных кибератак, в различных отчетах упоминались «мысленные эксперименты» и демонстрационные атаки на космические активы [Santamarta, www].

Заключение

Космические активы являются базовыми системами, на которых основывается наиболее важная инфраструктура государств. Исследователи, политики и инженеры все больше озабочены кибербезопасностью критически важной инфраструктуры, но не задействуют космические ресурсы, которые обеспечивают эти системы. Проблемы кибербезопасности станут более существенными, поскольку технологии продолжают развиваться, и злоумышленники всегда найдут самое слабое звено для проникновения в целевую систему. Сегодня космические активы – наиболее уязвимое звено. Организации, занимающиеся космическими активами, не должны ждать, пока директивные органы примут меры по этому вопросу, поскольку существует несколько шагов, которые могут быть предприняты для защиты своих систем без политического руководства.

Таким образом, ответственные лица должны включать космические активы при рассмотрении вопроса о том, какие технологии требуют киберзащиты, чтобы обеспечить сохраняющуюся цифровую «судьбу» государств, так как настоятельным требованием времени стала необходимость заполнения правового вакуума в обеспечении кибербезопасности космических активов.

Библиография

1. Byrne D.J., Morgan D., Tan K., Johnson B., Dorros C. Cyber defense of space-based assets: verifying and validating defensive designs and implementations // Procedia computer science. 2014. Vol. 28. URL: http://www.sciencedirect.com/science/article/pii/S1877050914001276
2. Dalton A. Russia hopes to block cruise missile attacks with cell towers. URL: https://www.engadget.com/2016/10/17/russia-jamming-cruise-missile-attacks-with-cell-towers/
3. David L. Sweating the small stuff: CubeSats swarm Earth orbit. URL: https://www.scientificamerican.com/article/sweating-the-small-stuff-cubesats-swarm-earth-orbit/
4. Gatherer A. Lost in space: how secure is the future of mobile positioning. URL: https://www.comsoc.org/ctn/lost-space-how-secure-future-mobile-positioning
5. Peterson S. Exclusive: Iran hijacked US drone, says Iranian engineer. URL: https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer
6. Pultarova T. Could cubesats trigger a space junk apocalypse? URL: https://www.space.com/36506-cubesats-space-junk-apocalypse.html
7. Santamarta R. A wake-up call for SATCOM security. URL: https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf
8. The Epic Turla operation. URL: https://securelist.com/the-epic-turla-operation/65545/
9. Trends in security framework adoption: a survey of IT and security professionals. URL: https://static.tenable.com/marketing/tenable-csf-report.pdf
10. Vaas L. Drone hijacked by hackers from Texas College with $1,000 spoofer. URL: https://nakedsecurity.sophos.com/2012/07/02/drone-hackedwith-1000-spoofer/

Cybersecurity in outer space

Anna I. Rozentsvaig

PhD in Law,
Associate Professor at the Department of theory
and history of state and law and international law,
Samara National Research University,
443086, 34 Moskovskoe hwy, Samara, Russian Federation;
e-mail: lawyeranna@mail.ru

Ruslan A. Konygin

Master's Degree Student,
Samara National Research University,
443086, 34 Moskovskoe hwy, Samara, Russian Federation;
e-mail: ru.konygin@gmail.com

Abstract

The article aims to carry out an analysis of the concept of space systems as assets that exist either in suborbital or ground-based control systems, including launch vehicles. Having considered the peculiarities of the space infrastructure from the perspective of ensuring cybersecurity in outer space, the authors of the article point out that there is little infrastructure to improve the security of space assets, such as space standards or organisations that deal with exchanging information on space systems. Space assets experience challenges in the sphere of ensuring cybersecurity that are similar to those in other industries. They face a unique combination of threats that make it much harder to reduce risks in the process of ensuring cybersecurity. The article considers the problems of cybersecurity of space systems, various attacks on space systems and modern methods used by organisations for their mitigation, as well as gives a number of examples of the main threats to space systems and points out the need for organisations and states to strengthen the level of the protection of space systems and to increase their interest in taking relevant measures. Taking into account the results of the analysis of these problems, the authors produce recommendations that will contribute to increasing the basic level of cybersecurity of space assets.

For citation

Rozentsvaig A.I., Konygin R.A. (2019) Obespechenie kiberbezopasnosti v kosmicheskom prostranstve [Cybersecurity in outer space]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 9 (11A), pp. 170-178. DOI: 10.34670/AR.2020.91.11.018

Keywords

Space systems, space assets, outer space, cybersecurity, international law.

References

1. Byrne D.J., Morgan D., Tan K., Johnson B., Dorros C. (2014) Cyber defense of space-based assets: verifying and validating defensive designs and implementations. *Procedia computer science*, 28. Available at: http://www.sciencedirect.com/science/article/pii/S1877050914001276 [Accessed 14/10/19].
2. Dalton A. *Russia hopes to block cruise missile attacks with cell towers*. Available at: https://www.engadget.com/2016/10/17/russia-jamming-cruise-missile-attacks-with-cell-towers/ [Accessed 14/10/19].
3. David L. *Sweating the small stuff: CubeSats swarm Earth orbit*. Available at: https://www.scientificamerican.com/article/sweating-the-small-stuff-cubesats-swarm-earth-orbit/ [Accessed 14/10/19].
4. Gatherer A. *Lost in space: how secure is the future of mobile positioning*. Available at: https://www.comsoc.org/ctn/lost-space-how-secure-future-mobile-positioning [Accessed 14/10/19].
5. Peterson S. *Exclusive: Iran hijacked US drone, says Iranian engineer*. Available at: https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer [Accessed 14/10/19].
6. Pultarova T. *Could cubesats trigger a space junk apocalypse?* Available at: https://www.space.com/36506-cubesats-space-junk-apocalypse.html [Accessed 14/10/19].
7. Santamarta R. *A wake-up call for SATCOM security*. Available at: https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf [Accessed 14/10/19].
8. *The Epic Turla operation*. Available at: https://securelist.com/the-epic-turla-operation/65545/ [Accessed 14/10/19].
9. *Trends in security framework adoption: a survey of IT and security professionals*. Available at: https://static.tenable.com/marketing/tenable-csf-report.pdf [Accessed 14/10/19].
10. Vaas L. *Drone hijacked by hackers from Texas College with $1,000 spoofer*. Available at: https://nakedsecurity.sophos.com/2012/07/02/drone-hackedwith-1000-spoofer/ [Accessed 14/10/19].