Секция «Международная безопасность: космос и мировая политика»

Коммерциализация космоса как источник роста киберугроз: пример Соединенных Штатов Америки

Научный руководитель – Веселов Василий Александрович

Котова Юлия Артемовна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра международной безопасности, Москва, Россия
E-mail: YuliaKUrusova@gmail.com

Современные тенденции освоения космического пространства все больше связаны с процессом коммерциализации (space commercialization). Отдельным примером в данном контексте выступают Соединенные Штаты Америки. За последние годы США смогли достичь большого прогресса с точки зрения освоения низкой околоземной орбиты. Так, на конец 2021 года в космосе уже функционировало более 4000 спутников, при чем, почти 1753 принадлежали американской компании SpaceX[1]. За счёт активного привлечения частных компаний и стартапов к космической деятельности НАСА образует основу для устойчиво-финансируемой космической отрасли, при этом получая возможность сосредоточиться на более амбициозных задачах и проектах, в том числе в дальнем космосе.

От космоса в своей работе зависит экономика США, ее социальные активы, военные системы, отслеживание непрерывности цепочек поставок и пр. В отчете НАСА о готовности агенства обеспечить кибербезопасность за 2021 год указывается, что за последние 4 года оно многократно подвергалось кибератакам. Так, было совершено 6 тыс. нападений на спутники, причем только в 2020 году произошло 1 785 атак [5]. На вопрос, будет ли публично раскрыта первая кибератака на космическую систему в 2022 году, Матье Байи, вице-президент швейцарской компании по кибербезопасности CYSEC, заявил, что никто не может сказать наверняка, но статистически, учитывая рост отрасли, это всего лишь вопрос времени [6].

Принимая во внимание нынешнюю динамику развития государственно-частного партнерства (ГЧП), уже сейчас космические, оборонные и разведывательные сообщества США ставят вопрос о защите космических объектов от возможных киберугроз. Ярким примером актуальности этого вопроса для американского истеблишмента стали публикации администрацией Д. Трампа трех специальных директив по космической политике (SPDS) с целью укрепления стандартов кибербезопасности космических систем. В Конгрессе США продолжает обсуждаться законопроект о признании космических систем в качестве критической инфраструктуры (Space Infrastructure Act, H.R.3713). По мнению Чарльза Деньера, эксперта по кибербезопасности, в нынешнем году США, наконец, могут, принять этот законопроект, что привлечёт дополнительное внимание к защите орбитальных объектов[6].

Коммерциализация, являясь обоюдоострым мечом, несёт в себе как новые угрозы, так и потенциал для их решения. С одной стороны, каждый новый коммерческий актор располагает собственными ресурсами и системами, которые могут не соответствовать необходимым критериям безопасности. Так, в Пентагоне уже всерьёз обеспокоены растущими потоками китайских инвестиций в космические стартапы США и использованием китайского программного обеспечения поставщиками Министерства обороны [2]. С другой стороны, в связи с изменением парадигмы НАСА в пользу более активного развития ГЧП, ресурсы, идеи и возможности частного сектора уже сейчас признаются в качестве важной основы для снижения вероятных рисков в будущем. В качестве примера, демонстрирующего важность координирования действий в киберпространстве в рамках ГЧП, можно

привести инициативу Отдела оборонных инноваций США о создании в «гибридной архитектуры» («hybrid architecture») в космосе [3]. Главная цель проекта — привлечь знания частного сектора для защиты правительственных и коммерческих спутников одновременно в различных доменах. Кроме этого, ряд американских компаний и правительственных структур активно изучают, как технология блокчейн может применяться для защиты важных данных и информации в сложных космических сетях [4]. Американский стартап Xage Security уже работает над стратегией защиты данных Космических сил США, которые прибегают к использованию технологий блокчейн для проверки доступа к отдельным каналам связи и обеспечения безопасности базы данных.

В процессе изучения темы было установлено, что освоение космического пространства представителями частного сектора США — долгосрочный тренд, который поддерживается американским истеблишментом, космическим агенством НАСА и др. Одновременно коммерциализация космоса расширяет поверхности угрозы атак. Для борьбы с ними потребуются ресурсы, знания и возможности как правительства, так и космических коммерческих организаций и компаний. Важным итогом исследования можно считать утверждение, что интенсивность и охваты дальнейшей коммерциализации космоса, развитие государственно-частного партнёрства будут во многом связаны с решением вопросов кибербезопасности. Это в свою очередь способно предопределить будущую эволюцию взглядов государственного сектора относительно перспектив деятельности в космосе частных лиц и структур. В ситуации, когда системы функционирования США завязаны на использовании кибердомена (финансовая, военная, гражданская, экономическая и пр.), вопросы о дальнейшем обеспечении безопасности и реагировании на угрозы будут оставаться центральными в отношениях государства и частных компаний.

Источники и литература

1) Ставицкий А. «Названо количество контролируемых Маском спутников на орбите» // Электронный ресурс Lenta.ru — 06.12.2021 — URL: https://lenta.ru/news/2021/12/06/starlink/ [Дата обращения: 07.03.2022]
2) Erwin S. “DoD trying to keep China from accessing critical U.S. space technology” // SpaceNews. — September, 30 2021. — Available at: https://spacenews.com/dod-trying-to-keep-china-from-accessing-critical-u-s-space-technology/ [Accessed 5 March 2022]
3) Erwin S. “DoD seeks ideas for connecting government and commercial satellites” // SpaceNews. — October, 1 2021. — Available at: https://spacenews.com/dod-seeks-ideas-for-connecting-government-and-commercial-satellites/ [Accessed 19 December 2021]
4) Erwin S. “Industry panel: U.S. space systems need protection against cyber attacks” // SpaceNews. — October, 19 2021. — Available at: https://spacenews.com/industry-panel-u-s-space-systems-need-protection-against-cyber-attacks/ [Accessed 27 February 2022]
5) NASA’s Cybersecurity Readiness, NASA Office of Inspector General Office of Audits, Report No. IG-21-019. — May 18, 2021. — pp. 2-3. — Available at: https://oig.nasa.gov/docs/IG-21-019.pdf [Accessed 7 March 2022]
6) Petkauskas V. “Space security in 2022: expect a hacked satellite” // Cybernews. —January 3, 2022. — Available at: https://cybernews.com/security/space-security-in-2022-expect-a-hacked-satellite/ [Accessed 4 March 2022]