Критерии для тезисов к Молодежному дню научно-практической конференции «Соперничество и сотрудничество в исследовании, освоении и использовании космического пространства»

Тезисы принимаются исключительно в формате Word.

Оформление шапки документа

В начале документа, перед основным текстом необходимо указать:

1) название секции;
2) ФИО автора;
3) название работы.

Объем тезисов не должен превышать 2 страницы (до 6500 печатных знаков включая пробелы). Список источников и литературы в указанный объем не входит.

Текст тезисов будет проходить проверку на оригинальность.

Оформление списка источников и литературы

Оформление списка источников и литературы осуществляется следующим образом:

1) Русскоязычные источники и литература в алфавитном порядке;
2) Англоязычные (и другие) источники в алфавитном порядке.

Список не должен включать более 7 пунктов. В тексте тезисов необходимо указать ссылки на все пункты из списка источников и литературы. Более наглядно ознакомиться с правилами оформления тезисов Вы можете, изучив шаблон.

Шаблон оформления тезисов

Секция «Перспективы сотрудничества в освоении космического пространства в новых политических и экономических условиях»

Котова Юлия Артемовна

Коммерциализация космоса как источник роста киберугроз: пример Соединенных Штатов Америки

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].

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/2021/1 2/06/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-idea s-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]