Литература:
1. *Бирин Д.А., Ляпустин Е.С., Мещеряков Р.В.* Беспилотный летательный аппарат сопровождения группы исследователей с многомодальным управлением / Материалы XII Мультиконференции (МКПУ-2019). 23-28 сентября 2019 г. Дивноморское, Геленджик. В 4 т. Т. 4. – Ростов-на-Дону – Таганрог: Издательство Южного федерального университета, 2019. – С. 67-70.

DOI: 10.25728/iccss.2023.96.61.009

Архипова А.Н., Промыслов В.Г.

Проблема обеспечения целостности и достоверности радиоастрономических данных в открытых проектах

Аннотация: В работе произведен анализ доступных политик информационной безопасности открытых астрономических проектов. Особое внимание, в связи с повышенным вниманием общества к проблеме внеземной жизни, уделено проектам, связанным с поиском внеземных цивилизаций. Анализ политик информационной безопасности позволяет заключить, что не во всех таких проектах информационной безопасности уделено должное внимание. В большинстве проектов отдается внимание угрозам, связанным с вредоносным использованием ресурсов удаленных пользователей или доступ к персональной информации участника. Вместе с тем политики безопасности умалчивают тот факт, что открытые научные проекты по обработке и наблюдению астрономических данных во многом полагаются на специфические технологии искусственного интеллекта и распределенной обработки данных, с участием, возможно, недоверенных субъектов. В работе делается вывод, что научным данным нужна особая политика безопасности, направленная на сохранение их целостности и достоверности, которая отлична от типовых политик информационной безопасности интернета, нацеленных на

сохранения конфиденциальности пользовательской информации.

Ключевые слова: радиоастрономия, открытые проекты, целостность, информационная безопасность

С тех пор как Натаном Ротшильдом был сформулирован известный тезис: «Кто владеет информацией – тот владеет миром», его истинность неоднократно подтверждалась на практике. Информация, вместе со средствами ее передачи и обработки составляют основу современного информационно-телекоммуникационного периода, в котором выделяют следующие основные черты [1]:

– закрепление положения, в том числе на уровне бытовых и юридических норм, что информация является продуктом деятельности человека;

– осознание обществом первичности информации перед другими продуктами человеческой деятельности, выраженное, например, в концепции, что информация правит миром;

– принятие тезиса, что первоосновой всех направлений деятельности человека: экономической, производственной, политической, образовательной, научной, творческой, культурной и т.п. является информация;

– развитие рынка информации, т.е. информация сама по себе является предметом купли-продажи;

– распространение норм, связанных с защитой интеллектуальной собственности на информацию в чистом виде;

– равные возможности в доступе к информации всех слоев населения;

– взаимозависимость безопасности информационного общества от безопасности информации;

– необходимость информационных систем для организации взаимодействия всех структур государства и государств между собой;

– управление информационным обществом со стороны государства и общественных организаций.

Можно заключить, что информация стала объектом, имеющим собственную ценность. Следовательно, как объект, информация является сущностью, которую необходимо защищать. Однако,

очевидно, что не материальность информации вызывает необходимость построения для нее особой модели защиты. Такие модели получили название референтные модели безопасности. Наиболее известные из них КЦД [2], куб Маккамбера [3], или более современная RMIS [4]. Достоинством таких моделей является то, что они выявили основные свойства информации как объекта защиты, а именно конфиденциальность, целостность, доступность, достоверность и др.

Внедрение цифровых, информационных технологий в научную сферу, произошло даже раньше, чем в другие отрасли человеческой деятельности, например банковскую или промышленность. Однако, до сих пор политике информационной безопасности для нее не уделялось достаточного внимания, если не брать во внимание прикладные исследования, связанные с критическими областями, как, например, ядерная физика, химия, и тд. В большинстве данные по фундаментальным исследованиям остаются доступными, и главной целью политики безопасности выступала охрана авторского права (проблема плагиата) [5].

Вместе с тем, в настоящее время в фундаментальной науке, особенно в таких ее областях как астрономия и астрофизика, наблюдается значительный рост объемов экспериментальных данных и переход к их распределенной модели обработки и хранения. Причинами взрывного роста данных в астрономии в последние десятилетия являются как эволюционное изменение используемой аппаратуры для наблюдения, так и появление существенно новых режимов работы. Объем памяти и чувствительность астрономических приемников излучения растут существенно быстрее, чем размеры и даже количество самих телескопов, а это пропорциональное увеличение объема получаемой информации. Появляются и научные задачи, требующие как получения огромного количества наблюдений одного и того же объекта с малыми экспозициями – это, например, поиск быстрой переменности космических объектов, так и задачи достижения дифракционного предела качества изображений на наземных инструментах (спекл-интерферометрия или Lucky Imaging).

Другим источником все возрастающего потока научной информации становятся многочисленные систематические обзоры

небесной сферы в различных диапазонах длин волн и с различными задачами [6]. Объемы данных, получаемых в этих обзорах, растут со временем. Например, объем астрономических каталогов вырос с нескольких десятков гигабайт в DSS [7] до десятка терабайт в SDSS [8].

Необходимость обрабатывать и анализировать гигантские массивы данных в астрономии стимулировала широкое применение алгоритмов искусственного интеллекта (ИИ), а также привело к переходу к распределенной модели вычисления. Для алгоритмов ИИ с обучением появились проекты, построенные на основе краудсорсинг – привлечение сторонних энтузиастов для анализа данных. Например, проекты гражданской науки (Citizen science), доступные для всех [9]. При этом быть специалистом не всегда обязательно: многие проекты рассчитаны на обычных людей и доступны даже детям. Астрономические наблюдения и обработка данных – самое развитое направление гражданской науки.

Переход к новым алгоритмам обработки научных данных в астрономии, совпавший с возрастанием роли науки в жизни общества и повышением влияния науки в обществе выявил актуальность вопроса анализа и возможного пересмотра политик безопасности открытых научных данных с точки зрения обеспечения их целостности и доверия.

Политики безопасности будут рассмотрены на примере астрономических проектов, построенных на основе краудсорсинга, а также проектов, связанных с поиском внеземных цивилизаций (англ. SETI-Searach extraterrestrial intelligence).

Выбор астрономической тематики, в особенности проектов, связанных с обнаружением внеземной жизни, во многом обусловлен тем резонансом, который вызывает в обществе публикация информации о космических явлениях, связанных с внеземным разумом, включая проблему неопознанных летающих объектов (НЛО). В работе не рассматриваются аспекты информационной безопасности характерные для активного поиска внеземных цивилизаций посредством материальных или информационных посланий, например проекты METI (англ. Messaging extraterrestrial intelligence) [10] или проблемы возможного обнаружения разумной деятельности на Земле другими разумными

существами по каналам утечки информации, в частности по побочному изучению Земли в радиодиапазоне [11].

Астрономические данные как часть общего информационного пространства

Тема космоса и внеземных цивилизаций с древнейших времен, никогда не исчезала с информационного ландшафта человеческого общества, но особую притягательность она получила, в связи с развитием технологий, связанных с полетом в космос и наблюдательной (радио)астрономии, начиная со второй половины 20 века. Наблюдения с помощью телескопов НАСА «Кеплер», «Тесс», «Джеймс Уэбб», ЕКА «Гайя», показали, что в нашей Галактике существуют миллиарды потенциально обитаемых экзопланет [12]. Изобилие экзопланет в сочетании с обилием строительных блоков жизни (сложных органических молекул и воды) во Вселенной, а также наблюдаемая однородность и изотропность Вселенной в целом, наводит на мысль, что сама жизнь должна быть рядовым явлением и в изобилии во Вселенной. Поиск жизни во Вселенной ведется путем поиска наличия как биосигналов, так и техносигналов.

В научном сообществе в разное время в разных странах разрабатывалось несколько проектов по поиску внеземной жизни, наибольшую известность, видимо, имеет фундаментальная программа SETI, которая велась параллельно в США, в Советском Союзе и некоторых других странах. Нам не удалось найти информацию о политике информационной безопасности подобных проектов. Мы предполагаем, что в этом случае политика безопасности не отличалась от принятой в научной среде политики безопасности для открытых научных данных, например [13].

На бытовом восприятии, тема Космоса проявляется в виде феномена неопознанных летающих объектов (НЛО), интерес к которому наблюдается до последнего времени в интерпретации неидентифицированных воздушных феноменов (англ. unidentified aerial phenomena) [14].

Поиск НЛО осуществлялся также в рамках отдельных правительственных программ, например, Blue Book, Sign и др. [15]. В отличие от фундаментальных подобных программ, в них аспекты, связанные с информационной безопасностью поиска НЛО, были

ясны достаточно рано [16]. В работе Хайнека [15] приведено мнение, что изначально официальная программа США изучения НЛО (проект Blue Book) имела сильный социологический и политический контекст. Основная цель политики безопасности военного ведомства США в отношении НЛО по Хайнекену заключается в том, что любое сообщения об НЛО, может рассматриваться как элемент информационной войны. В соответствии с этим было выделено две угрозы.

1. Информация об НЛО может маскировать, действительные события, и вызвать тенденцию игнорирования реальных замечаемых признаков враждебных действий, которые могут иметь влияние на безопасность государства;

2. Под влиянием ложных тревог, в обществе может культивироваться болезненная психология, в которой умелая враждебная пропаганда сумеет вызвать истерическое поведение и вредное недоверие к информации, предоставляемой по официальным каналам.

Добавим, что третьей угрозой, связанной с популярностью феномена НЛО и темы космоса, может считаться использование информации по данной тематике, в социальном аспекте [16], например, в качестве средства переключения внимания общества, с конкретных проблем.

Данные угрозы во многом являются переосмыслением классических угроз информационной безопасности в виде целостности и достоверности данных.

Если рассматривать жизненный цикл научных данных в контексте модели канала информации Шеннона, то можно заключить, что угрозы нарушения целостности и достоверности данных могут быть реализованы на любом из этапов жизненного цикла научных данных, однако на наш взгляд наиболее уязвимыми могут считаться этап формирования данных (наблюдение), этап передачи для обработки и сама обработка данных [17].

Интерес общества к космической тематике, влияние информации по ней на настроения и поведение как общество в целом, так и его индивидов поднимает важность проблемы разработки действенной политики информации для таких типов данных в соответствии с выявленными выше угрозами.

Открытые астрономические проекты по поиску техносигналов в радиодиапазоне

Перечислим некоторые основные открытые проекты, связанные с астрономическими наблюдениями по поиску техносигналов.

Проект SETI@home (1999 – 2020) [18] – это проект, созданный исследовательским центром при Калифорнийском университете, занимавшийся поиском и анализом возможных радиосигналов от внеземного разума. Проект являлся одним из пионерских проектов по внедрению распределенных научных вычислений в недоверенной среде. SETI@home показал научному сообществу, что проекты распределенных вычислений, использующие подключенные к Интернету компьютеры, могут быть эффективным инструментом анализа, даже превосходящим некоторые из лучших мировых суперкомпьютеров. В настоящий момент проект заморожен.

Его современным аналогом является проект по поиску радиосигналов с техносигнатурой UCLA SETI [19]. Проект заявляет две основные цели:

– определить наиболее многообещающие сигналы в данных SETI;

– помочь создать инструменты искусственного интеллекта для распознавания радиочастотных помех (англ. RFI).

При обработке сигналов используются алгоритмы ИИ. Для алгоритмов ИИ с обучением для улучшения классификации сигналов-кандидатов в качестве RFI или внеземных сигналов требуется помеченный обучающий набор. Добровольному участнику проекта предлагается классифицировать сигналы, сопоставляя их с распространенными классами радиочастотных помех для обнаружения наиболее перспективных сигналов в наблюдательных данных.

Астрономические данные как объект информационной безопасности

Согласно классическим подходам информационной безопасности Политика безопасности (security policy), это заявление о том, что является, а что нет, допустимым [20] в контексте объекта защиты. В более развернутом смысле это означает, что должен быть определен набор правил, которые регламентируют способ

предоставления сервисов безопасности системой или организацией для защиты ее объектов и обеспечивает планирование всей программы обеспечения безопасности.

Из приведенного выше обзора открытых астрономических проектов можно заключить, что общим трендом является широкое использование ИИ и развертывание распределенной архитектуры проекта, что определяет основную модель угроз таких проектов:

– Применение ИИ позволяет предположить наличие спектра сценариев атак, характерных для данной технологии [21].

– Распределенная обработка и наблюдение данных, выполняемой за пределами доверенной среды, приводит к уменьшению общего доверия к результатам [22], например это порождает возможность для злонамеренного конечного пользователя напрямую вкладывать недостоверную информацию на этапе наблюдения.

Являясь в большинстве случаев открытым и публичным документом, политика безопасности, дает возможность составить представление о программе безопасности астрономических проектов указанного типа. Нами рассмотрены доступные политики безопасности открытых проектов обработки астрономических данных [13, 19, 23] и проанализированы их свойства по основным признакам, принятым для политик безопасности:

1. Заявлены ли цели информационной безопасности и если они заявлены, то их формулировки;
2. Содержит ли обязательство соответствовать применимым требованиям, относящимся к информационной безопасности;
3. Содержит ли обязательство постоянно улучшать систему менеджмента информационной безопасности.
4. Доступна ли политика в виде документированной информации.

Из открытого материала политик безопасности мы не можем выделить, какие цели безопасности являются основными для проектов под эгидой NASA [13].

Заключение

Как можно заключить из анализа доступных политик безопасности и их характеристик, приоритетной целью

большинства проектов является сохранение конфиденциальности данных участника проекта. Целостность данных и доверия к результатам обработки не указаны явно в приоритетных целях. Проведенный анализ позволяет заключить, что в некоторых проектах, использующий распределенную обработку в недоверенной среде и применение алгоритмов искусственного интеллекта возможна реализация угрозы информационной безопасности, связанной с нарушением целостности, ошибками обработки, или подмены данных. Данные технологии позволяют недобросовестному участнику воздействовать на результаты исследований, посредством прямого изменения данных, и/или воздействия на формирование пространства признаков в системах искусственного интеллекта с обучением. Поэтому следует рекомендовать как разработчиком таких проектов, так и пользователям, вовлеченным в проект, больше уделять внимания вопросам обеспечения кибербезопасности для данных угроз.

Литература:

1. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы». – URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения 30.10.2023*).*

2. *Saltzer J.H., Schroeder M.D.* The Protection of Information in Computer Systems. – URL: http://www.acsac.org/secshelf/papers/protection_information.pdf (дата обращения 30.10.2023*).*

3. *McCumber J.* Information Systems Security: A Comprehensive Model / Proceeding of the 14th National Computer Security Conference, NIST. – Baltimore, MD, 1991. – P. 328-337.

4. *Cherdantseva Y. and Hilton J.* A Reference Model of Information Assurance & Security / International Conference on Availability, Reliability and Security. – Regensburg, 2013. – DOI: 10.1109/ARES.2013.72.

5. *Куркова Н.А., Шершень Т.В.* О принципе добросовестности в научных исследованиях // Методологические проблемы цивилистических исследований. – 2019. – №1. – URL: https://cyberleninka.ru/article/n/o-printsipe-dobrosovestnosti-v-nauchnyh-issledovaniyah (дата обращения 04.11.2023).

6. *Padovani Paolo.* The faint radio sky: radio astronomy becomes mainstream // The Astronomy and Astrophysics Review. – 2016. – № 24. – Article number 13. – DOI: 10.1007/s00159-016-0098-6.

7. Digital Sky Survey System (DSS) – Canadian Astronomy Data Centre Enabling the next astronomical discoverie. – URL: https://www.cadc-ccda.hia-iha.nrc-cnrc.gc.ca/en/dss/ (дата обращения 04.11.2023).

8. The Sloan Digital Sky Survey. – URL: https://www.sdss.org/science/ (дата обращения 04.11.2023).

9. NASA's citizen science projects are collaborations between scientists and interested members of the public. – URL: https://science.nasa.gov/citizen-science/ (дата обращения 12.10.2023).

10. *Schirber M.* Attempts to Contact Aliens Date Back More Than 150 Years. – URL: https://www.space.com/6370-attempts-contact-aliens-date-150-years.html& (дата обращения 12.10.2023).

11. *Зайцев А.Л.* Вероятность обнаружения земных радиосигналов враждебной суперцивилизацией // Электронный «Журнал радиоэлектроники». – 2008. – № 5. – URL: http://jre.cplire.ru/jre/may08/index.html (дата обращения 12.10.2023).

12. *Steve Bryson et al.* The Occurrence of Rocky Habitable-zone Planets around Solar-like Stars from Kepler Data // The Astronomical Journal. – 2021. – Volume 161. Number 1. – 36 (32 p.). – DOI: 10.3847/1538-3881/abc418.

13. NRAO Computer Use Policy. – URL: https://www.nrao.edu/policy/usepolicy.shtml (дата обращения 12.10.2023).

14. NASA to Release, Discuss Unidentified Anomalous Phenomena Report. – URL: https://www.nasa.gov/news-release/nasa-to-release-discuss-unidentified-anomalous-phenomena-report/ (дата обращения 12.10.2023).

15. *Hynek J.* The Hynek UFO Report. – New York: Dell Publishing Company, 1977. – 299 p.

16. *Westrum R.* Social Intelligence about Anomalies: The Case of UFOs // Social Studies of Science. – 1977. – Vol. 7. № 3. – P. 271-302. – DOI:10.1177/030631277700700302.

17. Belgium UFO that puzzled NASA was polystyrene fake. – URL: https://phys.org/news/2011-07-belgium-ufo-puzzled-nasa-polystyrene.html (дата обращения 12.10.2023).

18. SETI@Home. – URL: https://setiathome.berkeley.edu/ (дата обращения 12.10.2023).

19. UCLA SETI. Are we alone in the universe? – URL: https://seti.ucla.edu/wp (дата обращения 12.10.2023).

20. ГОСТ Р 56205. Защищенность (кибербезопасность) сети и системы. Часть 1-1. – М.: Стандартинформ, 2014. – 80 с.

21.*Swagat M. Karve, ArpitYadav, Prateek Datta.* Artificial Intelligence in Cyber Security // REST Journal on Emerging trends in Modelling and Manufacturing. – 2022. – Vol. 8(2). – P. 99-106. – DOI: 10.46632/jemm/8/2/6.

22. *Richard A. Carrigan Jr.* Do potential SETI signals need to be decontaminated? // Acta Astronautica. – 2006. – Volume 58. Issue 2. – P. 112-117. – DOI: /10.1016/j.actaastro.2005.05.004. – URL: https://www.sciencedirect.com/science/article/abs/pii/S0094576505002286?via%3Dihub (дата обращения 12.10.2023).

23. *Azra, M.N., Wong, L.L., Aouissi H.A., Zekker I., Amin M.A., Adnan W.N.W., Abdullah M.F., Abd Latif Z., Noor M.I.M., Lananan F., Pardi F.* Crayfish Research: A Global Scientometric Analysis Using CiteSpace // Animals. – 2023. – Vol. 13(7). – 1240. – DOI: 10.3390/ani13071240. – URL: https://www.mdpi.com/2076-2615/13/7/1240

DOI: 10.25728/iccss.2023.65.11.010

Plotnikov N.I.

Ontological design of the concepts of the safety

Abstract: The safety of technosphere activity presupposes the existence of scientific grounds for research and development of an intellectual product in the form of technical regulation standards. The problem of identification of the subject and definitions of aviation safety notes contradictions and inconsistencies in the terms and definitions of existing practiced standards. The solution of the terminological problem is possible through the reduction of the meanings of the linguistic units of the word and the definition of the term. The method of ontological designing in this paper is considered as a scientific approach to reduce the uncertainty in the description of complex structural objects and events.