Шаханова М.В., Битян М.А., Шаханова Э.С. Информационная безопасность в космической сфере // Международный журнал информационных технологий и энергоэффективности. – 2024. –
Т. 9 № 2(40) с. 97–101

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОСМИЧЕСКОЙ СФЕРЕ

[1]Шаханова М.В., Битян М.А., Шаханова Э.С.
ФГБОУ ВО «МОРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АДМИРАЛА Г.И. НЕВЕЛЬСКОГО», Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

В данной статье проанализировано понятие информационной безопасности, из чего она состоит и как применяется. Также рассмотрено более узкое применение информационной безопасности в такой сфере как космос. Особое внимание уделяется роли космической информации в современных условиях и показана взаимосвязь космической деятельности и информационной безопасности.

Ключевые слова: Информационная безопасность, информация, безопасность в космосе, космос, безопасность, космическая сфера.

INFORMATION SECURITY IN THE SPACE SECTOR

[1]Shakhanova M. V., Bityan M.A., Shakhanova E.S.
MARITIME STATE UNIVERSITY NAMED AFTER G.I. NEVELSKOY, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

This article analyzes the concept of information security, what it consists of and how it is applied. A narrower application of information security in such an area as space is also considered. Special attention is paid to the role of space information in modern conditions and the relationship between space activities and information security is shown.

Keywords: Information security, information, security in space, space, security, space sphere.

Информационная безопасность — это практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации. Это достигается, в основном, посредством многоэтапного процесса управления рисками, который позволяет идентифицировать основные средства и нематериальные активы, источники угроз, уязвимости, потенциальную степень воздействия и возможности управления рисками. Этот процесс сопровождается оценкой эффективности плана по управлению рисками.

В реальности пока не видно масштабных и успешных кибератак на космическую технику. Хотя подозрения иногда возникают. Так, некоторые конспирологи обвиняли хакеров в провалах последних запусков российских зондов к Марсу. Тут есть определенная логика: ведь первую мягкую посадку на Марс совершила советская станция «Марс-3» еще в 1971 году, она даже доставила туда первый марсоход. Казалось бы, дальше все должно быть еще успешнее. Но спустя четверть века, в 1996 году, станция «Марс-96» с четырьмя посадочными модулями сгорела вскоре после запуска. Та же история повторилась в 2011 году: неудачей закончился запуск российской станции «Фобос-Грунт», вместе с которой погиб и первый китайский зонд для Марса «Инхо-1».[1]

Да, в официальной версии аварий этих станций нет никаких хакеров. Но если почитать интервью гендиректора НПО им. Лавочкина, там ясно сказано, что проблемы с безопасностью у них были очень серьезные, и аппаратуру марсианских станций можно было легко повредить еще до запуска: «Поленился надеть антистатический браслет, коснулся тайком аппарата — щелкнуло статическое электричество, и все, где-то перегрузилась микросхема, бомба для будущих проблем заложена…»

Информационная безопасность в космических системах играет ключевую роль в обеспечении успешного функционирования и защите критически важных данных. Космические системы, такие как спутники связи, спутники навигации и космические аппараты, подвержены различным угрозам, включая кибератаки, воздействие на операционные системы и физическое воздействие из космоса.[2]

Для обеспечения информационной безопасности в космических системах используется комплексный подход, который включает в себя криптографическую защиту данных, защиту от вредоносного программного обеспечения, аутентификацию и авторизацию пользователей, мониторинг и обнаружение аномалий в работе системы.

Также важным аспектом обеспечения информационной безопасности в космических системах является физическая защита оборудования от радиационных воздействий, электромагнитных помех и других внешних факторов, которые могут повлиять на нормальное функционирование системы.

Кроме того, важную роль играет защита от несанкционированного доступа к космическим системам и сетям, что включает разработку надежных систем аутентификации и контроля доступа.

Конфиденциальность данных в космических проектах означает, что только авторизованные лица имеют доступ к информации. Для обеспечения конфиденциальности данных используются различные криптографические методы, такие как шифрование. Шифрование позволяет преобразовать данные в непонятный вид, который может быть прочитан только с использованием специального ключа. Таким образом, даже если злоумышленник получит доступ к зашифрованным данным, он не сможет прочитать их без ключа.

Целостность данных в космических проектах означает, что данные не были изменены или повреждены в процессе передачи или хранения. Для обеспечения целостности данных используются хэш-функции. Хэш-функция преобразует данные в непрерывную строку фиксированной длины, называемую хэш-значением. Любое изменение данных приведет к

изменению хэш-значения. При получении данных получатель может вычислить хэш-значение и сравнить его с полученным хэш-значением, чтобы убедиться в целостности данных.[3]

Доступность данных в космических проектах означает, что данные доступны для использования в нужное время. Для обеспечения доступности данных используются методы резервного копирования и репликации данных. Резервное копирование позволяет создать резервную копию данных, чтобы в случае потери или повреждения основных данных можно было восстановить информацию. Репликация данных позволяет создать несколько копий данных и распределить их по различным местам, чтобы обеспечить доступность данных в случае отказа одного из хранилищ.[4]

В современном мире космос становится все более активной сферой деятельности. Космические аппараты не только проводят научные исследования, но и выполняют коммерческие миссии, связанные с телекоммуникациями, навигацией и другими аспектами жизни на Земле. Как следствие, вопрос информационной безопасности в космосе становится все более актуальным. В данной статье рассмотрим вызовы, с которыми сталкиваются специалисты в области космической информационной безопасности, а также возможные решения этих проблем.

Космическая сфера деятельности становится все более важной и интенсивной, что приводит к появлению новых вызовов в области информационной безопасности. Одним из главных вызовов является защита от хакерских атак. Космические аппараты, особенно те, которые используются в коммерческих целях, часто содержат конфиденциальную информацию, которая может быть целью для злоумышленников. [5]Кроме того, данные, передаваемые с космических аппаратов, могут быть подвержены перехвату или подмене, что также является серьезной угрозой.

Другим вызовом является защита космических аппаратов от вредоносного программного обеспечения. Поскольку аппараты работают в условиях космического пространства, где обновление программного обеспечения может быть затруднено, защита от вирусов и других вредоносных программ становится особенно важной задачей.

Для решения вызовов информационной безопасности в космосе необходимо предпринять целый ряд мер. Одним из ключевых решений является использование криптографических методов защиты данных. Это позволяет зашифровать информацию, передаваемую с космических аппаратов, и предотвратить ее перехват или подмену. Кроме того, важно обеспечить защиту от хакерских атак путем применения современных методов обнаружения и предотвращения вторжений.

Еще одним решением вызовов информационной безопасности в космосе является использование защищенных систем управления и управления доступом. Это позволяет предотвратить несанкционированный доступ к информации, а также обеспечить защиту от вредоносного программного обеспечения.

Кроме того, важно проводить регулярные аудиты безопасности космических аппаратов, чтобы выявлять и устранять уязвимости в системах информационной безопасности. Это позволит минимизировать риски воздействия внешних угроз на космические миссии и обеспечить сохранность конфиденциальной информации.

В космической области информационная безопасность проявляется в защите информационных систем, коммуникаций и данных, которые используются в космических

миссиях, на борту космических аппаратов, спутников связи и навигации, а также на земле для управления и контроля космическими объектами.

Основные компоненты информационной безопасности в космосе включают в себя:

1. Защиту от кибератак: Космические системы подвержены угрозам кибербезопасности, их нужно защищать от несанкционированного доступа, вредоносных программ, кибершпионажа и других киберугроз.
2. Криптографическую защиту: для обеспечения конфиденциальности и целостности данных в космических системах применяются различные методы криптографии.
3. Защиту от физических угроз: В космосе данные и оборудование могут подвергаться воздействию радиации, космических лучей, метеоритов, экстремальных температур и других физических воздействий. Информационная безопасность также включает защиту оборудования от этих факторов.
4. Аутентификацию и авторизацию: Важные компоненты информационной безопасности, позволяющие предотвратить несанкционированный доступ к системам и данным.
5. Мониторинг и обнаружение инцидентов: Непрерывное мониторинг и обнаружение аномалий в работе информационных систем позволяют оперативно реагировать на возможные проблемы и атаки.

Таким образом, информационная безопасность в космосе защищает как данные, так и оборудование от кибератак, физических воздействий и несанкционированного доступа, обеспечивая надежную и безопасную работу космических систем.

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.

Список литературы

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с.
2. Международное космическое право: Учебник / Отв. ред. Г.П. Жуков, Ю.М. Колосов. – М.: Междунар. отношения, 1999. – С. 360.
3. Шаханова М.В., Четверик М.А., Шаханова Д.С. – «Механизмы защиты информации в беспроводных сетях» // Международный журнал информационных технологий и энергоэффективности ISSN 2500-1752 Т. 7 № 4(26) 2023.
4. Sakhanova M.V., Mongush E.L. Virtual machine detection techniques used by malwares and possible countermeasures. The 5th annual student scientific conference in English. Conference proceedings. 2018. С. 110-111.

5. Шаханова М.В., Малый М.Г., Шаханова Д.С. – «Автоматизация процессов информационной безопасности»//Международный журнал информационных технологий и энергоэффективности ISSN 2500-1752 Т. 7 № 4(26) 2023.

References

1. Malyuk A.A. Information security: conceptual and methodological foundations of information protection. Textbook for universities. – M.: Hotline-Telecom, 2004. – 280 p.
2. International space law: Textbook / Ed. by G.P. Zhukov, Yu.M. Kolosov. – M.: International Law. relations, 1999. – p. 360.
3. Shakhanova M.V., Chetverik M.A., Shakhanova D.S. – "Information security mechanisms in wireless networks" // International Journal of Information Technology and Energy Efficiency ISSN 2500-1752 Vol. 7 No. 4(26) 2023.
4. Sukhanova M.V., Mongush E.L. Virtual machine detection techniques used by malware and possible countermeasures. The 5th annual student scientific conference in English. Conference proceedings. 2018. pp. 110-111.
5. Shakhanova M.V., Maly M.G., Shakhanova D.S. – "Automation of information security processes" // International Journal of Information Technology and Energy Efficiency ISSN 2500-1752 Vol. 7 No. 4(26) 2023.