УДК: 656

УГРОЗЫ ТРАНСПОРТНОГО КИБЕРПРОСТРАНСТВА

Дешко И.П.

к.т.н., доцент, РТУ МИРЭА, E-mail: dip@mirea.ru, Москва, Россия

Аннотация

В статье исследуются угрозы транспортного киберпространства как объективной реальности в результате технологического развития общества. Появление киберпространства привело к появлению киберугроз, которые в ряде случаев являются информационными угрозами, а в других случаях имеют свою специфику. Дана структурная схема транспортного киберпространства, которая обуславливает появление угроз. По сравнению с другими видами киберпространств транспортное киберпространство обладает наибольшим числом связей и отношений внутри себя. Кибербезопасность является более общим понятием по сравнению с информационной безопасностью. Рассмотрены общие и частные классификации угроз для транспортного киберпространства. Отмечены методы борьбы с угрозами.

Ключевые слова:

Транспорт, транспортное киберпространство, информационные угрозы.

THREATS TO TRANSPORT CYBERSPACE

Deshko I.P.

PhD, Associate Professor, RTU MIREA, E-mail: dip@mirea.ru,
Moscow, Russia

Abstract

The article examines threats to transport cyberspace as an objective reality as a result of technological development of society. The emergence of cyberspace has led to the emergence of cyber threats, which in some cases are information threats, and in other cases have their own specifics. A structural diagram of transport cyberspace is given, which determines the emergence of threats. Compared with other types of cyberspace, transport cyberspace has the largest number of connections and relationships within itself. Cybersecurity is a more general concept compared to information security. General and specific classifications of threats to transport cyberspace are considered. Methods for combating threats are noted. For these conditions, a modified method for solving the transport problem is proposed, which reduces the imbalance of the solution under any transportation conditions.

Keywords:

Transport, transport cyberspace, information threats.

Введение

Современное управление транспортом характеризуется использованием различных информационных пространств. Широко применяют информационное пространство [1], применяют информационное управляющее пространство [2], применяют информационное радиорелейное пространство [3], информационное пространство электронных меток [4], спутниковое навигационное пространство [5], пространство мобильной связи, пространство интернета вещей [6] и другие. В дополнение к пространству применяют модель информационного поля [1] как интегральную модель реальности. информационное поле определяет содержательность информационных пространств.

Одним из наиболее сложных пространств является киберпространство [7], которое также существует в сфере транспорта, но использует либо неявно как среда коммуникации, либо с помощью специальных технологий, например, транспортных киберфизических систем [8]. Интеграция управления транспортом приводит к объективной необходимости создания и применения транспортного киберфизического пространства [9]. Одна из особенностей транспортного киберфизического пространства состоит в росте числа угроз [9]. Это ставить задачу отражения таких угроз. Для отражения угроз необходим их глубокий анализ. систематика и рекомендации по отражению. В процессе анализа угроз необходимо использовать информационное моделирование [10] и имитационное моделирование [11].

Киберпространство содержит большие объемы необходимой для управления информации. Кроме этого, оно характеризуется информационной неопределенностью [12]. Исходной информацией для анализа неопределенности и управления транспортом являются фактофиксирующие модели [13]. Современные транспортные киберпространства характеризуются ростом сложности и ростом информационных объемов. Требование оперативного принятия решений приводит к необходимости «держать под рукой» большие объемы информации на случай различных ситуаций. Чем более скоростное движение, тем большие объемы информации о ситуации надо иметь. Чем больше объемы информации, тем больше угроз в киберпространстве. Таким образом, анализ угроз киберпространства представляет собой сложную комплексную задачу.

Модель транспортного киберпространства

В настоящее время киберпространство определяют по-разному, но за рубежом есть устойчивое понятие киберпространства как сетевой «системы систем». Термин «киберпространство» официально принят в 1990-х годах [14] для обозначения пространства Всемирной паутины или Интернета. С появлением интернета Вещей и киберфизических систем термин приобрел расширенное значений. В каждой отрасли имеется свое специфическое киберпространство. В транспортной отрасли существует транспортное киберпространство. На рис.1 дано схематическое изображение транспортного киберпространства.

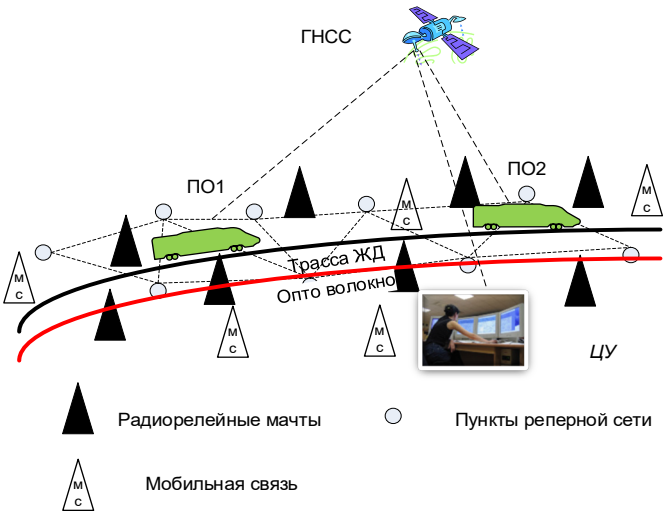

Рисунок 1. Примерная структура транспортного киберпространства

Исходя из сетевой концепции, киберпространство есть интеграция разных сетей в единую систему. На рисунке 1 показана трасса ЖД черной линией. Транспортное киберпространство является одним из самых сложных киберпространств. Оно включает оптоволоконную линию (линия красного цвета рис.10. Оно включает пространство мобильной связи, которое показано базовыми станциями с символами «МС». Транспортное киберпространство включает радиорелейное информационное пространство. На рисунке 1 они обозначены радиорелейными станциями в виде черной пирамидки.

Транспортное киберпространство включает спутниковое информационное пространство. На рисунке 1 показан один спутник ГНСС. В реальности их не менее четырех. Транспортное киберпространство включает информационное пространство электронных меток. На рисунке 1 они не показаны, так как крепятся на трассе и совпадают с трассой. На рисунке 1 символами ЦУ показан центр управления. Особенностью транспортного киберпространства является то, что оно имеет физическую конфигурацию [15] и требует координатного обеспечения и координатной привязки [16]. Транспортное киберпространство тесно связно с геоинформационным пространством [17]. На рисунке 1 показаны подвижные объекты (ПО). Схема на рисунке 1 является статической. В реальном киберпространстве существуют информационные отношения и связи разных типов: «ПО-ПО»; «ГНСС-ПО»; «ГНСС-ЦУ»; «ПО – радиорелейное пространство»; «ЦУ – радиорелейное пространство»; «ПО – сенсоры»; «сенсоры – видимая ситуация»; «сенсоры – невидимая ситуация»; «ЦУ – пространство электронных меток»; «ПО – состояние внешней среды»; «ЦУ -состояние реперной сети»; «ЦУ – состояние пути»; «ПО – мобильная связь»; «ЦУ – связь по оптоволокну»; «ЦУ – киберу-

грозы»; ПО – киберугрозы»; «трафик – план перевозок»; «трафик – оптимизация маршрута»; «состояние груза -ЦУ» и другие. Многообразие связей создает сложность их контроля и обработки информации. В таком многообразии риски угроз возрастают. Схема на рис. 1 задает типы угроз транспортного киберпространства.

Общие типы угроз

Транспортное киберпространство подвергается различным типам угроз безопасности, которые могут привести к значительным финансовым потерям в транспортной системе и повреждению ресурсов киберпространства. Типы ущерба, вызванного угрозами безопасности, различны, например, нарушения безопасности целостности базы данных, физическое уничтожение всего информационного объекта, порча данных, задержка в передаче данных и пр.

Угрозы в киберпространстве называют киберугрозами. Источником киберугроз могут быть субъективные, зависимые от человека, и объективные, независимые от человека, факторы. К субъективным относят: нежелательные действия «надежных» сотрудников, умышленные вредоносные действия сотрудников, хакерские атаки, случайные ошибки при вводе данных и т. д.

Финансовые потери, вызванные нарушениями безопасности, часто невозможно точно определить из-за того, что значительное количество инцидентов безопасности меньшего масштаба никогда не обнаруживается, часть инцидентов описывается как случайные ошибки, и все это является результатом тенденции минимизировать ответственность лица, ответственного за инцидент безопасности.

Угрозу безопасности можно определить как любое событие, которое может привести к нарушениям конфиденциальности, целостности и доступности информации или к любой другой форме повреждения ресурсов киберпространства. Последствия угроз безопасности различны, поэтому некоторые угрозы безопасности влияют на конфиденциальность или надежность хранимых данных, а некоторые угрозы влияют на функциональность и эффективность всего киберпространства. Угрозы безопасности можно наблюдать и классифицировать разными способами и по разным критериям. Существуют значительные различия в уровне безопасности в разных киберпространствах, например, транспортное, финансовое, коммуникационное, банковское и другие.

По данным [18] только 10,81% участников опроса. проводили систематический мониторинг и регистрацию угроз безопасности, которым подвергается их организация. Только 8,82% участников использовали одну из международных признанных классификаций угроз безопасности киберпространства.

В области безопасности киберпространства используются различные типы классификаций угроз безопасности. Причина, по которой необходимы классификации угроз, заключается в том, что ресурсы киберпространства должны быть не только защищены, но мы должны знать источники и угрозы, от которых мы их защищаем [18]. Проблема усложняется при комбинированном действии угроз безопасности. Типовым решением создание гибридной, временной классификации, которую используют в течение короткого периода времени.

Классификация NIST

Классификация NIST [19.] основана на критериях значимости угроз ИБ и различает следующие типы угроз безопасности:

1. Ошибки и упущения - это типичные угрозы безопасности, которые недооценивают. Угроза есть каждое событие, которое может привести к нарушению целостности киберпространства (аппаратных средств, программного обеспечения, программного обеспечения данных, жизненно важного оборудования). Наиболее распространенной причиной ошибок и упущений являются преднамеренные и непреднамеренные человеческие ошибки. Проблема с ошибками и упущениями заключается в том, что невозможно встроить механизмы приложения для всех возможных типов контроля ошибок (ввода данных).

Решение заключается в улучшении условий труда и образования сотрудников, а также осведомленности сотрудников об этом типе угроз безопасности. Этот тип угрозы может возникнуть во время процессов программирования и разработки киберпространства. Этот тип угрозы может возникнуть при некорректном определении прав пользователей, что может привести к значительным и серьезным последствиям для безопасности киберпространства. Исследование угроз безопасности киберпространства показало, что почти 65% всех угроз безопасности киберпространства являются ошибками и упущениями, как случайного, так и преднамеренного характера [19.]. Особенно опасным типом ошибок и упущений являются те, которые возникают во время процессов программирования, и их обычно называют «багами». Ошибки могут быть любыми: от безобидных ошибок до ошибок, которые приведут к сбоям в работе приложений, что в конечном итоге приведет к высоким расходам, необходимым для последующих процессов отладки.

2. Мошенничество и кража — это угроза кибербезопасности, которую можно реализовать путем простой автоматизации «традиционных» форм мошенничества и кражи. Например, злоумышленник может использовать компьютер для кражи небольших порций информации, предполагая, что небольшая транзакция не будет проверена как подозрительная. Но объектом этого типа угроз безопасности являются базы и банки данных. Компьютерное мошенничество и кражи могут совершаться как инсайдерами, так и аутсайдерами [18]. Инсайдеры — это лица, кото-

рые являются авторизованными пользователями киберпространства. Они используют киберпространство ежедневно для выполнения ежедневных рабочих заданий. Интересно, что большинство этих угроз исходят от инсайдеров. Этому есть несколько объяснений: они имеют (неограниченный) доступ к ресурсам киберпространства, хорошо знакомы с системными ресурсами и средствами управления безопасностью, знают возможности мошенничества (и кражи) и потенциальную ценность этих действий. Основываясь на этих фактах, Отдел компьютерных преступлений Министерства юстиции США утверждает, что «инсайдеры составляют «наиболее серьезную угрозу компьютерным системам» [20,21.]. Помимо возможности использования ресурсов киберпространства для совершения мошенничества или кражи, они сами могут стать объектом кражи. Анализ страхования Safeware показал, что в 2002 году из-за кражи был нанесен ущерб на сумму 882 млн долларов. [18, 20].

3. Потеря физической и инфраструктурной поддержки может быть реализована многими различными способами, например, потеря электроснабжения, потеря связи, наводнение, пожар, землетрясение. Это тип угрозы безопасности киберпространства, который не может находиться под полным контролем владельцев ресурсов киберпространства, и который потенциально может оказать значительное влияние на функциональность киберпространства [18].

4. Хакеры — относительно новая угроза безопасности киберпространства, которая становится все более важной с развитием Интернета и сетей связи. Термин «хакер» относится к человеку, который несанкционированным образом пытается получить доступ и (неправильно) использовать ресурсы киберпространства. Хотя масштаб ущерба, причиненного хакерами, гораздо менее значителен, чем ущерб, причиненный мошенничеством или кражей, их влияние может быть больше. Тот факт, что хакеры часто крадут пароли, делает их новым гибридным типом угрозы. По данным отдела компьютерных преступлений Министерства юстиции США, для этого есть три основные причины [21]:

а. Источниками этой угрозы обычно являются посторонние лица, и из-за этого у организации нет соответствующих механизмов, необходимых для санкционирования этих действий.

б. Основная цель хакерской атаки часто неизвестна. Это может быть кража данных, удаление или несанкционированное изменение данных, или просто хакер хочет указать на системные потоки и ошибки.

в. Хакерская атака делает людей уязвимыми - они атакуют без особой причины, и невозможно предвидеть, какой ущерб они нанесут.

5. Вредоносное ПО — это тип угрозы безопасности, который охватывает различные типы компьютерных вирусов, троянских коней, червей, логические бомбы и другие формы «нежелательного» программного обеспечения. Наиболее значимыми угрозами такого рода являются [21.]:

а. Компьютерные вирусы — части программного кода, которые индивидуально реплицируются и прикрепляются к исполняемым файлам. Когда пользователь запускает exe-файл, он автоматически запускает прикрепленный вирус. Компьютерные вирусы могут выполнять различные действия на компьютере пользователя — от безвредных (например, вывод сообщений на экран) до более серьезных (например, форматирование диска).

б. Троянские кони — это программы, которые автоматически устанавливаются на компьютер пользователя и выполняют различные нежелательные действия.

в. Черви — программы, которые при автоматическом запуске значительно снижают производительность систем.

6. Угрозы личной конфиденциальности — это новый тип угроз безопасности. Большие объемы персональных данных, которые хранятся в разных базах данных (например, государственных и частных учреждений, банков, компаний), могут попасть в публичный доступ. Существует реальная угроза того, что эти виды персональных данных могут быть использованы не по назначению многими различными способами (теория заговора «Большой брат») [18].

Классификация CSI/FBI

Классификация CSI/FBI Computer Crime and Security Survey 2004 [22, 23] в качестве критерия использует источник угрозы ISS. Согласно классификации CSI/FBI, существует два основных типа угроз безопасности киберпространства, основанных на положении источника угрозы безопасности на основе атакованной информационной системы. Источник угрозы может находиться как внутри, так и вне атакуемой системы.

Организации и их системы безопасности обычно сосредоточены на защите себя от угроз, которые исходят извне киберпространства. Угрозы, исходящие изнутри, часто не учитываются. Исследование CSI/FBI Computer Crime and Security Survey 2004 [22, 23] показало, что большинство инцидентов безопасности провоцируется изнутри организации, и эти угрозы обычно являются ошибками (почти 39% [22,23.] всех внутренних угроз безопасности являются ошибками сотрудников). Наиболее значимыми угрозами, которые исходят извне системы организации, являются различные типы вредоносных программ (компьютерные вирусы, троянские кони), спам, фишинг и атаки типа «отказ в обслуживании». Спам (или нежелательные электронные письма) становится более серьезной проблемой, поскольку он блокирует сетевой трафик и может использоваться в качестве транспортного средства для вредоносного программного обеспечения, мошенничества и т. д.

Почти две трети всех сообщений электронной почты, которыми обменивались в сентябре 2004 г., были спам-сообщениями [24]. Одной из последних форм компьютерного мошенничества является фишинг [25]. Это тип угрозы безопасности, который может осуществляться несколькими способами, и чаще всего жертва получает поддельное сообщение электронной почты, которое очень похоже на официальную переписку от банка или финансовых учреждений. В фишинговом сообщении отправитель объясняет, что по каким-то причинам жертва должна ввести и отправить свои персональные данные (включая номер банковского счета, PIN-код и т. д.) в прикрепленной веб-форме. Сообщение и форма не являются официальной перепиской и используются для кражи персональных данных (включая номера банковских счетов), а жертва становится жертвой «кражи личных данных» [26]. Увеличение зависимости от сетей связи привело к появлению новой формы угрозы безопасности — атак типа «отказ в обслуживании» или DoS. Идея DoS-атак заключается в блокировании системы компании (например, системы связи, интернет-магазина) большим количеством отправленных сообщений, запросов и т. д. Этот тип атаки может быть особенно опасен, если направлен на компанию, которая основана на электронной коммерции или зависит от услуг связи [27]. Помимо отдельных компаний, DoS-атаки часто направлены на крупные телекоммуникационные области, что может привести к значительному снижению функциональности телекоммуникационных услуг.

В заключение следует отметить роль моделирования при анализе и отражении угроз. При создании киберпространства важно использовать имитационное моделирования [28] как средство нахождения уязвимых мест и последствий воздействия угроз. Для обобщения опыта целесообразно применения метамоделирования [29,30].

Заключение

Одной из основных предпосылок успешного процесса управления безопасностью транспортного киберпространства является использование определенной классификации угроз киберпространства. Таким образом можно определить, от чего мы защищаем киберпространство, можно более эффективно использовать ограниченные информационные ресурсы, инвестируя в те защитные элементы управления, которые имеют дело с наиболее распространенными угрозами. Этим повышаем уровень безопасности киберпространства, устраняя наиболее распространенные угрозы безопасности, больше ресурсов будет доступно для использования в других областях безопасности транспортного киберпространства. Для этих целей мы должны использовать некоторую классификацию угроз безопасности киберпространства. Существующие классификации устаревают, особенно в контексте их совместимости и сопоставимости между собой. Для решения этой проблемы можно использовать модель CIA Triad [31]. Ее основными характеристиками являются то, что она является гибкой, динамичной и многомерной моделью, что дает ей определенное преимущество по сравнению с другими моделями защиты и классификации.

Список литературы

1. Цветков В.Я. Информационное поле и информационное пространство // Международный журнал прикладных и фундаментальных исследований. - 2016. - №1-3. – С.455-456.
2. Ознамец В.В. Информационное управляющее транспортное пространство // Наука и технологии железных дорог. 2020. Т.4.– 4(16). – С.43-50.
3. Ознамец В.В. Интервальное управление в радиорелейном информационном пространстве // Наука и технологии железных дорог. 2023. Т.8. №1 (29). – С.27-31.
4. Цветков В.Я., Ознамец В.В. Геодезические сети электронных меток // Науки о Земле. – 2018. - №4. – С.17-27.
5. Yibin Y. A. O., Shun Z., Jian K. Research progress and prospect of GNSS space environment science // Acta Geodaetica et Cartographica Sinica. – 2017. – Т. 46. – №. 10. – С. 1408.
6. Soares D. et al. Programming iot-spaces: A user-survey on home automation rules //International Conference on Computational Science. – Cham : Springer International Publishing, 2021. – С.512-525.
7. McCarthy G. Cyber-spaces //Routledge handbook of contemporary Myanmar. – Routledge, 2018. – С.92-105.

8. Лёвин Б.А., Цветков В.Я. Киберфизические системы в управлении транспортом // Мир транспорта. - 2018. Т. 16. № 2 (75). - С.138-145.
9. Нестеров Е. А., Цветков В. Я. Транспортная кибербезопасность // Мир транспорта. 2023. Т. 21. № 6 (109). С.103–109.
10. Максудова Л.Г., Цветков В.Я. Информационное моделирование как фундаментальный метод познания // Известия высших учебных заведений. Геодезия и аэрофотосъемка. - 2001. - №1. - С.102-106.
11. Кобелев Н. Б., Половников В. А., Девятков В. В. Имитационное моделирование. – Москва.: Курс, 2020.-352 с.
12. Матчин В.Т. Неопределенность в информационном поле // Перспективы науки и образования. - 2017. - №3(27). - с.7-12.
13. Цветков В.Я. Фактофиксирующие и интерпретирующие модели // Международный журнал прикладных и фундаментальных исследований. – 2016. - №9-3. – С.487.
14. Lippert K. J., Cloutier R. Cyberspace: a digital ecosystem //Systems. – 2021. – Т. 9. – №. 3. – С. 48.
15. Nosirovich A. N. et al. Cyberspace in the real world //Journal of Academic Research and Trends in Educational Sciences. – 2022. – Т. 1. – №. 10. – С.410-414.
16. Chen M. et al. Artificial intelligence and visual analytics in geographical space and cyberspace: Research opportunities and challenges //Earth-Science Reviews. – 2023. – Т. 241. – С. 104438.
17. Матчин В.Т. Интегрированное геоинформационное пространство // Славянский форум. -2018. – 3(21). - С.21-27.
18. Gerić S., Hutinski Ž. Information system security threats classifications //Journal of Information and organizational sciences. – 2007. – Т. 31. – №. 1. – С. 51-61.
19. Taherdoost H. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview //Electronics. – 2022. – Т. 11. – №. 14. – С. 2181.
20. Lehtinen R., Gangemi Sr G. T. Computer security basics: computer security. – « O'Reilly Media, Inc.», 2006.
21. Guttman B. An introduction to computer security: the NIST handbook. – US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1995. – Т. 800. – №. 12.
22. Richardson R., Director C. S. I. CSI computer crime and security survey //Computer security institute. – 2008. – Т. 1. – С. 1-30.
23. Computer Crime and Security Survey // /Computer security institute. – 2005. – Т. 1. – С. 1-24.
24. http://www.cccure.org/Documents/HISM. Дата просмотра 23.06.2024.
25. Kuraku D. S. et al. Exploring How User Behavior Shapes Cybersecurity Awareness in the Face of Phishing Attacks //International Journal of Computer Trends and Technology. – 2023.
26. Sylvester F. L. Mobile device users' susceptibility to phishing attacks //arXiv preprint arXiv:2203.01823. – 2022.
27. Jha A. K., Rajan P. Software protection and software piracy //The Journal of World Intellectual Property. – 2022. – Т. 25. – №. 2. – С. 251-270.
28. Law A. M. How to build valid and credible simulation models //2022 Winter Simulation Conference (WSC). – IEEE, 2022. – С. 1283-1295.
29. Цветков В.Я., Булгаков С.В., Титов Е.К., Рогов И.Е. Метамоделирование в геоинформатике // Информация и космос. 2020. - №1. –С .112-119.
30. Saleh M. et al. A Metamodeling Approach for IoT Forensic Investigation //Electronics. – 2023. – Т. 12. – №. 3. – С. 524.
31. Yampolskiy M., Gatlin J., Yung M. Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad //Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security. – 2021. – С. 3-9.