УДК 004.056+004.6

ИССЛЕДОВАНИЕ МЕТОДОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦЕЛЯХ ЗАЩИТЫ ДАННЫХ

УРСУНБОЕВА Д. Т., ЮСУПБЕКОВА Б. Н.

Евразийский национальный университет имени Л. Н. Гумилёва
(г. Астана, Казахстан)

E-mail: Dinara.tursynbaeva@list.ru

Аннотация. Быстрое развитие больших данных привело к появлению новых проблем в области сетевой информационной безопасности и защиты конфиденциальности. В этом документе будут изучены конкретные технологии сетевой информационной безопасности и защиты конфиденциальности в этом контексте. В первой части этой статьи сначала обсуждается значение и характеристики больших данных, а затем выдвигаются проблемы информационной безопасности и защиты частной жизни в эпоху больших данных. Последняя часть глубоко изучает, как решать решения, соответствующие этим проблемам.

Abstract. The rapid development of big data has brought more problems in network information security and privacy protection. This paper will study the specific network information security and privacy protection technologies in this context. The first part of this paper firstly discusses the connotation and characteristics of big data, and then puts forward the information security and privacy protection problems in the era of big data. The last part deeply studies how to solve the solutions corresponding to these problems.

Введение

Современное общество называется информационным. Широкое развитие средств вычислительной техники и связи позволило собирать, хранить, обрабатывать и передавать информацию в таких объемах и с такой оперативностью, которые были немыслимы раньше. С непрерывным развитием компьютерных технологий и сетевых технологий концепция больших данных больше не незнакома людям, а с резким ростом популярности интеллектуальных устройств интеграция технологий больших данных и других отраслей стала неизбежной. Большие данные сами по себе обладают множеством типов данных, высокой скоростью обработки данных и другими характеристиками, которые смогут эффективно способствовать развитию этих отраслей [1] , но в то же время, поскольку концепция больших данных и связанные с ней технологии находятся в периоде быстрого развития, широкое применение таких технологий будет неизбежно приводят к большому количеству проблем информационной безопасности. В то же время большие данные будут собирать и анализировать различные типы данных, генерируемых пользователями во время использования Интернета. Если не будет эффективной защиты конфиденциальности, произойдет утечка личной информации пользователя. Очень вероятно, что информация просочится, и это окажет серьезное влияние на пользователей. Чтобы усилить положительное влияние, которое большие данные могут оказать на социальное развитие страны на основе оригинала, влияние больших данных на сетевую информационную безопасность и защиту конфиденциальности сведено к минимуму, и используется метод защиты сетевой информационной безопасности, соответствующий большим данным. Исследования очень необходимы.

Основная часть

Активное развитие информационных технологий обуславливает актуальность изучения проблем информационной безопасности: угроз для информационных ресурсов, различных средств и мер защиты, барьеров для проникновения, а также уязвимостей в системах защиты информации. Под информационной безопасностью в более общем виде следует понимать совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются. Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Информационная безопасность включает:

- состояние защищенности информационного пространства, обеспечивающее его формирование и

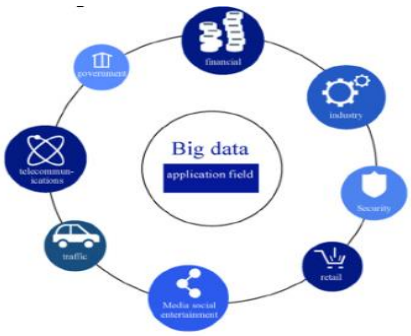
развитие в интересах граждан, организаций и государства;

-состояние инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании;

- состояние информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность;

-экономическую составляющую (структуры управления в экономической сфере, включая системы сбора, накопления и обработки информации в интересах управления производственными структурами, системы общеэкономического анализа и прогнозирования хозяйственного развития, системы управления и координации в промышленности и на транспорте, системы управления энергосистем, централизованного снабжения, системы принятия решения и координации действий в чрезвычайных ситуациях, информационные и телекоммуникационные системы);

- финансовую составляющую (информационные сети и базы данных банков и банковских объединений, системы финансового обмена и финансовых расчетов).



Обеспечение информационной безопасности должно нанаться с выявления субъектов отношений, связанных с использованием информационных систем. Спектр их интересов может быть разделен на следующие основные категории: доступность (возможность за приемлемое время получить требуемую информационную услугу), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения), конфиденциальность (защита от несанкционированного ознакомления).

Заключение

Таким образом, на основе простого обсуждения основных вопросов сетевой информационной безопасности и защиты конфиденциальности пользователей в эпоху больших данных в этой статье в основном применяется процесс обработки больших данных с помощью анонимной информации, технологии управления доступом к ролям и технологии управления доступом к рискам. Метод защиты конфиденциальности и безопасности пользователей был тщательно изучен. В процессе последующей разработки, чтобы большие данные могли лучше играть свою роль, соответствующие исследовательские подразделения должны уметь придавать значение вопросам сетевой информационной безопасности в контексте больших данных, а государственные ведомства должны оказывать помощь в построении специальные законы и правила. Отдельные предприятия или организации могут использовать большие данные для разумной работы и принципиально избегать нарушений конфиденциальности пользователей.

Список использованных источников

1. [1] Гао Юй, Ли Ли. Новые возможности и требования информационной безопасности в эпоху больших данных [J].
2. Электронные технологии и программная инженерия, 2018 (24).
3. [2] Чжан Цзянь, Ян Цзянь. Информационная безопасность и защита компьютерных сетей в эпоху больших данных [J].
4. Электронные технологии и программная инженерия, 2018 (24).
5. [3] Чжан Ган. Информационная безопасность компьютерных сетей и меры противодействия ее защите [J].
6. Электронные технологии и программная инженерия, 2018 (24).
7. [4] Ли Сяося. Меры предосторожности при компьютерной информационной безопасности, основанные на эпохе больших данных[J].
8. Электронные технологии и разработка программного обеспечения, 2018 (24).
9. [5] Лян Чживэнь. Построение системы обработки компьютерной информационной безопасности в режиме облачных вычислений[J].
10. Электронные технологии и разработка программного обеспечения, 2018 (24).