УДК 004.056.57

ВЫЗОВЫ И РЕШЕНИЯ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭПОХУ БОЛЬШИХ ДАННЫХ

ЗОТОВ Д.В.[1]

Научный руководитель: д.т.н., проф. Найдыш А.В.[1]

[1]*Федеральное государственное бюджетное образовательное учреждение высшего образования (ФГБОУ ВО) «Мелитопольский государственный университет», г.Мелитополь, e-mail: naydysh2@gmail.com*

Аннотация: Процветание больших данных приносит не только удобство повседневной жизни людей и больше возможностей для предприятий, но и новые проблемы с информационной безопасностью. В этой статье исследуются новые типы и особенности проблем информационной безопасности в эпоху больших данных, а также предлагаются решения вышеупомянутых проблем: создание платформы управления безопасностью больших данных, создание системы информационной безопасности и внедрение соответствующие законы и правила.

Ключевые слова: информационная безопасность; большие данные; конфиденциальность данных; информационные технологии.

CHALLENGES AND SOLUTIONS TO INFORMATION SECURITY PROBLEMS IN THE AGE OF BIG DATA

ZOTOV D.V.[1]

Science director: Doctor of Technical Sciences, Professor Naydysh A.V.[1]

[1]*Federal State Budgetary Educational Institution Higher Education (FSBEI HE) "Melitopol State University", Melitopol, e-mail: naydysh2@gmail.com*

Abstract: The prosperity of big data not only brings convenience to people's daily lives and more opportunities for businesses, but also new information security challenges. This article explores the new types and features of information security problems in the era of big data, and proposes solutions to the above-mentioned problems: establishing a big data security management platform, establishing an information security system, and implementing relevant laws and regulations.

Keywords: Information Security; big data; data privacy; information Technology.

Введение. Быстрый рост больших данных не только приносит удобство в повседневную жизнь людей, но и открывает большие возможности для предприятий. Например, в условиях бума больших данных Microsoft создает свою собственную интеллектуальную систему управления данными, основанную на больших данных, и производит своего рода программное обеспечение, управляемое данными, главным образом для экономии энергии и повышения эффективности, которое может сэкономить 40% энергии для этого приложения. Однако большие данные также создают проблемы, особенно для информационной безопасности из-за их особых характеристик. Прежде всего, большие данные могут увеличить риск утечки информации из-за их большого объема и скорости. Призма является ярким примером, показывающим, что один человек или один компьютер может вызвать серьезные последствия в результате анализа больших данных [1]. Между

тем быстрое развитие интеллектуальных терминалов сопровождается растущим риском утечки информации. Это касается конфиденциальности, прогнозирования поведения людей при использовании этих терминалов, иногда даже угрожает безопасности страны. Кроме того, поскольку данные социальных контактов становятся открытыми и доступны хакерам, это делает большие данные легкой мишенью для атаки, поскольку все эти данные коррелируют друг с другом, если хакеры используют одну из этих коррелирующих данных в качестве носителя. вируса, который невозможно обнаружить вовремя, ущерб будет огромен. Кроме того, из-за особенности разнообразия больших данных не все данные являются структурированными данными, а неструктурированные данные либо не имеют заранее определенной модели данных, либо не организованы заранее определенным образом, в то время как традиционные базы данных и обработка данных не могут удовлетворить требования к хранению неструктурированных данных, которые обычно содержат много текста, но также могут содержать такие данные, как даты, числа и факты [2]. В связи с чем данная статья посвящена решениям этих проблем в эпоху больших данных.

Цель исследования — оценить актуальное состояние развития технологий информационной безопасности баз больших данных.

Материал и методы исследования

В ходе исследования, были проанализированы научные работы отечественных и зарубежных ученых, был проведен анализ истории становления электронной коммерции и проблемы, связанные с ее внедрением в бизнес процессы на каждом этапе развития.

Результаты исследования и их обсуждение

Данные киберпространства охватывают широкий спектр, например, датчики, социальные сети и электронная почта. Сбор данных неизбежно увеличивает риск утечки информации. Поставщик больших данных имеет огромную информацию, но сохранение этих собираемых данных, которые включают в себя многочисленные записи правительственной информации, деловых данных и информации клиентов, увеличивает риск утечки информации, и, если этими данными будут злоупотреблять, это будет угрожать личному, фирменному и государственному безопасность. При этом не существует явного ограничения права собственности и права на некоторые конфиденциальные данные, что все равно создает риск утечки информации. И именно поэтому анализ, основанный на больших данных, включающий утечку информации, на самом деле является актуальной проблемой информационной безопасности, которая угрожает личной конфиденциальности и национальной безопасности в эпоху больших данных [3]. Проводя обобщение, можно выделить два направления главных угроз, связанных с информационной безопасностью:

1. Угрозы личной жизни – риск утечки информации приведет к угрозе неприкосновенности частной жизни

2. Угрозы национальной безопасности - быстрое развитие информационных технологий облегчает утечку информации в Интернете, различных интеллектуальных терминалах и портативных устройствах хранения данных, причем утечка может оказать большое влияние на безопасность отдельных лиц, предприятий и государства.

Причин появления подобных опасностей существует множество, проведя анализ литературных источников, нами было выделено три основных группы:

1. Большие данные становятся очевидной целью кибератак - огромный объем интегрированных данных позволяет хакеру, успешно атакующему базу данных, получать больше данных и снижать стоимость атаки.

2. Большие данные бросают вызов существующим мерам экономии и безопасности - большие данные создают новые проблемы безопасности для мер экономии из-за их разнообразия.

3. Большие данные используются в качестве меры нападения - хакеры используют большие данные для запуска эксплойта «bonnet», который может контролировать миллионы компьютеров и запускать атаки одновременно, а традиционная атака не имеет этой функции или порядка величины.

Для развития конвергенции сетей и Интернета социальная информатизация проникла во все области, что привело к тому, что вопросы информационной безопасности стали более важными, чем когда-либо прежде. Столкнувшись с угрозами и проблемами информационной безопасности в эпоху больших данных, правительство и предприятия вынуждены искать решения, включая создание платформы управления безопасностью больших данных, ускорить создание системы информационной безопасности и повысить осведомленность людей, чтобы гарантировать информационная безопасность.

Проведя обширный анализ международного опыта противодействия угрозам информационной безопасности, нами был сформулирован план обобщенный план мероприятий по обеспечению информационной безопасности больших данных:

1. Создать платформу управления безопасностью больших данных (платформа управления безопасностью больших данных разделена на пять уровней: уровень хранения данных, уровень обработки данных, интерфейс, уровень приложений данных и уровень управления данными).

2. Ускорить создание системы технологий информационной безопасности (платформа ускорения разделена на пять подзадач: защита разных доменов, иерархическая защита, защита таймшера)

Конфиденциальность данных является очень деликатным вопросом в эпоху больших данных, и поскольку общественность все больше осознает риски киберпреступности и утечки персональных данных, законодательство о защите данных становится задачей, которая не терпит отлагательств.

Поэтому, во-первых, это фундаментальная мера по реализации соответствующих законов и правил для усиления защиты информационных сетей и ключевой информационной системы в целях обеспечения безопасности сетевых данных. В частности, законодательство о правах на ресурсы данных должно быть включено в повестку дня законотворчества как можно скорее.

Во-вторых, важно продвигать законодательство о защите личной информации в Интернете, определять объем сбора и применения личной информации, уточнять права, обязанности и обязанности соответствующих субъектов, а также ужесточать наказание за неправомерное поведение, такое как вторжение в частную жизнь.

И последнее, но не менее важное: поскольку осведомленность людей о безопасности играет важную роль в информационной безопасности, осведомленность о личной информационной безопасности необходимо повышать под руководством [4].

Таким образом, активизация усилий по разработке защищенных систем, удовлетворение поставленных условий, достижение качественной работы всех уровней безопасности и активизация работы по надзору за администрацией и обучению абонентов, особенно подросткового возраста, являются практическими мерами по повышению осведомленности об информационной безопасности и регулированию поведения в сети [5]. Только тогда, когда осведомленность об информационной безопасности будет повышена, можно будет добиться улучшения информационной безопасности.

Выводы. Большие данные возглавляют информационную революцию с развитием информационных технологий, и они были приняты в качестве национальной стратегии в Китае. Тем не менее, эта стратегия может иметь проблемы, связанные с тем, что люди по-прежнему не смогут воспользоваться преимуществами больших данных, если безопасность информации не может быть гарантирована. Таким образом, информационная безопасность имеет большое значение в эпоху больших данных, и защита информационной безопасности требует создания платформы и системы управления безопасностью больших данных, внедрения соответствующих законов и правил, а также усилий граждан Интернета по использованию различных интеллектуальных терминалов. и соответствующих законодательных органов и сетевых операторов для обеспечения информационной безопасности в эпоху больших данных.

Список литературы

1. Букреев Д. А. Прогнозирование фондового рынка с помощью нейросетей//Информационные технологии в образовании и науке: сб. науч. раб. – 2018. – №. 10. – С. 36-43.

2. Bukreiev D. et al. Features of the development of an automated educational and control complex for checking the quality of students. – CEUR Workshop Proceedings, 2021.

3. Machanavajjhala A., Reiter J. P. Big privacy: protecting confidentiality in big data //XRDS: Crossroads, The ACM Magazine for Students. – 2012. – Т. 19. – №. 1. – С. 20-23.

4. Gerber M., von Solms R., Overbeek P. Formalizing information security requirements //Information Management & Computer Security. – 2001. – Т. 9. – №. 1. – С. 32-37.

5. Hawkins S., Yen D. C., Chou D. C. Awareness and challenges of Internet security //Information Management & Computer Security. – 2000. – Т. 8. – №. 3. – С. 131-143.