Гаджиев Г.К. Защита персональных данных и приватности в эпоху цифровизации: вызовы и решения // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 10(48) с. 38–41

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРИВАТНОСТИ В ЭПОХУ ЦИФРОВИЗАЦИИ: ВЫЗОВЫ И РЕШЕНИЯ

Гаджиев Г.К.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: gugac134@gmail.com

В условиях стремительного развития технологий и цифровизации защита персональных данных и приватности становится одной из ключевых задач современного общества. В статье рассматриваются основные вызовы, связанные с обеспечением кибербезопасности, включая рост объема персональных данных, угрозы кибератак, сбор данных без согласия и недостаточную защиту в организациях. Анализируются подходы к решению этих проблем, такие как внедрение современных технологий безопасности, соблюдение законодательства, обучение сотрудников и развитие международного сотрудничества. Особое внимание уделяется роли граждан в защите своих данных и созданию культуры безопасности на всех уровнях общества.

Ключевые слова: Цифровизация, персональные данные, кибербезопасность, приватность, утечка данных, кибератаки, защита данных, шифрование, законодательство о защите данных.

PROTECTION OF PERSONAL DATA AND PRIVACY IN THE ERA OF DIGITALIZATION: CHALLENGES AND SOLUTIONS

Gadzhiev G.K.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: gugac134@gmail.com

With the rapid development of technology and digitalization, the protection of personal data and privacy is becoming one of the key tasks of modern society. The article examines the main challenges associated with ensuring cybersecurity, including the growth of personal data, the threat of cyber attacks, the collection of data without consent and insufficient protection in organizations. Approaches to solving these problems are analyzed, such as the introduction of modern security technologies, compliance with legislation, employee training and the development of international cooperation. Particular attention is paid to the role of citizens in protecting their data and creating a culture of security at all levels of society.

Keywords: Digitalization, personal data, cybersecurity, privacy, data leakage, cyber attacks, data protection, encryption, data protection legislation.

Введение

В современном цифровом мире, где технологический прогресс стремительно продвигает нас к цифровой трансформации в различных сферах жизни, защита персональных данных и приватности становится все более актуальной и критической задачей. Организации и частные лица сталкиваются с растущими угрозами безопасности данных и нарушениями приватности, которые могут привести к серьезным последствиям. В данной статье рассматриваются вызовы и решения в области защиты персональных данных и приватности в эпоху цифровизации.

Рост объема персональных данных.

Одним из ключевых вызовов в обеспечении защиты данных является взрывной рост объема персональных данных, создаваемых и хранимых в цифровой форме. С развитием интернета, цифровых платформ, социальных сетей, мобильных приложений и интернета вещей, каждый пользователь генерирует большое количество данных о своей жизни, привычках, предпочтениях и финансовых операциях. Это создает огромный потенциал для злоумышленников получить доступ к этим данным и злоупотребить ими [1].

С ростом объема цифровых данных увеличивается и уровень киберугроз. Хакерские атаки, вирусы, фишинг, атаки мальваре и другие формы киберпреступности становятся все более изощренными и распространенными. Организации и частные лица подвергаются риску утечек данных, финансовых потерь, утраты репутации и других негативных последствий.

Многие компании собирают и используют персональные данные пользователей без их явного согласия или даже осведомленности. Это может включать сбор данных через онлайн-трекинг, аналитику поведения пользователей, использование куки-файлов и другие методы. Подобные практики могут нарушать приватность и индивидуальные права пользователей [2].

Многие организации не обеспечивают должного уровня защиты для хранящихся у них данных. Уязвимости в сетевых системах, слабые пароли, недостаточное шифрование данных - все это делает персональную информацию уязвимой для кибератак и утечек. Недостаточная защита данных может привести к серьезным нарушениям безопасности и утечкам конфиденциальной информации.

Современные данные могут быть переданы через границы и храниться на серверах в различных странах. Это создает сложности в обеспечении соблюдения законодательства о защите данных, так как различные страны имеют разные правила и требования к хранению и использованию персональной информации. Это также означает, что данные могут подвергаться риску перехвата и злоупотребления на протяжении всего пути их передачи через интернет [3].

Решения для обеспечения защиты персональных данных:

- Внедрение современных технологий безопасности: Организации должны активно использовать современные технологии для защиты данных, такие как шифрование, многофакторная аутентификация, системы мониторинга безопасности и идентификации аномального поведения [4].
- Соблюдение законодательства: Компании должны строго соблюдать законы и нормативные акты о защите данных, включая Общий регламент по защите данных (GDPR) в Европейском союзе и другие региональные законы о защите данных.
- Обучение персонала: Важно обучать сотрудников компаний и организаций принципам безопасности данных и правильным процедурам обращения с конфиденциальной информацией, чтобы снизить риск утечек данных из-за человеческого фактора.
- Разработка прозрачной политики конфиденциальности: Организации должны разработать и публично опубликовать политику конфиденциальности, в которой четко определены цели сбора данных, способы их использования и права пользователей [5].
- Развитие международного сотрудничества: Государства и международные организации должны сотрудничать в области разработки стандартов безопасности данных и обмена информацией о киберугрозах для обеспечения более эффективной защиты персональных данных.
- Активная роль граждан и потребителей: Граждане и потребители должны быть проактивны в защите своих персональных данных. Это включает осознанное использование интернет-сервисов, регулярное обновление паролей, отказ от сомнительных приложений и веб-сайтов, а также внимательное отношение к запросам на предоставление персональной информации.

- Развитие инновационных методов защиты данных: Непрерывное исследование и разработка новых методов и технологий для защиты данных является важным аспектом обеспечения кибербезопасности в эпоху цифровизации. Это включает в себя использование искусственного интеллекта, машинного обучения, блокчейна и других инновационных подходов.
- Создание культуры безопасности данных: Не менее важно создать культуру безопасности данных как на уровне организаций, так и в обществе в целом. Это включает в себя проведение обучающих мероприятий, освещение вопросов кибербезопасности в СМИ, мотивацию сотрудников и граждан к ответственному обращению с данными.

Заключение

Защита персональных данных и приватности является неотъемлемой частью кибербезопасности в эпоху цифровизации. С ростом объема данных и угроз кибербезопасности становится все более важно разрабатывать эффективные стратегии и методы защиты данных, соблюдать законодательство и создавать культуру безопасности как на уровне организаций, так и в обществе в целом. Только совместные усилия всех заинтересованных сторон позволят обеспечить надежную защиту персональных данных и приватности в эпоху цифровой трансформации.

Список литературы

1. Бирих Э. В. и др. Исследование вопросов повышения уровня защищенности органов исполнительной власти //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – [С. 107-110].
2. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – [С. 72-76].
3. Герлинг Е. Ю. Исследование эффективности методов обнаружения стегосистем, использующих широкополосное вложение //Телекоммуникации. – 2014. – №. 1. – [С. 06-12].
4. Ковцур М. М. и др. Исследование способов удаленного перехвата трафика в корпоративных сетях //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия. – 2021. – Т. 1. – [С. 68-75].
5. Герлинг Е. Ю. и др. Анализ и выявление психологических аспектов внутренних угроз на объектах связи //Известия высших учебных заведений. Технология легкой промышленности. – 2018. – Т. 39. – №. 1. – [С. 13-16].

References

1. Birikh E. V. et al. Research on issues of increasing the level of protection of executive authorities //Actual problems of infotelecommunications in science and education (APINO 2018). – 2018. – [pp. 107-110].
2. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – №. 4. – [Pp. 72-76].
3. Gerling E. Y. Investigation of the effectiveness of methods for detecting stegosystems using broadband embedding //Telecommunications. – 2014. – №. 1. – [Pp. 06-12].

4. Kovtsur M. M. et al. Research of methods of remote interception of traffic in corporate networks //Bulletin of the St. Petersburg State University of Technology and Design. Series. – 2021. – Vol. 1. – [pp. 68-75].
5. Gerling E. Yu. et al. Analysis and identification of psychological aspects of internal threats at communication facilities //News of higher educational institutions. Light industry technology. - 2018. – vol. 39. – No. 1. – [pp. 13-16].