УДК 004.056

**ТРЕНДЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Курманбакеев В.А.**

*ФГБОУ ВО "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича", Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков д.22, корп.1), e-mail: slavan787@gmail.com*

**Информационная безопасность становится все более актуальной в нашей цифровой эпохе, когда все больше информации хранится и передается через сети. С каждым годом уровень угрозы для информационной безопасности растет, и в настоящее время существует несколько трендов и перспектив, которые влияют на развитие этой области.**

Ключевые слова: Информационная безопасность.

**TRENDS AND PROSPECTS OF INFORMATION SECURITY DEVELOPMENT**

**Kurmanbakeev V.A.**

*Bonch-Bruevich St. Petersburg State University of Telecommunications*, St. Petersburg, *Russia (193232, St. Petersburg*, *22 Bolshevikov Ave., bldg. 1),* *e-mail: slavan787@gmail.com*

**Information security is becoming more and more relevant in our digital age, when more and more information is stored and transmitted through networks. Every year the threat level for information security is growing, and currently there are several trends and prospects that affect the development of this area.**

Keywords: Information security.

Одним из основных трендов является увеличение количества кибератак на корпоративные сети и государственные учреждения. Стремительное развитие технологий и внедрение новых приложений и сервисов создают новые уязвимости, которые могут быть использованы злоумышленниками. Вместе с тем, многие организации не обладают достаточной квалификацией и опытом в области информационной безопасности, что делает их еще более уязвимыми.

Другим трендом является увеличение объема данных, которые собираются и обрабатываются организациями. Это может привести к возникновению проблем с конфиденциальностью и утечкой данных, если не принимать соответствующие меры для защиты информации. Поэтому важно уделять больше внимания не только защите сетей и устройств, но и защите данных, которые они обрабатывают.

Одной из перспектив развития информационной безопасности является использование искусственного интеллекта и машинного обучения. Это может помочь автоматизировать процессы по обнаружению угроз и анализу данных, что упростит задачу защиты информации. Также возможно использование блокчейн технологии для защиты данных, что обеспечит их целостность и надежность.

Вместе с тем, развитие информационной безопасности может быть затруднено недостатком высококвалифицированных специалистов. В настоящее время существует дефицит квалифицированных специалистов в этой области, что может привести к тому, что организации не будут иметь достаточных ресурсов для защиты своей информации.

Таким образом, тренды и перспективы развития информационной безопасности указывают на необходимость усиления мер по защите информации и обучению специалистов в этой области. Необходимо развивать новые технологии и подходы к защите данных, а также повышать осведомленность среди пользователей и работников организаций о методах и мероприятиях по защите информации.

Также важно учитывать международные стандарты и регуляторные требования по защите данных, такие как GDPR в Европейском союзе или HIPAA в США.

Эти стандарты определяют правила сбора, хранения и обработки данных, а также наказания за их нарушение.

С учетом этих факторов можно сделать вывод, что информационная безопасность является ключевой проблемой для организаций и государственных учреждений. Необходимо принимать все возможные меры для защиты информации и обучения специалистов, чтобы справиться с растущими угрозами и сохранить доверие пользователей и клиентов. Только так можно обеспечить стабильный и безопасный развитие цифровой экономики и общества в целом.

Еще одним важным аспектом развития информационной безопасности является международное сотрудничество и обмен информацией между государствами. Многие кибератаки имеют международный характер, и их успешная предотвращение требует координации усилий различных стран. Для этого необходимо создание международных платформ и механизмов сотрудничества, которые позволят эффективно обмениваться информацией о киберугрозах и совместно принимать меры по их предотвращению.

Также необходимо учитывать социальные и этические аспекты информационной безопасности. Существуют опасности связанные с использованием личной информации пользователей, такие как дискриминация, нарушение приватности и даже кража личности. Поэтому необходимо уделять больше внимания правам и свободам пользователей, а также развивать механизмы контроля за использованием персональных данных.

В целом, развитие информационной безопасности является сложным и многогранным процессом, который требует участия различных заинтересованных сторон. Необходимо учитывать текущие тренды и перспективы в этой области, а также принимать соответствующие меры для защиты данных и повышения осведомленности пользователей и работников. Только так можно создать безопасную и надежную среду для хранения и передачи информации в цифровой эпохе.

Еще одним перспективным направлением в развитии информационной безопасности является использование искусственного интеллекта и машинного обучения для автоматизации процессов защиты данных. Инструменты и алгоритмы искусственного интеллекта могут помочь в обнаружении и анализе киберугроз, а также в автоматической защите от них. Машинное обучение может помочь в создании адаптивных систем защиты, которые могут быстро реагировать на новые угрозы и атаки.

Также стоит упомянуть о развитии квантовых технологий, которые могут изменить парадигму информационной безопасности. Квантовые компьютеры могут быстро взламывать существующие системы шифрования, поэтому необходимо разрабатывать новые квантово-устойчивые методы защиты данных.

Наконец, важно отметить, что информационная безопасность должна рассматриваться как неотъемлемая часть общественной безопасности и защиты прав и свобод граждан. Существующие угрозы в области информационной безопасности могут привести к серьезным последствиям, включая угрозы жизни и здоровью людей. Поэтому необходимо уделять больше внимания этой проблеме и принимать меры для ее решения.

В заключение, можно сказать, что информационная безопасность является важным и перспективным направлением развития в цифровой эпохе. Существующие тренды и перспективы в этой области показывают, что необходимо принимать все возможные меры для защиты данных и повышения осведомленности пользователей и работников о киберугрозах. Только так можно создать безопасную и стабильную среду для развития цифровой экономики и общества в целом.

Еще одним важным аспектом, который следует упомянуть при рассмотрении трендов и перспектив развития информационной безопасности, является роль человеческого фактора в кибербезопасности. Несмотря на все технологические инновации и новые методы защиты данных, человеческий фактор остается одним из самых слабых звеньев в цепи безопасности.

Все чаще хакеры используют социальную инженерию и фишинговые атаки, чтобы получить доступ к конфиденциальной информации. Поэтому необходимо уделять больше внимания обучению и повышению культуры кибербезопасности среди пользователей и работников. Компании и государственные организации должны проводить регулярные тренинги и обучения, чтобы повысить осведомленность своих сотрудников о возможных угрозах и обучить их правильному поведению в сети.

Кроме того, важно улучшать законодательную базу в области кибербезопасности и ужесточать ответственность за нарушение правил и мер безопасности. Только так можно создать эффективную систему защиты данных и обеспечить безопасность в интернете.

В целом, развитие информационной безопасности в наши дни является сложной и многогранной задачей. Необходимо учитывать множество факторов, включая технологические инновации, роль человеческого фактора, социально-экономические тенденции и геополитические риски. Однако, при правильном подходе и принятии необходимых мер, можно создать безопасную и устойчивую среду для развития цифрового мира.

**Список литературы**

1. Петров А. Информационная безопасность: теория и практика. - М.: Издательство Юрайт, 2020.
2. Лукин А. М., Старкова Н. В. Информационная безопасность: угрозы, защита, нормативно-правовое обеспечение. - М.: КНОРУС, 2021.
3. Поляков А. Б., Булыгин Е. В. Кибербезопасность: введение в проблематику. - СПб.: Питер, 2020.
4. Малышев В. Н. Информационная безопасность и защита информации: учебник для студентов высших учебных заведений. - М.: Юрайт, 2021.
5. Безопасность в информационных системах и технологиях. Учебное пособие / Под ред. Ю. А. Шумилина. - М.: Издательство МГТУ им. Н.Э. Баумана, 2020.
6. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
7. Гельфанд А. М. и др. Интернет вещей (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
8. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.

**References**

1. Petrov A. Information security: theory and practice. - M.: Yurait Publishing House, 2020..
2. Lukin A. M., Starkova N. V. Information security: threats, protection, regulatory and legal support. - M.: KNORUS, 2021
3. Polyakov A. B., Bulygin E. V. Cybersecurity: introduction to the problematics. - St. Petersburg: Peter, 2020.
4. Malyshev V. N. Information security and information protection: a textbook for students of higher educational institutions. - M.: Yurayt, 2021.
5. Security in information systems and technologies. Textbook / Ed. by Y. A. Shumilin. - Moscow: Bauman MSTU Publishing House, 2020.
6. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – . pp.1-6.
7. Gelfand A. M. et al. Internet of Things (IoT): threats to security and privacy // Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
8. Gelfand A. M. et al Study of a distributed security mechanism for Internet of Things devices with limited resources // Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.