

СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Иброхимова Нафосатхон Пахлавон кизи

Студентка Ферганского филиала Ташкентского университета информационных технологий

Аннотация: В условиях стремительно развивающихся информационных технологий обеспечение информационной безопасности стало важной задачей для современных обществ. В этой статье рассматривается концепция информационной безопасности, выявляются различные виды угроз и описываются нормативно-правовые базы, разработанные для защиты информации. Подчеркивается важность защиты данных от несанкционированного доступа, промышленного шпионажа и других киберпреступлений.

Ключевые слова: информационная безопасность, угрозы информационной безопасности, защита информации, нормативно-правовые документы, национальная безопасность, конфиденциальная информация, компьютерная безопасность, целостность данных, политика безопасности, обеспечение.

MODERN METHODS AND MEANS OF ENSURING INFORMATION SECURITY

Ibrokhimova Nafosathon Pahlavon kizi

Student of the Fergana branch of the Tashkent University of Information Technologies

Abstract: In the context of rapidly developing information technologies, ensuring information security has become an important task for modern societies. This article examines the concept of information security, identifies various types of threats and describes the legal frameworks developed to protect information. The importance of protecting data from unauthorized access, industrial espionage and other cybercrimes is emphasized.

Keywords: information security, information security threats, information protection, legal documents, national security, confidential information, computer security, data integrity, security policy, ensuring.

Защита информации: Информационная безопасность и ее современная концепция. Угрозы информационной безопасности и их виды. Нормативно-правовые документы по информационной безопасности и защите данных. Международные стандарты в области защиты информации. В любом развитом обществе значение информации постоянно растет. Исторически данные, имеющие военно-стратегическое значение, всегда были строго конфиденциальны и защищены. В настоящее время информация, связанная с производственными технологиями и продажей продуктов, становится товаром, востребованным как на внутреннем, так и на внешнем рынках. Информационные технологии постоянно развиваются в областях автоматизации и защиты информации. Развитие современных информационных технологий сопровождается негативными явлениями, такими как промышленный шпионаж, компьютерные преступления и несанкционированный доступ к конфиденциальным данным, их изменение или утрата. Поэтому защита информации является значимой государственной задачей в любой стране.

В Узбекистане необходимость защиты информации выражается в создании государственной системы защиты информации и разработке правовой базы для обеспечения информационной безопасности. Были приняты и внедрены такие законы, как «Об информатизации», «О защите государственных тайн», «О правовой защите программного обеспечения и баз данных» и несколько правительственных постановлений. Меры по защите информации должны предотвратить ущерб от добровольной утраты (кражи, повреждения, подделки) информации. Эти меры должны быть организованы на основе существующих законов и норм по информационной безопасности и интересов пользователей информации. Для обеспечения высокого уровня защиты информации необходимо постоянно решать сложные научные и технические задачи и совершенствовать меры защиты.

Закон «О принципах и гарантиях свободы информации» Республики Узбекистан от 12 декабря 2002 года № 439-II дает следующие определения информации и ее видов:

Информация: Данные об отдельных лицах, объектах, фактах, событиях, явлениях и процессах независимо от их источников и форм представления. **Защита информации:** Меры по предотвращению угроз информационной безопасности и ликвидации их последствий. **Публичная информация:** Документированная информация, предназначенная для неограниченной аудитории в печатной, аудио, аудиовизуальной и других формах. **Документированная информация:** Информация, зафиксированная на материальном носителе с идентификационными признаками. **Конфиденциальная информация:** Документированная информация, использование которой ограничено законом.

Эти определения также выражены в постановлении Кабинета Министров Республики Узбекистан «О мерах по реализации Указа Президента Республики Узбекистан "О дополнительных мерах по защите национальных информационных ресурсов"» от 7 ноября 2011 года № 296. Конфиденциальная информация означает документированную информацию, использование которой ограничено законом.

Концепция информационной безопасности включает защиту информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий, как природных, так и искусственных, которые могут нанести значительный ущерб владельцам информации, пользователям и поддерживающей инфраструктуре.

Роль информационной безопасности в национальной безопасности.

В 21 веке растущая роль информационных ресурсов и технологий в развитии отдельных лиц, общества и государства, наряду с задачей построения информационного общества в Узбекистане, позиционирует информационную безопасность как ведущий компонент в обеспечении национальной безопасности. На это влияют такие факторы, как:

- Национальные интересы выражаются и реализуются через информацию и информационную сферу.

- Информация и информационные системы, наряду с их владением, являются не только основными объектами информационной безопасности, но и ключевыми элементами всех объектов безопасности.

- Использование информационного подхода как основного научного и практического метода для решения вопросов национальной безопасности.

- Проблема национальной безопасности имеет отчетливую информационную характеристику.

Система информационной безопасности связывает информационную политику государства с политикой национальной безопасности, интегрируя основные компоненты государственной политики в единое целое. Это подчеркивает роль и положение информационной безопасности в системе национальной безопасности.

Современная концепция информационной безопасности включает официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности, включая:

- Защита информации (в смысле охраны персональных данных, государственных и служебных тайн и других видов ограниченной информации).

- Компьютерная безопасность или безопасность данных: Набор аппаратных и программных средств, обеспечивающих целостность, авторизованное использование и конфиденциальность данных в компьютерных сетях, и меры по защите информации от несанкционированного использования.

- Защита информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий, которые могут нанести значительный ущерб владельцам информации, пользователям и поддерживающей инфраструктуре.

- Обеспечение гражданам, социальным группам и обществу в целом доступа к качественной информации, необходимой для жизни, обучения и развития.

Обеспечение информационной безопасности

Защита информации включает меры по обеспечению ключевых аспектов информационной безопасности: целостности данных, доступности и конфиденциальности при вводе, хранении, обработке и передаче. Надежная система контролирует доступ к информации для чтения, записи, создания и удаления

авторизованными лицами или процессами, действующими от их имени. Хотя абсолютных систем безопасности не существует, используются надежные системы (в смысле заслуживающих доверия систем). Надежная система позволяет одновременно обрабатывать данные с различными уровнями конфиденциальности группами пользователей без нарушения прав доступа. Основными критериями надежности являются политика безопасности и обеспечение.

Политика безопасности - это набор правил, определяющих процедуры и механизмы обеспечения безопасности заданного набора объектов и субъектов. Конкретные механизмы обеспечения безопасности системы выбираются в соответствии с принятой политикой безопасности.

Обеспечение, пассивная часть защиты, отражает уровень доверия к системе в процессе ее использования. Надежная система должна регистрировать все процессы, связанные с безопасностью.

Список использованной литературы:

1. Umarov, A., Ro'zaliyev, A., & Qodirov, A. (2023). FISHING VA (SOCIAL ENGINEERING) IJTIMOYIY MUHANDISLIKKA QARSHI KURASHISH TATU FARG 'ONA FILIALI. Educational Research in Universal Sciences, 2(12), 330-333.
2. Vahobjon, A., Umarov, A., & Ahmadxon, Q. (2023). PYTHONDA ARRAYLAR, MASSIVLAR, MATRITSALAR VA NUMPY KUTUBXONASI IMKONIYATLARI. Educational Research in Universal Sciences, 2(12 SPECIAL), 327-329.
3. Qodirov, A., Umarov, A., & Ro'zaliyev, A. (2023). OBYEKTGA YO 'NALTIRILGAN DASTURLASHGA KIRISH. Educational Research in Universal Sciences, 2(14), 481-484.454
4. Umarov, A., & Ro'zaliyev, A. (2023). AXBOROTNI RUXSATSIZ FOYDALANISHLARDAN HIMOYALASH. Educational Research in Universal Sciences, 2(11), 500–502
5. Ro'zaliyev Abdumalikjon Vahobjon o'g'li, Umarov Abdumuxtor Maxammad o'g'li, & R. Adaxanov. (2022). AXBOROT XAVFSIZLIGIDA BIOMETRIK HIMOYA USULLARI. Proceedings of International Educators Conference, 1(2), 177–181.
6. Muxtorov Farrux Muxammadovich, Umarov Abdumuxtor Maxammad o'g'li, & Ro'zaliyev Abdumalikjon Vahobjon o'g'li. (2022). Умаров , А. (20
7. Umarov, A., & Qutlug'beka, T. (2023). FISHING HUYUMLARDAN HIMOYA QILISHNING ASOSIY USULLARI VA CHORALARI. INNOVATION IN THE MODERN EDUCATION SYSTEM, 3(36), 317-320.

8. Muxtarov, F., Umarov, A., & Ro'zaliyev, A. (2023). Axborot tizimlarida xavfsizlik tahdidlarining tasnifi. Engineering problems and innovations.