шифрования, регулярные аудиты безопасности и обеспечение прозрачности обработки данных для граждан.

Исследование потенциала расширения использования биометрической идентификации в таможенной сфере позволило оценить значительные преимущества этой технологии для повышения эффективности и безопасности границ. Биометрическая идентификация обладает уникальной способностью к быстрой и точной проверке личности, что является критически важным для таможенных операций в условиях современных миграционных и экономических вызовов. [2]

Основные выводы:

Технологическая эффективность: Биометрические системы, благодаря своей способности к быстрому и точному сбору и анализу уникальных физиологических данных, могут значительно ускорить процессы на таможне, сократить очереди и повысить общую пропускную способность границ.

Безопасность и контроль: Улучшение контрольных процедур на границах с помощью биометрии способно значительно снизить риски нелегальной иммиграции, контрабанды и терроризма благодаря высокой точности идентификации личностей.

Правовые и этические аспекты: Несмотря на технические преимущества, биометрические технологии требуют тщательной правовой регуляции для обеспечения защиты личных данных и соблюдения прав человека.

Литература

1. ООН. Комиссия по народонаселению (2019). Биометрическая идентификация и защита данных: тенденции и вызовы. Доклад № E/CN.17/2019/9.

2. Харитонов, А. (2019). Биометрическая идентификация в таможенной сфере: технологии и инновации. Москва: Издательство "Техногиз".

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Немогай К.О., Филимонова Т.И.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

В современном мире каждый человек ежедневно использует интернет и информационные технологии, однако необходимо помнить о существовании киберугроз. Поэтому обеспечение кибербезопасности является

важнейшей задачей для всех секторов общества. Выделяют следующие правила обеспечения кибербезопасности в современных условиях.

Во-первых, кибергигиена, с помощью которой пользователи могут защитить свои данные и устройства, путем использования сложных паролей, обновляя программное обеспечение и ограничивая доступ к личной информации.

Во-вторых, пользователи должны предпринимать меры по защите компьютерных сетей, используя, в первую очередь, системы по обнаружению вторжений, а также применение политик безопасности, использование различных брандмауэров и шифрование данных, которое может применяться как для хранения данных, так и для их передачи по сети. Важно помнить, что существует огромное количество алгоритмов шифрования, и нужно выбирать только самые надёжные и современные методы.

Нельзя забывать про антивирусное программное обеспечение, которое предназначено не только для блокировки и удаления различных вирусов, но и вредоносных программ в целом. Каждому пользователю необходимо установить и регулярно обновлять антивирусные программы, как и своевременно осуществлять резервное копирование данных, путем создания копии на жёстких дисках, дискетах и съёмных носителях, чтобы в случае потери данных можно было легко восстановить потерянную или повреждённую информацию. [1]

Одной из важных программ считается система мониторинга и реагирования на киберугрозы, которая позволяет своевременно обнаружить несанкционированные атаки со стороны и предоставит план действий и команды ответов на поступающие уведомления о нарушении безопасности.

Обучение и постоянное обновление знаний в сфере кибербезопасности является ещё одним немаловажным аспектом, ведь киберугрозы постоянно меняются и развиваются, поэтому необходимо быть в курсе последних событий. Чтение специальной литературы, посещение различного рода конференций и семинаров помогут вам быть осведомлёнными в сфере защиты личной информации и данных.

Многие организации и государства взаимодействуют между собой как на региональном уровне, так и на международном, что способствует обмену информацией о новых видах атак, киберугроз и методах борьбы с ними, чтобы обеспечить коллективную защиту от киберпреступности. Помимо этого необходимо соблюдать законодательные акты и требования в сфере защиты информации от киберугроз, разрабатываемые государством. Благодаря совместным усилиям можно обеспечить безопасность в цифровом мире. [2]

В случае несоблюдения основных правил обеспечения кибербезопасности, пользователи и организации могут столкнуться с рядом серьёзных

последствий, например, потерей данных. Выполненная кибератака может нарушить конфиденциальность личной, финансовой информации, а также данных, что может нанести ущерб пользователю или организации.

Киберугрозы могут временно или полностью остановить бизнес-процесс и прервать работу системы организации, в следствии чего возникают проблемы, связанные с потерей дохода, недовольством клиентов и простоями в работе в целом.

Кибератаки могут привести и к юридическим последствиям, в случае нарушения законодательства о защите данных, пользователи и организации могут столкнуться с правовыми последствиями, что включает санкции, штрафы и судебные разбирательства.

Защита кибербезопасности в наши дни представляет собой сложную задачу, требующую постоянного внимания и усовершенствования. Сочетание технических средств безопасности, организационных процессов и обучения пользователей является фундаментом успешной защиты информации от киберугроз. Важно регулярно модернизировать системы и методы защиты, следить за новыми угрозами и активно сотрудничать с другими организациями и структурами для обмена информацией и опытом. Только так можно минимизировать риски и обеспечить надежную кибербезопасность в современном цифровом мире.

Литература

1. О некоторых вопросах обеспечения кибербезопасности в современных условиях // [Электронный ресурс].Режим доступа : https://cyberleninka.ru/article/n/o-nekotoryh-voprosah-obespecheniya-kiberbezopasnosti-v-sovremennyh-usloviyah / Дата доступа: 23.04.2024.

2. Что такое кибербезопасность // [Электронный ресурс].Режим доступа: https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-kiberbezopasnost / Дата доступа: 20.04.2024.

УДК 004.658.6

ИСПОЛЬЗОВАНИЕ БАЗ ДАННЫХ В ТАМОЖЕННЫХ ОРГАНАХ

Перевозникова Д.Д., Удовидчик А.О.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Обработка огромных объёмов данных является обычным явлением в нашем современном мире, в основе которого лежат информационные