Проект Synapse Dress от нидерландского дизайнера Anouk Wipprecht позволяет отображать на ткани эмоции, которые чувствует человек, в виде световых сигналов. Данное платье считывает сердцебиение человека и загорается синхронно с ним.

Продукт, созданный Levi's и Google, представляет собой куртку с вплетенными в нее нитями, реагирующими на прикосновение. Она способна взаимодействовать со смартфоном и превращаться в сенсорный элемент управления. Так похлопывая и поглаживая рукав, можно менять громкость музыки

Футболка Ambiotex способна считывать ваши жизненные показатели: частоту пульса и дыхания, вариабельность сердечного ритма и общую динамику показателей. Она способна сообщить о проблемах со здоровьем и указать на недостатки при тренировке.

Так как концепция умной одежды находится в начале своего развития, почти каждый продукт можно описать словом перспективный. Но о некоторых проектах уже ясно, что они провалились. Ярким примером этого служит серия Tommy Jeans Xplore от компании Tommy Hilfiger. Линейка состояла из 23 предметов одежды, от бейсболок до худи. Цены на новую одежду были завышены более чем в полтора раза, от 30 до 100 долларов США. А так как функционал данной одежды состоял лишь в том, чтобы передавать ваше местоположение, продукт стал одним из основных провалов компании. Другим примером служит куртка Omius Jacket. Она служит для регулирования температуры вашего тела. Однако производители не справились с поставленной задачей.

**Заключение.** Умная одежда является перспективной отраслью. Она способна дать нам много возможностей во множестве сфер жизни. Она может спасать жизни, быть предметом моды, упрощать жизнь и повышать ее качество. С другой стороны, данная сфера только начала развиваться и нет четкого представления о том, как концепция умной одежды будет выглядеть через 10—15 лет. Но очевидно то, что, чтобы такая технология стала массовой, придется вложить большое количество ресурсов, времени и денег. Ведь далеко не все вещи становятся привычными быстро и легко.

**Список цитируемых источников**

1. Future Force Warrior [Electronic resource]. — Mode of access : https://en.wikipedia.org/wiki/Future_Force_Warrior . — Date of access: 07.05.2022.

2. Vêtements biométriques pour le sport, la recherche et la santé [Electronic resource]. — Mode of access : https://fr.hexoskin.com . — Date of access: 07.05.2022.

3. Nadi X — Smart Yoga Pants that Guide Your Form by Wearable X [Electronic resource]. — Mode of access : https: //www.kickstarter.com/projects/1727484594/nadi-x-yoga-pants-smart-yoga-pants-for-travel-and . — Date of access: 07.05.2022.

УДК 37.015.3:004.056.34

**А. А. Мороз, О. Л. Бушейко**

*Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь*

## ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНТЕРНЕТА В МИРОВОМ ПРОСТРАНСТВЕ

**Введение.** Средства массовой информации постепенно уступают позиции средствам массовой коммуникации. Сегодня одним из основных средств общения, обучения, образования становится интернет-пространство. Пользование Интернетом стало неотъемлемым правом человека. Однако, большинство стран мира вынуждены регулировать доступ к информации, размещенной в Интернете.

**Основная часть.** В зависимости от страны выделяют такие модели правового регулирования Интернета как континентальная (европейская) модель, англо-американская, азиатская и ближневосточная.

Континентальная (европейская) модель направлена на обеспечение баланса интересов государства и частной инициативы. Особенность ее состоит в том, что личная инициатива жестко регламентирована законодательством. На первое место ставится развитие услуг по информированию граждан. Данная модель применяется во Франции, Германии, России.

Закон Российской Федерации № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации» предусматривает ограничение доступа к материалам, нарушающим его. К нарушениям относятся: призывы к массовым беспорядкам, осуществление экстремистской деятельности, участие в массовых (публичных) мероприятиях, информация, содержащая детскую порнографию, призывающая к участию в ней, пропагандирующая наркотики, самоубийства и т. д. Доступ к таким сайтам должен быть ограничен в течение суток с момента включения сетевого адреса в реестр оператора связи, оказывающего услуги по предоставлению доступа к сети Интернет [1].

С 2018 года для обмена электронными сообщениями предусмотрена обязательная идентификация пользователей по абонентским номерам [2]. В Республике Казахстан с 5 июля 2004 года действует Закон № 567-II «О связи», согласно которому, обязанности по ограничению доступа к информации, размещенной в сети Интернет, возлагаются на оператора связи. В случае обнаружения распространения запрещенной информации

генеральный прокурор или его заместители вносят предписание Министерству информации и коммуникаций об устранении нарушений закона в течение не более трех часов.

В 2017 году в Закон Республики Казахстан «О средствах массовой информации» внесены поправки, предполагающие введение обязательной идентификации пользователей, комментирующих сообщения в Сети [3].

Германия одна из первых в 1997 году приняла закон, регламентирующий использование Интернета. Согласно ему, ответственность за размещение информации несут интернет-провайдеры, и, если это технически возможно, должны блокировать известные им предосудительные материалы, созданные другими. Закон закрепляет базовый принцип: «Что не законно вне Интернета — не законно и в Интернете».

Согласно германского закона об авторском праве уголовным преступлением считается скачивание музыки и фильмов из Сети. Правоохранительными органами контролируется возможность использования интернет-пространства преступниками. Законом ФРГ о защите сетей (с 2017 года) предусмотрено удаление всех записей и комментарий, нарушающих законодательство, в течение суток с момента поступления жалоб пользователей на содержание опубликованного контента. Так же владельцам соцсетей за не своевременное удаление фейковых новостей предусмотрены штрафы.

Яркими чертами англо-американской модели являются полная либерализация рынка, информационных технологий, гибкое законодательство, сведение до минимума контроля государства, максимальная поддержка частной инициативы, стимулирование технического прогресса как главной цели правового регулирования. Данная модель применяется в США и Великобритании. В США Интернет со стороны государства остается свободным от технических методов цензуры. Фильтрация контента добровольно осуществляется частными компаниями при поддержке госструктур. Отдельной темой в сети Интернет США является борьба с терроризмом. После теракта 11 сентября 2001 г. был принят Закон «Об объединении и укреплении Америки». В соответствии с ним, любое действие, ведущее к нарушению работы или незаконному проникновению в компьютер, классифицируется как терроризм. В публичных пунктах доступа к Интернету введены фильтры, ограничивающие доступ к экстремистским материалам.

В Великобритании нормативные правовые акты, позволяющие правительству ограничивать или запрещать доступ пользователей к информации в Интернете в масштабах государства, отсутствуют. Все же деятельность информационного пространства контролируют различные общественные организации. Так же у интернет-провайдеров для блокировки к запрещенным сайтам есть специальное программное обеспечение, разработанное в 2004 г. государственной корпорацией.

Характерной чертой азиатской модели является доминирующая роль государства в регулировании Интернета, обеспечение им крупных инвестиций в развитии информационно-коммуникационных технологий. Азиатская модель реализуется в Китае, Сингапуре, Вьетнаме. Главный регулятор в Китае, принимающий решения о блокировке Интернет-контента, является Государственная канцелярия Интернет-информации, которая регулярно публикует списки незаконных сайтов.

Китайская система контроля Интернета – это механизм, базирующийся на трех основных элементах:

– системе фильтрации трафика «Золотой щит»;

– системе блокировки поиска нежелательной информации;

– ручной системе фильтрации контента, публикуемого в соцсетях и блогосфере.

В Интернет-сфере запрещено провоцировать национальную ненависть, подрывать национальное единство, пропагандировать культы, насилие, убийство, террор, распространять порнографию и др.

В Китае установлены требования к регистрации аккаунтов с указанием реальных паспортных данных, обязательному тестированию и сертификации IT-оборудования, ограничению хранения данных за пределами государства. Требуется специальное разрешение на хранение сведений за рубежом.

Для ближневосточной модели характерно доминирование религиозного фактора. Так как эта модель характерна для таких стран как Саудовская Аравия, Индонезия, Иран, где большинство населения исповедуют ислам, то власти стремятся блокировать контент, который противоречит его нормам [1].

Если мы возьмем Беларусь то, согласно Закону «О средствах массовой информации», запрещено распространение сведений о потреблении наркотических средств; информации, направленной на пропаганду войны, экстремистской деятельности или содержащей призывы к ней; порнографии, насилия и жесткости, и других сведений, способных нанести вред национальным интересам республики. Принимает решение об ограничении доступа к интернет-ресурсу Министерство информации.

Оперативно-аналитический центр при Президенте Республики Беларусь, совместно с Министерством связи и информатизации, устанавливает порядок ограничения доступа пользователей к запрещенной информации по сформированному Госинспекцией списку. Работа интернет-ресурса, попавшего в список ограниченного доступа должна быть прекращена в течение суток.

Для совершенствования законодательства в информационной сфере, в 2018 г. был принят Закон «О внесении изменений и дополнений в некоторые законы Республики Беларусь», установлена обязанность владельца проводить идентификацию пользователей (комментирование) [4].

**Заключение.** Исходя из выше сказанного, мы понимаем, что большинство развитых стран мира регулируют доступ к информации в сети Интернет. Общими мерами являются запретительные меры по отношению к охраняемой законом государственной тайне, порнографическим материалам, информации, направленной на пропаганду наркотиков, содержащей призывы к терроризму, национальной, расовой вражде, носящей оскорбительный характер, нарушающий неприкосновенность личной жизни.

**Список цитируемых источников**

1. Актуальные вопросы обеспечения информационной безопасности : пособие для педагогов учреждений образования, реализующих образоват. программы общего сред. образования / В. А. Арчаков [и др.]. — Минск : Нац. ин-т образования, 2021. — 168 с. : ил.
2. Фильтрация контента в интернете. Анализ мировой практики [Электронный ресурс]. — Режим доступа : https://www.slideshare.net/MatveyAlexeev/ss-25553826 . — Дата доступа :28.04.2022.
3. Закон Республики Казахстан от 5 июля 2004 года № 567-II «О связи» [Электронный ресурс]. — Режим доступа : https://online.zakon.kz/Document/?doc_id=1049207#pos=0;0 . — Дата доступа :05.05.2022.
4. О мерах по совершенствованию использования национального сегмента сети Интернет : Указ Президента Республики Беларусь от 1 февр. 2010 г., № 60. // Нац. реестр правовых актов Респ. Беларусь. — 2012. — № 8. — 1/13223.

УДК 004.8

**О. И. Наранович, Е. Г. Шапович**
*Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь*

# БИОМЕТРИЧЕСКАЯ ВЕРИФИКАЦИЯ ЛИЧНОСТИ

**Введение.** Кражи идентификационных данных вызывают все большую обеспокоенность в обществе. Жертвами хищения идентифицирующих сведений ежегодно становятся миллионы, а «кража личности» стала самой распространенной жалобой потребителей. В цифровую эпоху традиционных методов аутентификации — паролей и удостоверений личности — уже недостаточно для борьбы с хищением идентифицирующих сведений и обеспечения безопасности.

Биометрические системы распознают людей на основе их анатомических особенностей (отпечатков пальцев, образа лица, рисунка линий ладони, радужной оболочки, голоса) или поведенческих черт (подписи, походки). Поскольку эти черты физически связаны с пользователем, биометрическое распознавание надежно в роли механизма, следящего, чтобы только те, у кого есть необходимые полномочия, могли попасть в здание, получить доступ к компьютерной системе или пересечь границу государства.

Цель этого исследования состоит в разработке модуля биометрической верификации личности на основе бинокулярной стерео-реконструкции плоскости лица с использованием интерполяции.

**Основная часть.** Разрабатываемый модуль должен выполнять следующий функции:

– корректная верификация пользователей по лицевым ориентирам, с занесением данных об авторизации в базу данных;

– распознавание незарегистрированного пользователя, с сохранением информации о нем, и возможностью наделения его в дальнейшем регистрационными данными;

– авторизация большого количества лиц на потоковом видео;

– реконструкция плоскости лица на основе стереопары.

Объектом исследования является биометрическая верификация на основе лицевых ориентиров.

Предметом исследования является разработка модуля биометрической верификации на основе бинокулярной стерео-реконструкции.

Актуальность данного исследования заключается в возможности внедрения полученных данных в системы безопасности, информационные системы и терминалы, доступ к которым будет открыт только после прохождения аутентификации.

Для создания приложения выбрана версия интегрированной среды разработки программного обеспечения JetBrains Intellij IDEA 2018.1 на языках высоко уровня Java и Python.

Java — сильно типизированный объектно-ориентированный язык программирования, разработанный компанией Sun Microsystems (в последующем приобретенной компанией Oracle). Приложения Java обычно транслируются в специальный байт-код, поэтому они могут работать на любой компьютерной архитектуре, с помощью виртуальной Java-машины [1].

Python — высокоуровневый язык программирования с динамической типизацией, поддерживающий объектно-ориентированный, функциональный и императивный стили программирования. Это язык общего назначения, на котором можно одинаково успешно разрабатывать системные приложения с графическим интерфейсом, утилиты командной строки, научные приложения, игры, приложения для веб и много другое [2].

Для корректного определения контрольных точек лиц на фото необходимо последовательно выполнить следующие действия: распознать и локализовать лица на фото; определить уникальные характеристики каждого лица. Для обнаружения лиц на фото используется метод гистограммы направленных градиентов. Согласно данному методу, исходное изображение приводиться к черно-белому. Затем последовательно происходит работа с каждым пикселем. На каждом шаге происходит исследование прилегающей области пикселей, с целью нахождения локальных направлений затемнения пикселей. В результате получаем градиенты,