оптимизации ЭДО должны дополняться, объединяться и формировать единое и сильное «цифровое государство».

1. Цифровое государственное управление – Цифровая экономика, URL: <https://data-economy.ru/government>
2. Электронное правительство – Министерство цифрового развития, связи и массовых коммуникаций, URL: <https://digital.gov.ru/ru/activity/statistic/rating/elektronnoe-pravitelstvo-v-rf/>
3. Доброва О.А. Цифровая реформа. Анализ Российского опыта внедрения информационных систем, поддерживающих деятельность органов государственной власти, URL: <http://government.e-rus.ru/site.shtml?id=82>
4. Рейтинг стран мира по Индексу развития электронного правительства. / Гуманитарная энциклопедия: Исследования // Центр гуманитарных технологий, 2006–2021, URL: <https://gtmarket.ru/ratings/e-government-development-index>
5. Мордакин О. В. Технология организации электронного документооборота в органах государственной власти // Эпоха науки - № 6 – 2016 г. – С. 68
6. Система межведомственного электронного документооборота органов власти – EOS, URL: https://eos.ru/eos_products/solution/gosudarstvennyy_sektor/medo/
7. Портал государственных услуг Российской Федерации – Госуслуги, URL: <https://www.gosuslugi.ru/>
8. Федеральная служба государственной статистики – Росстат, URL: <https://rosstat.gov.ru/>

Постникова М.С.

Современные технологии обеспечения информационной безопасности

*Московский университет МВД России имени В.Я. Кикотя
(Россия, Москва)*

doi: 10.18411/lj-04-2021-22

Аннотация

В данной статье рассказывается о том, какой должна быть информационная безопасность в век развития и постоянного совершенствования Интернет - технологий. А также раскрывается суть и назначение основных способов защиты информации в информационном обществе.

Ключевые слова: Интернет - технологии, информационная безопасность, информация, информационное общество.

Abstract

This article describes what information security should be like in an age of development and continuous improvement of Internet technologies. And also reveals the essence and purpose of the main ways of protecting information in the information society.

Keywords: The Internet - technologies, information security, information, information society.

Какой должна быть информационная безопасность в век развития Интернет – технологий? Нужно ли организациям, фирмам, индивидуальным пользователям персональных компьютеров предусмотреть финансирование защиты электронных данных при их создании, обработке, хранении и использовании?

В век развития цифровых технологий решение проблемы защиты информации позволяет предотвратить множество политических, экономических, социальных и иных проблем, остро стоящих перед современным обществом, которое активно использует различные гаджеты и Интернет - технологии.

Сегодня создана своеобразная система взаимосвязанных методов и способов сбора, обработки, хранения, накопления информации, которые основаны на применении вычислительной техники. На этой основе строятся системы верификации и идентификации информации для государственных и негосударственных структур.

В настоящее время активно развиваются и криптографические компьютерные технологии, основанные на шифровании данных - обновлении и видоизменении информации для того, чтобы обеспечить её конфиденциальность.

Согласно закону РФ «Об информации, информационных технологиях и защите информации» конфиденциальность информации - обязательное требование не передавать такую информацию третьим лицам без согласия её обладателя.

Криптографические технологии главным образом позволяют обеспечить нормальную работоспособность приложений, работающих в сети. Советский и российский историк, доктор исторических наук, профессор, публицист, общественный деятель Аполлон Кузьмин считает, что при этом важны гарантии позитивного использования как уже имеющихся, так и планируемых к реализации «перспективных криптографических решений на... множество прикладных программных продуктов, сетевых операционных систем и аппаратных платформ, на которых базируются ... информационные системы и ресурсы». Сегодня на их базе уже работают в сети банки, магазины, школы, бизнес.

Развитие данных технологий без сомнения важно и нацелено не только на текущий момент, но и на дальнейшую перспективу. Без включения в механизм защиты данных новых прогрессивных технологий и их развития, усовершенствования, просто не мыслима современная жизнь.

Судите сами. Может ли современное общество, например, обойтись без прочно вошедшей в обиход *электронной подписи*, которая сегодня не только полностью может заменить рукописную, но и обладают определенной юридической силой? Стандарт электронной подписи помогает реализовать обеспечение безопасности информации. Подпись присоединена к документу и во всех случаях её можно проверить и невозможно подделать. При её создании заложены серьёзные криптографические методы защиты информации. В отличие от рукописной подписи электронная подпись имеет более широкую сферу применения. В некоторых ситуациях невозможно подписать документ от руки и необходимо использование именно электронной подписи.

Важным вектором обеспечения информационной безопасности является и *развивающаяся и разрастающаяся система электронных цифровых сертификатов с помощью центров поддержки*. Целью таких систем является обеспечение безопасного соединения между облачными технологиями и браузером, создание надежной защиты данных от замены и подделки информации.

При их поддержке данные посещаемых сайтов зашифровываются и применяется процесс аутентификации, что обеспечивает возможность посетителям и пользователям сайтов прекратить сомнения по поводу того, что вводимые ими личные данные не выйдут за пределы сайта и не попадут в руки злоумышленников.

Эффективно работает и *система шифрования трафика компьютерных сетей*, обеспечивающая целостность и достоверность информации в процессе её обработки, хранения и передачи. Шифрование переводит данные в нечитаемый код, обеспечивая защиту информации.

Не стопроцентным, но достаточно эффективным средством обеспечения защиты информации является использование *антивирусных программ*, которые способствуют обнаружению компьютерных вирусов и программ, наносят вред компьютеру. Они помогают найти, не допустить размножения и удалить с устройства компьютерные вирусы.

Важным представляется и проработка механизма *гарантии защиты электронных данных от несанкционированного доступа посторонних лиц*. Это позволяет избегать утечки информации, быстро реагировать на попытки несанкционированного доступа, применяя меры беспрецедентной защиты. Данные

методы контроля срабатывают в случаях потери или хищения носителей, действенны при работе с объектами критической информационной инфраструктуры.

Всё более широким становится сектор *средств биометрической аутентификации*, например, электронная дактилоскопия, аутентификация по сетчатке или по радужной оболочке глаза, по геометрии руки или лица, термография лица, распознавание голоса, почерка, верификация подписи и тому подобное. Это перспективное и постоянно развивающееся направление, новые открытия в котором ещё, несомненно, впереди.

Несомненно, фактором успеха в современном мире является не столько создание информации, сколько умение обеспечить её безопасность, сохранность. Поэтому не оставляет сомнения, что информационная защищённость организаций, индивидуальных пользователей персональных компьютеров в современном мире должна быть беспрецедентной. Состояние незащищенности информационной среды – задача первого плана для современного общества, которое всё больше зависти от Интернет-технологий.

1. Федеральный закон от 27.07.2006 (ред. 09.03.2021) №149-ФЗ «Об информации, информационных технологиях и защите информации»
2. <https://referat.me/informatics/130892-sovremennye-tehnologii-obyasneniya-informacionnoy-bezopasnosti>
3. ГОСТ 34.10-2018 (полное название: «ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», англ. «Information technology. Cryptographic data security. Signature and verification processes of electronic digital signature»)
4. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (последняя редакция)

Сафонов Н.М.

Классификация радиосигналов свёрточными нейронными сетями

*Российский технологический университет МИРЭА
(Россия, Москва)*

doi: 10.18411/lj-04-2021-23

Аннотация

В настоящей статье представлен краткий экскурс в теоретическую и практическую сферу классификации радиосигналов с помощью метода свёрточных нейронных сетей, представление того, что такое радиосигнал, его виды и сферы применения. Оценка возможностей нейронной сети.

Ключевые слова: нейронная сеть, радиосигнал, глубокое обучение, свёрточная сеть.

Abstract

This article presents a brief overview of the theoretical and practical field of classification of radio signals using the convolutional neural network method, an idea of what a radio signal is, its types and applications. Evaluating the capabilities of a neural network.

Key words: neural network, radio signal, deep learning, convolutional network.

На сегодняшний день объёмы данных нещадно растут в сравнении с предыдущими десятилетиями, как и человеческие ресурсы, затрачиваемые на их обработку. С развитием технологий человечество всегда упрощало свою работу, делая её более эффективной и продуктивной. Технологии машинного обучения берут своё начало ещё в 19-ом веке, но не получили должного распространения ввиду отсутствия достаточных вычислительных мощностей. Любой метод машинного обучения