При использовании такой системы на контрольно-пропускных пунктах, получая данные с камер видеонаблюдения установленных в локальных зонах АЭС, можно создавать базы данных психофизиологического состояния сотрудников станции, и при резких изменениях состояния человека оперативно на это реагировать.

ЛИТЕРАТУРА

1. "Безопасность Окружающей Среды" №3-2007: Безопасность ядерных и радиационных объектов. Статья «Системы физической защиты объектов ядерной энергетики». Севрюков Д.В., Асфандияров А.Х.

2. http://vi.elsys.ru/storage/nto.pdf

3. Signal Processing in the Vestibular System During Active Versus Passive Head Movements, Kathleen E. Cullen and Jefferson E. Roy Aerospace Medical Research Unit, Department of Physiology, McGill University, Montreal, Quebec H3G 1Y6, Canada Submitted 14 October 2003; accepted in final form 9 January 2004

RU 2289310 приоритет 16.02.2004г. Патент на изобретение Российской Федерации «Способ получения информации о психофизиологическом состоянии живого объекта», В.А.Минкин, А.И.Штам.

А.А.ГРИГОРЬЕВ[1], А.А.ОХРИМЕНКО[2], И.П.СИДОРЧУК[3]

ФОРМИРОВАНИЕ НОВЫХ ПОДХОДОВ ДЛЯ СИСТЕМНОЙ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИИ

[1]*Государственная инспекция Республики Беларусь по электросвязи Министерства связи и информатизации Республики Беларусь (республиканское унитарное предприятие по надзору за электросвязью «БелГИЭ»), г.Минск, Республика Беларусь*

[2]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Республика Беларусь*

[3]*Академия управления при Президенте Республики Беларусь, г.Минск, Республика Беларусь*

Развитие современных технологий, в том числе возможность мобильной передачи данных в больших объемах, их ускоренной обработки, возможности упрощенного хранения и быстроты доступа к ним сделали привлекательным использование электронных систем и их интегрированность в систему государственного управления, в том числе при работе с обращениями граждан и юридических лиц как приоритетном направлении развития демократического общества в современных условиях. Однако те же самые характеристики сделали привлекательными современные технологии также и для лиц (в том числе иностранные государства и лица негосударственные организованные группы и отдельные граждане), стремящихся нанести урон государственным интересам.

Не случайно, в пункте 42 Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, в числе внешних источников угроз национальной безопасности в информационной сфере названы среди прочих: открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия; доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами; нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве; попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам [1].

При этом широкое распространение получили попытки криминальных структур внедрения в информационное пространство, в том числе в целях распространения наркотиков, вербовки наемников, внедрения в общественное сознание противоречащих общечеловеческим и национальным духовно-нравственным ценностям взглядов, что требует безотлагательной реакции как Республики Беларусь, так и иностранных государств, в рамках обеспечения

международного сотрудничества. Не случайно, уровень угроз повлек к объединению усилий для устранения противоправной деятельности даже государств с различными политическими системами и доминирующими моральными ценностями, таких как США и КНР.

Республика Беларусь также не остается в стороне от данных процессов примером чему служит ряд новых нормативных правовых актов в данной сфере, в том числе Декрет Президента Республики Беларусь от 28 декабря 2014 г. № 6 «О неотложных мерах по противодействию незаконному обороту наркотиков», постановление Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 г. № 6/8 "Об утверждении Положения о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет» [1]. Данные документы позволили безотлагательно отреагировать на ряд общественно опасных угроз, в том числе, связанных с распространением опасных психотропных веществ.

Несмотря на принятие ряда мер, направленных на защиту общества от неблагоприятных процессов в глобальной компьютерной сети Интернет, а также направленных на повышение доступности государственной власти и активизацию ее присутствия в данной сети, например, Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» (в редакции Указа Президента Республики Беларусь от 23 января 2014 г. № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий»), ряд вопросов остается недостаточно урегулированным как на национальном, так и на международном уровнях.

Например, остается четко не определенным правовой статус договоров об обмене информацией о персональных данных граждан и юридических лиц (относятся ли данные договоры к сфере административного или гражданского права, каков характер ответственности за их нарушения, понуждению к заключению, возмещению убытков и т.п.), что существенно препятствует правовой защите прав и свобод граждан и организаций, затрудняет реализацию их обязанностей. В этой связи представляется, что должны найти свое нормативное отражение правила регламентации заключаемых на практике административных договоров, форма и содержание. Целесообразно рассмотрение вопроса о централизации данных процессов и устранения необходимости многоступенчатой системы передачи данных, например, при принятии решений об ограничении доступа к информационным ресурсам. В ряде государств такие функции сконцентрированы у специализированных правоохранительных структур, что исключает вовлечение в данный процесс различных организаций, не относящихся к системе органов обеспечения национальной безопасности. При этом зачастую различными государствами ставится вопрос о законности такой деятельности [2].

Также остается неурегулированным вопрос о правовой защите граждан и организаций при деятельности глобальных поставщиков услуг, в том числе безвозмездных в данной сфере, которые используют персональные данные, предоставляют услуги электронных «почтовых» серверов, поисковых систем и т.п., ограничению их прав по поиску и распространении информации о гражданах и организациях, сохранению конфиденциальности.

При этом сохраняет важность вопрос уязвимости государственных информационных систем при монополизации отдельных программных продуктов и технологических систем зарубежными коммерческими организациями, которые в ряде случаев осуществляют широкомасштабное сотрудничество с правоохранительными и разведывательными структурами иностранных государств. Представляется, что решению данных проблем могло бы способствовать формирование независимого программного продукта и технических средств индивидуально ориентированных на государственные нужды с учетом специфики функционирования государственных структур.

В связи с глобализацией отношений, усилением миграции, требует универсального правового решения вопрос рассмотрения электронных обращений граждан и организаций, осуществления в отношении их административных процедур, которые не во всех случаях могут идентифицироваться при помощи электронной цифровой подписи (при этом данный вид идентификации также не является абсолютно надежным при появлении копий таких ключей). Данный вопрос может быть урегулирован нормами международных договоров. При этом в таких договорах следует особо оговорить правила, исключающие ответственность чиновников

и иных лиц, рассматривающих обращения, при рассмотрении сообщений, сформированных виртуальными машинами, в том числе с использованием вымышленных или похищенных персональных данных, учитывая, что соответствующие права, свободы и обязанности при формировании электронных обращений могут существовать только у реальных граждан и организаций, а не у виртуальных или иных механизмов и структур.

Таким образом, представляется оправданным усиление взаимного сотрудничества государств, в том числе в лице чиновников и научных работников различных областей знания, в целях минимизации угроз обществу и государствам, международному сообществу в целом при использовании средств электронных коммуникаций.

ЛИТЕРАТУРА

1. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Режим доступа: http://www.pravo.by. – Дата доступа: 26.09.2015.

2. Дельфинов, А. СМИ: Шпионский скандал может осложнить отношения BND с другими спецслужбами [Электронный ресурс] / А.Дельфинов // Deutsche Welle. – Режим доступа: http:// www.dw.com. – Дата доступа: 26.09.2015.

А.М.ДРАКО[1]

НЕЙРОСЕТЕВОЕ ДЕКОДИРОВАНИЕ ЛИНЕЙНЫХ БЛОЧНЫХ КОДОВ

[1]*Учреждение образования «Белорусский государственный технологический университет», г. Минск, Республика Беларусь*

В помехоустойчивом кодирование существует множество методов декодирования. Однако до сих пор не существует универсальных методов для декодирования данных. Развитие технологии нейронных сетей реализует возможность вплотную приблизиться к единому методу декодирования, при этом не уступающему по основным показателям классическим методам.

Помехоустойчивое кодирование является неотъемлемой частью процесса передачи информации, значимость которого на данный момент в современном информационном обществе трудно переоценить. При этом необходимо отметить, что именно декодер играет ключевую роль в исправлении ошибок. Идеальный декодер должен работать как универсальное средство с единым методом декодирования и отличаться высокой скоростью декодирования и уровнем обнаружения и исправления ошибок. В рамках диссертационной работы исследуется нетривиальный способ декодирования, а именно декодирование с использованием нейронных сетей. Данный метод отличается от классических методов, тем что система не делает «прямых» вычислений при декодировании, а пытается «по памяти» получить из полученного сообщения исходное.

Как уже было сказано нейронная сеть не вычисляет исходное сообщение, а скорее пытается «узнать» его. Человек обладает способностью читать предложения с ошибками, а также исправлять их, путем тренировки нейронов мозга на запоминание и дальнейшее распознавание (классификацию) полученных паттернов. С появлением идеи нейронных сетей стало возможно обучить машину запоминать необходимый словарь (например исходное сообщение) и распознавать в полученном сообщение исходное. При содержании в переданном сообщение ошибки замена исходным сообщением исправит ошибку. Однако нельзя просто передать исходящее сообщение и надеяться, что машина поймет его правильно, как человеку так и машине нужен контекст. Именно этим контекстом является избыточные символы при кодировании.

Нейронные сети на данный момент могут решать ряд задач. Для декодирования наиболее интересна возможность решения задачи классификации, которая состоит в определении принадлежности входного образа (например, языкового сигнала или рукописного символа), представленного вектором признаков, к одному или нескольким предварительно определенным классам. Нейронные сети применяться, как наиболее эффективным способом классификации, потому что генерируют фактически большое число регрессионных моделей (которые используются в решении задач классификации статистическими методами).