Таким чином, тональність тексту визначається трьома факторами: 1 суб'єкт тональності; 2) власне тональна оцінка (позитив / нейтрально / негатив); 3) об'єкт тональності. Під суб'єктом тональності маємо на увазі автора статті (автора цитати, пряма чи непряма або непрямої мови), під об'єктом тональності – того, про кого він висловлюється, і під тональною оцінкою – емоційне ставлення автора до такого об'єкта.

Дослідження у сфері теорії лінгвістичних емоцій почалися не так давно. У 50-х роках минулого століття Чарльз Осгуд за допомогою методу семантичного диференціала намагався визначати емотивний простір різними наборами парних слів У сучасних системах автоматичного визначення емоційної оцінки тексту найчастіше використовується одновимірний емотивний простір: позитив-негатив, тобто добре-погано. Однак відомі успішні випадки використання і багатовимірних просторів [4, 5].

Емоційна складова комунікації поки не настільки активно застосовується в системах обробки текстової інформації не тільки через труднощі виділення «потрібної» (тобто такої, що потрібна саме даному об'єкту) емоційної лексики в текстах, але і складності визначення самого емотивного простору, кількості і складу його вимірів. На жаль, теорія емоцій в лінгвістиці ще недостатньо розвинена.

Література

1. Бездрабко В. Терміносистеми документознавства: нормативна база / В. Бездрабко // Вісник Книжкової палати. – 2005. – № 9. – С. 23–25.

2. Водолазька С. А. Лінгвістичні основи документознавства: курс лекцій / С. А. Водолазька. – К.: Навч.-вид. лаб. Інституту журналістики, 2007. − 208 с.

3. Грушко С. П. Документна лінгвістика науково-технічного спрямування у сучасному прикладному мовознавстві / С. П. Грушко // Документ. Комунікація. Вип. 1, 2016. – С. 195–201.

4. Котельников Е. В. Распознавание эмоциональной составляющей в текстах: проблеми и подходы / Е. В. Котельников, М. В. Клековкина, Т. А. Пескишева, О. А. Пестов; под. ред. С. М. Окулова. − М. : НОУ «Интуит», 2012. – 103 с.

5. Лемская В. М.Особенности интертекста на исходном и переводящем языках: на материале двуязычных параллельных корпусов /В. М. Лемская // Филологические науки. Вопросы теории и практики. – Тамбов: Грамота, 2012. № 7. Ч. 1. – С. 130–132. [Електронний варіант]. Режим доступу: http://gramota.net/materials/2/2012/7-1/33.html

6. Луговой А. В. Комп'ютерні технології в документній лінгвістиці для спеціальності «Документознавство та інформаційна діяльність» / А. В. Луговой, Н. О. Заніздра, В. В. Шабуніна, Н. В. Рилова // Вісник КПДУ імені Михайла Остроградського. Випуск 5/2008 (52). Частина 2. − С. 180–183.

7. Чемеркін С. Г. Українська мова в Інтернеті: позамовні та внутрішньо-структурні процеси. − К.: НАН України. Інститут української мови, 2009. – 240 с.

УДК 004.056:334.722.2

ОРГАНИЗАЦИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ КОРПОРАЦИИ

И. В. Мальцева

Конечной целью создания системы компьютерной безопасности является защита всех категорий субъектов, прямо или косвенно участвующих в процессах информационного взаимодействия, от нанесения им материального, морального или

иного ущерба в результате случайных или преднамеренных нежелательных воздействий на информацию и способы ее обработки и передачи.

Для защиты компьютерных систем от неправомерного вмешательства используют следующие способы: *идентификация* (опознавание); *аутентификация* (подтверждение подлинности) пользователей; *разграничение доступа* к ресурсам и авторизация (присвоение полномочий); *регистрация и оперативное оповещение* о событиях, происходящих в системе (аудит); *криптографическое закрытие* хранимых и передаваемых по каналам связи данных; *контроль целостности и аутентичности* (подлинности и авторства) информации; выявление и нейтрализация действий компьютерных *вирусов; затирание остаточной информации* на носителях; *обнаружение уязвимостей* (слабых мест) системы; *изоляция (защита периметра) сетей* (фильтрация, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы); *обнаружение атак* и оперативное реагирование; *резервное копирование;* маскировка. Эти варианты защиты могут применяться в конкретных технических средствах и системах в различных комбинациях и вариациях. Наибольший эффект достигается при их использовании в комплексе с другими мерами.

Охарактеризуем способы защиты, применяемые корпорацией Google, которая имеет инфраструктуру глобального масштаба, предназначенную для работы администраторов, общения с клиентами через Интернет, хранения данных конечных пользователей, связи между внутренними службами. Среди основных Интернет - сервисов можно выделить потребительские службы – Search, Gmail, Photos и корпоративные сервисы – G Suite и Google Cloud Platform. Защита у Google условно разделена на несколько уровней, которые включают как аппаратные, так и программные средства защиты.

Физические системы безопасности. Google разрабатывает и создает собственные центры обработки данных. Доступ к ним имеет ограниченное количество сотрудников. Кроме этого, чтобы защитить обработку данных используются такие методы, как биометрическая идентификация, детекторы металла, барьеры, которые закрывают проезд транспортным средствам, лазерные системы обнаружения вторжений.

Аппаратное обеспечение. Центр обработки данных состоит из тысяч серверных машин, подключенных к локальной сети. Это оборудование проходит многократную проверку специалистами. Кроме того, для обеспечения безопасности компания самостоятельно разработала специальные чипы, в том числе аппаратный, который в настоящее время установлен на серверах и периферийных устройствах. Эти чипы позволяют идентифицировать и аутентифицировать законность устройств на аппаратном уровне. В серверах сторонних компаний корпорация использует и другие методы защиты. В частности, все устройства сотрудников подвергаются тщательному просмотру. Google таким образом проверяет наличие актуальных обновлений для ОС и ПО, установленного в системе.

Криптографические подписи, системы аутентификации и авторизации. Каждая служба, которая работает в инфраструктуре, имеет соответствующий специфический идентификатор учетной записи, криптографические учетные данные, которые могут быть связаны с аппаратным или программным обеспечением и используются для подтверждения при работе с другими подразделениями. Эта информация проверяется во время каждой загрузки или обновления. Кроме этого, корпорация Google разработала автоматизированные системы, чтобы гарантировать, что серверы будут обновлять версии программного обеспечения, в том числе патчи безопасности, обнаруживать и диагностировать аппаратное и программное обеспечение, а также, при необходимости, отключать обслуживание компьютеров.

Google предоставляет разнообразные услуги хранения – BigTable и Spanner. Большинство приложений в физическом хранилище косвенно обращаются через них. Для защиты всей информации в них применяются ключи для шифрования данных до их

записи в физическое хранилище. Это позволяет инфраструктуре изолировать себя от потенциальных угроз хранилища, таких как вредоносные прошивки на диске.

Для обеспечения безопасной связи через Интернет, Google проводит аутентификацию пользователя. Эта услуга выражается как страница входа, на которой осуществляется запрос имени и пароля, а также дополнительной информации о клиенте, которая может использоваться для последующих загрузок.

Разработка безопасного программного обеспечения. Корпорация запускает программу Vulnerability Rewards Program, в рамках которой она финансово стимулирует каждого, кто обнаруживает ошибки в инфраструктуре или приложениях и сообщает о них.

Ограничение и контроль действий сотрудников, которым предоставлен административный доступ. Каждый сервер, сервис и сотрудник получают собственный идентификатор. Связи между людьми-операторами, компьютерами и программной частью кодируются и распределяются в глобальном пространстве имен. Команда безопасности Google активно отслеживает шаблоны доступа и исследует необычные события.

Корпорация уделяет особое внимание защите накопителей, стараясь на аппаратном и программном уровне закрыть доступ к своим системам вредоносным скриптам или ПО иного типа. После списания накопители проходят многоэтапную процедуру очистки и проверки независимыми специалистами. Те устройства, которые не прошли процедуру очистки, уничтожаются физически.

Кроме этого, руководство Google решило полностью перенести в облачную инфраструктуру собственные корпоративные приложения. На данный момент в ней работает более 90 % ресурсов. При этом корпорация пересмотрела саму концепцию сети, уйдя от модели ее ограничения определенными границами, открыв для работы извне, и одновременно усилив меры защиты изнутри. Такая концепция получила название *BeyondCorp.* В этой сети доступ ограничивается не только для отдельных пользователей, но и для устройств. При наличии определенного уровня доступа, сотрудник получает возможность подключиться к корпоративной сети из любого места. Для ограничения уровня доступа используются разные методы аутентификации, авторизации и шифрования.

Таким образом, защита в корпорации Google разрабатывается в виде уровней – от физических компонентов и центра обработки данных до аппаратных, которые обеспечивают безопасность загрузки, межсервисной связи, данных пользователей, защищенного доступа к службам из Интернета, технологии действий сотрудников.

Литература

1. Защита информации в Google [Электронный ресурс]. – Режим доступа: https://cloud.google.com/security/security-design

УДК 658:004:316.3

КОНКУРЕНТОСПРОМОЖНІСТЬ ПІДПРИЄМСТВА В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

І. С. Московкіна

В умовах формування ринкової економіки, що передбачає самостійність підприємств у питаннях виробничо-господарської діяльності, для більшості з них актуальною стає проблема забезпечення конкурентоспроможності. Особливо ця проблема загострюється у зв’язку з наростанням невизначеності у зовнішньому середовищі підприємств та прагненням України до інтеграції в європейське й світове