ID, а на телефонах под управлением ОС Android это Fingerprint.

Алгоритмы реализации данной технологии в этих системах разные. Заранее скажу, что сканер отпечатков пальца на IOS на порядок лучше и гораздо труднее поддается взлому, чем аналогичная технология на Android-телефонах. Физически, эти сканеры реализованы по-разному, а также имеют разные способы шифрования самих сканов.

В телефонах компании Apple сканированный отпечаток пропускается через хеш-функцию и сохраняется в Secure Enclave – защищенном от доступа извне микрокомпьютере.

В телефонах под ОС Android до 6 версии операционной системы были даже такие казусы, как хранение сканов в памяти телефона, в незашифрованном виде, в общедоступной папке. С выходом Android 6.0 в Google не только разработали собственный API для аутентификации по отпечаткам пальцев, но и обновили Compatibility Definition Document, которому обязаны следовать все производители, желающие сертифицировать свои устройства для установки сервисов Google (это очень важный момент, о нем чуть позже).Было выпущено сразу два референсных устройства: Nexus 5X и Nexus 6P. В них – и неотключаемое шифрование раздела данных, и правильная реализация датчиков отпечатков, получившая название Nexus Imprint.

Сравнить безопасность Touch ID с ситуацией в мире Android не получится: если у Apple устройств единицы, то смартфонов на Android, наоборот, слишком много. В них могут использоваться самые разные датчики, основанные на разнообразных технологиях (от емкостных и оптических до ультразвуковых). Для разных датчиков подбирают разные технологии обхода. К примеру, для Samsung Galaxy S6 вполне срабатывает финт с разблокированием телефона моделью пальца, напечатанной на 3D-принтере из самого обычного пластика (с Apple Touch ID такой простой трюк не пройдет; для печати нужно будет использовать материал, обладающий особыми свойствами). Некоторые другие устройства легко обманываются распечатанными с высоким разрешением картинками. А вот сравнение с Nexus Imprint вполне имеет смысл. В Nexus 5X и 6P Google использовал образцово-показательный подход к безопасности. Это и неотключаемое шифрование раздела данных, и грамотная интеграция датчиков отпечатков, да и сами датчики выбраны не абы как. В устройствах сторонних производителей могут использоваться недостаточно безопасные датчики, могут зиять откровенные дыры в безопасности (несмотря на формальное соответствие требованиям Android Compatibility Definition). Дактилоскопическая аутентификация – не панацея. Ее основное предназначение не в том, чтобы сделать более безопасным конкретно твое устройство, а в том, чтобы снизить неудобства, связанные с безопасной блокировкой телефона, и таким образом убедить основную массу пользователей все-таки блокировать свои устройства.

АУДИТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ ЭЛЕКТРОННОГО БИЗНЕСА

Л.М. Лыньков, В.С. Князькова

Организация электронного бизнеса (ОЭБ) с точки зрения технического обеспечения представляет собой единое информационное пространство, интегрирующее в себя функциональные области маркетинга, производства, финансов, кадров и т.п. Комплексная оценка информационной инфраструктуры ОЭБ, в частности ее информационной безопасности (ИБ) организуется через аудит системы ИБ. К основным особенностям проведения аудита ИБ ОЭБ можно отнести следующие. Во-первых, ОЭБ представляет собой сложную и многоуровневую систему, включающую множество подсистем (функциональные области, например, финансы и маркетинг) и надсистем (например, контролирующие органы). Во-вторых, средой функционирования ОЭБ является сеть Интернет, использование которой привносит дополнительные риски для организации в силу ее общедоступности. В-третьих, в ОЭБ на первый план выходит обучение всех без исключения сотрудников как минимум основам ИБ. Согласно исследованию, проведенному в 2014 г. компанией Ernst & Young, 33% респондентов назвали именно персонал одним из основных источников угроз ИБ.

Обычно ОЭБ осуществляет свою деятельность через интернет-сайт. В таком случае при аудите системы ИБ необходимо оценить такие аспекты, как соответствие контента и

назначения веб-сайта заявленным в уставе организации вилам деятельности, сам веб-сайт (его дизайн, контент, СЕО-продвижение), поведение посетителей сайта, а также уязвимость по отношению к внешним и внутренним угрозам ИБ. Аудитору необходимо также оценить ИБ ОЭБ с точки зрения ИБ при идентификации и аутентификации клиентов и контрагентов, обеспечения целостности, доступности и конфиденциальности информации о бизнес-трансакциях, получения или осуществления переводов денежных средств и пр. В данном контексте аудит системы ИБ ОЭБ осуществляется с целью: оценки рисков, связанных с возможностью реализации угроз ИБ ОЭБ; оценки текущего уровня защищенности информационной системы ОЭБ; выявления «узких мест» в системе защиты ИБ; оценки соответствия информационной системы требованиям стандартом по ИБ; разработки рекомендаций по внедрению новых и совершенствованию существующих механизмов ИБ ОЭБ.

Литература

1. Overcoming compliance fatigue. Reinforcing the commitment to ethical growth. 13th Global Fraud Survey [Electronic resource]. – Mode of access: http://www.ey.com/Publication/vwLUAssets/EY-13th-Global-Fraud-Survey/$FILE/EY-13th-Global-Fraud-Survey.pdf. – Date of access: 10.05.2017.

2. Ситнов А.А. Особенности аудита электронного бизнеса / А.А. Ситнов // Аудитор. 2013. № 7.

ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ ОЦЕНКИ КОЛИЧЕСТВА ПРОСМОТРОВ ИНТЕРНЕТ-ПУБЛИКАЦИЙ

Т.Н. Михайлова, Д.В. Щегрикович

Продвижение публикаций в сети Интернет – сложная динамически развивающаяся отрасль. Авторам интернет-статей необходимо понимать возможности популяризации материала и быть уверенным в сохранности авторского права. Разработанное программное решение позволит журналистам и редакторам оптимизировать текст публикаций и сохранить уникальность своего материала, рекламодателям уменьшить затраты на рекламный бюджет, а содержателям новостных ресурсов расширить их функционал. Принцип работы описываемого подхода заключается в извлечении 120 признаков из текста публикации методами обработки естественного языка [1], описывающих ее морфологические, графематические, синтаксические, семантические и пунктуационные свойства [2]. Разработанная система представляет собой веб-ресурс, который на основе текста статьи предсказывает популярность публикации. Прогнозирование популярности представляет собой бинарную классификацию: отнесение потенциальной публикации к классу «Популярная публикация» – набранное количество просмотров за неделю – от 0 до 2500 просмотров, или «Не популярная публикация» – от 2500 просмотров за неделю [3, 4]. Достигнутая точность работы модели – 67 % правильно классифицированных объектов из тестовой выборки. Выделены значимые и не значимые признаки для популяризации новостной интернет-публикации на данном ресурсе [5]. Характеристики, которыми описывается текст с целью построения прогноза популярности можно использовать для сравнения публикаций на предмет похожести: высокое значение корреляции признаков двух статей свидетельствует о возможном незаконном использовании материалов. Такой способ позволит защитить авторское право, избежать плагиата, и, самое главное, – избежать использование видоизмененного текста, так как в отличие от систем антиплагиата, которые производят стандартное сравнение текстов, он позволяет произвести глубокую оценку их структуры: тональности, сложности, запутанности и мн. др.

Литература

1. Natural Language Processing and Text Mining / Edited by Anne Kao and Stephen R. Poteet. 272 p.

2. Stefan, T.H. Quantitative corpus linguistics with R.

3. Flah, P. Machine Learning: The Art and Science of Algorithms That Make Sense of Data / P. Flah. – 2015. – 400 p.

4. Duda, R.O. Pattern Classification / R.O. Duda, P.E. Hart, D.G. Stork. – NY.: John Wiley Sons, 2001. – 639 p.

5. Breiman, L. Out-Of-Bag estimation. Technical report, Statistics Department University of California / L. Breiman. – Berkeley, 1996.