стических и протекционистских настроений [1, с. 520]. Т. Пикетти подчеркивает, что без контроля политиков глобализация приведет не к объединению, а к уничтожению слабых стран сильными.

Книга «Капитал в XXI веке» вызвала неоднозначные оценки. Критика касается серьезных расхождений между данными книги и официальной статистикой, неточностями с определениями и первоисточниками и невнимания к «Капиталу» К. Маркса [2].

Вместе с тем высокую оценку получила сама постановка проблемы неравномерного распределения богатства и быстрого увеличения доходов некоторых классов общества. Книгу Пикетти охарактеризовали, как широкомасштабное исследование по проблемам неравенства [3].

Таким образом, Т. Пикетти рассматривает проблему неравенства распределения богатства на уровне неравноправия классов и стран, трактует ее как ключевое препятствие социально-экономическому прогрессу общества и для ее решения предлагает ряд экономических реформ. Они не являются чем-то принципиально новым (в XIX в. подобные меры совершенствования распределения богатства предложил Дж. Ст. Милль), однако приобретают новое звучание и актуальность в условиях современного этапа развития мировой экономики.

Литература

1. Пикетти, Т. Капитал в 21 веке / Т. Пикетти. — Москва: Ад Маргинем Пресс, 2015. — 592 с.

2. Data problems with Capital in the 21st Century [Electronic resource]. — Mode of access: http://piketty.pse.ens.fr/files/capital21c/en/media/FT23052014c.pdf. — Date of access: 18.03.2016.

3. Why We're in a New Gilded Age [Electronic resource]. — Mode of access: http://www.nybooks.com/articles/archives/2014/may/08/thomas-piketty-new-gilded-age/. — Date of access: 18.03.2016.

Защита банковских сайтов

Ткач А. О., Чикулова А. С., студ. II к. БГЭУ,
науч. рук. Акинфина М. А., канд. физ.мат. наук, доц.

В мире интенсивного развития информационных технологий и глобальной сети Интернет под угрозой разного рода хакерских атак находятся любые сайты, программные комплексы и системы, в том числе и банковские. Так, за последние несколько лет злоумышленники атаковали такие банки и платежные системы, как Европейский центральный банк, Приватбанк и Биткойн.

Проанализировав деятельность хакеров, можно выделить две основные причины, которые движут киберпреступниками: личное обогащение и политические мотивы.

Прежде чем рассматривать способы защиты банковских веб-сайтов, необходимо рассмотреть, какие именно угрозы банкам и их клиентам могут нести киберпреступники, атакующие корпоративные сайты:

1. Кража информации о юридических и физических лицах. Это одна из самых актуальных проблем для банков, так как с ростом популярности электронных сервисов растет объем информации, которую клиенты оставляют в данном банке. Однако быстро растет и число злоумышленников, которые хотят получить доступ к этой информации. И зачастую именно сайты становятся самым легким объектом для атаки;

2. Отказ в работе систем. Атака на ресурсы банка может привести к повышенной нагрузке и в результате отказу систем, когда пользователи не могут воспользоваться ни сайтом банка, ни другими сервисами;

3. Доступ посторонних лиц к внутренним банковским системам. Если сайт не защищен должным образом, то он становится уязвимым для хорошо подготовленных киберпреступников;

4. Проблема репутации банка. Независимо от того, что произошло с сайтом, серьезный урон будет нанесен именно репутации банка. «Если банк не смог защитить даже собственный сайт, сможет ли он защитить мои деньги и информацию?» — это ключевой вопрос, который наглядно иллюстрирует эту проблему [1].

К сожалению, злоумышленники обычно являются профессиональными программистами и экономистами. Поэтому для обеспечения безопасности банковского сайта необходимо подходить комплексно и подключать все имеющиеся механизмы.

Механизмы и процессы, необходимые для защиты банковских сайтов, можно разделить на две группы: функционирование и администрирование сайта.

Функционирование сайта включает следующие инструменты:

1. Сервера, на которых расположен сайт банка. Имеются два варианта защиты серверов, каждый из которых имеет свои достоинства и недостатки: сторонний хостинг, сопровождающийся профессиональной техподдержкой, круглосуточной работой профессионалов, и собственные сервера банка, обеспечивающие полный контроль над сайтом и его работой.

• Система управления сайтом. В случае с банковскими сайтами предъявляются следующие требования к этой системе: защищенность, постоянные обновления системы ее разработчиком, гарантия, техподдержка, сертификаты соответствия;

• Компетенция компании-разработчика. Безопасность может нарушаться уже при самой разработке сайта, поэтому необходимо тщательно выбирать

разработчиков, имеющих соответствующий сертификат и опыт разработки подобных сайтов;

• Проактивная защита. На любом этапе работы с сайтом является необходимым просчитывать все угрозы заранее и разрабатывать механизмы по их предотвращению;

• Мониторинг состояния сайта и активности вокруг него. Атаку злоумышленников часто можно предотвратить, зафиксировав подозрительную активность вокруг сайта и ограничив ее. Такие инструменты могут быть подключены на различных уровнях либо предусмотрены в выбранной системе управления сайтом;

• Передача данных. Крайне важно настроить защиту на каждом этапе этого процесса: сертификаты безопасности на самих страницах, где клиенты заполняют форму, шифрование передаваемых в банк данных, хранение полученной и расшифрованной информации на защищенных серверах внутри банка, отсутствие возможности передачи этих данных «наружу», в Интернет [1].

2. Администрирование сайта является чуть ли не самым важным элементом в работе по обеспечению безопасности банковских сайтов, ведь даже самые совершенные инструменты по работе и защите сайтов не учитывают человеческий фактор. Имеется как минимум пять четко выделенных инструментов, обеспечивающих эффективное управление сайтом: разделение ролей и ограничение доступа, четкие процедуры, физические ограничения доступа к системе управления сайтом, современные браузеры для администраторов сайтов, безопасность компьютеров администраторов и соответствующее обучение.

Каждый из этих способов является очевидным, но не всегда имеется возможность использовать их в совокупности, однако только все вместе они дают нужный результат.

Литература

1. Безопасность банковских сайтов: проблемы и решения [Электронный ресурс]. — Режим доступа: http://www.nbrb.by/bv/articles/10158.pdf. — Дата доступа: 29.04.2016.

Финансовый лизинг в Республике Беларусь: проблемы и направления развития

Ткачук И. С., студ. III к. БГЭУ,
науч. рук. Сидорова А. В., ассистент

В условиях становления рыночных отношений в Республике Беларусь и острой необходимости ускоренной модернизации устаревшей материаль-