УДК 004.056:005.922.1:334

О. В. Пугачева
OPugacheva@gsu.by
Гомельский государственный университет им. Ф. Скорины, Беларусь

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ БЕЛАРУСИ

Исследуются основные проблемы обеспечения кибербезопасности белорусского бизнеса, анализируются существующие угрозы и меры противодействия им.

Республика Беларусь заняла 39-е место из 165 в Глобальном рейтинге кибербезопасности (Global Cybersecurity Index 2017), составленном Международным союзом электросвязи и ABI Research.

Глобальный индекс кибербезопасности (GCI) отражает уровень киберзащищенности государств и усилия, которые прилагает страна для его улучшения. При составлении GCI учитывается уровень обязательств в 5 сферах – правовые, технические меры, организационные, развитие потенциала и международное сотрудничество.

Лидерами рейтинга кибербезопасности являются Сингапур, США, Малайзия. Китай занял 32–е место, Польша – 33–е. Республика Беларусь с индексом 0,59 заняла 39–е место в общем рейтинге (таблица 1) и 3–е среди стран СНГ.

Таблица 1 – Место Республики Беларусь в Глобальном рейтинге кибербезопасности в 2017 году

Страна	Законода-тельство	Технические меры	Организационные меры	Потенциал	Международное сотрудничество	Итого
Сингапур	0,95	0,96	0,88	0,97	0,87	0,92
США	1	0,96	0,92	1	0,73	0,91
Малайзия	0,87	0,96	0,77	1	0,87	0,89
Эстония	0,99	0,82	0,85	0,94	0,64	0,84
…						
Грузия	0,91	0,77	0,82	0,9	0,7	0,81
Россия	0,82	0,67	0,85	0,91	0,7	0,78
Беларусь	0,85	0,63	0,33	0,68	0,47	0,59

Среди постсоветских стран наилучших результатов добились Эстония, занявшая 5-е место, Грузия – 8-е и Россия – 10-е (0,78). Латвия заняла 22-е место, Литва – 57-е, Азербайджан – 48-е, Украина – 59-е, Молдова – 73–е, Казахстан – 83-е, Таджикистан – 91-е, Узбекистан – 93-е, Армения – 111-е, Туркменистан – 132-е. Замыкают список в Глобаль-ном рейтинге кибербезопасности Экваториальная Гвинея, Йемен и ЦАР [1].

Республика Беларусь традиционно занимает высокие позиции по уровню риска заражения через интернет, которому подвергаются компьютеры пользователей в разных странах мира. По данным Kaspersky Security Network, 27 % белорусских пользователей столкнулись со срабатыванием веб–антивируса. Таким образом, страна оказалась на 8-м месте в рейтинге стран с наибольшим риском заражения через интернет [2].

Является очевидным, что в отдельно взятой стране невозможно построить безопасный интернет, поскольку современные угрозы транснациональны. Поэтому в Беларуси выстраивается система работы в этой области на основе международных практик, внедряются правовые акты, которые определяют, как на рынке действуют те или иные компании.

Так, в 2010 г. в Беларуси появился институт уполномоченных поставщиков интернет–услуг – провайдеров, которые оказывают услуги для госорганов (хостинга и передачи данных). Они должны выполнять ряд требований по безопасности, которые корректируются в зависимости от существующих угроз. Эта система позволяет каждому из них создать базовую модель безопасности и предоставлять через нее безопасные услуги.

В Беларуси появилась команда реагирования на компьютерные инциденты – Cert.by, через которую ведется взаимодействие с аналогичными командами во всем мире. Происходит обмен информацией о текущих угрозах, взаимодействие в части предупреждения. На территории Европы нет проблем при взаимодействии в юридическом или техническом плане. Но когда поддержка нужна специалистам другой страны, тех же США, Австралии, Беларуси, то возникают проблемы юридического характера. Сегодня важный международный документ в этой сфере – Будапештская конвенция киберпреступности, и, несмотря на то, что некоторые страны не хотят ее ратифицировать, это реально работающий правовой инструмент. Белорусское уголовное законодательство практически полностью повторяет Будапештскую конвенцию.

С целью обеспечения кибербезопасности Нацбанк Республики Беларусь объявил о создании центра мониторинга и противодействия компьютерным атакам в кредитно–финансовой сфере (FinCERT) по примеру российских и прочих зарубежных коллег. Опыт работы в белорусской банковской сфере, в т.ч. по вопросам информационной безопасности, подсказывает, что при создании подобной структуры придется столкнуться с рядом проблем.

Любой банк крайне зависим от своих информационных систем и информационной инфраструктуры. Если одновременно будут атакованы все серверы какого-нибудь крупного банка, это будет коллапс с огромными потерями. Поэтому естественно желание регулятора как–то стандартизировать работу информационных систем и, главное, – отслеживать любые

инциденты, влияющие на их работу. В целом процедура мониторинга описана в ТКП 288–2010 (07040) «Банковские технологии. Управление рисками в сфере информационных технологий» и содержит перечень типовых источников (причин) рисков в сфере информационных технологий, по которым каждый банк отчитывается перед регулятором. На деле отдел рисков банка отсылает профильным руководителям (IT и информационная безопасность чаще всего) формы таблиц, которые те с определенной периодичностью заполняют. Отдел рисков консолидирует эту информацию и отсылает регулятору.

На этом этапе обеспечения кибербезопасности возникают следующие проблемы [3]. Во–первых, они связаны с самой процедурой мониторинга событий, будь то шпионаж, хищение активов, утечка информации и т.п. Их отслеживание требует серьезных и дорогостоящих систем. Например, DLP (Data Leak Prevention) системы, SIEM (security information and event management), организованы SOC (Security Operation Center) и другие. Любая из них стоит сотни тысяч долларов. Далеко не у всех белорусских банков они есть. Но без них нельзя эффективно собирать данные о проблемах в информационных системах и предоставлять регулятору полные и точные сведения.

Во–вторых, кадровая проблема. Обучить специалиста пользованию сложными SIEM–системами стоит около 4 тыс. у.е. Соответственно, таких людей на рынке крайне мало и стоят они дорого. Даже если банк оплатит учебу для своего сотрудника, это не значит, что он станет платить ему зарплату в соответствии с ее рыночным уровнем.

Третья и наиболее важная проблема в том, что банки не хотят делиться информацией об инцидентах и проблемах, опасаясь внеплановых проверок регулятора или иных неприятностей.

Работа создаваемого центра должна быть направлена по следующим типам инцидентов:

– DDoS–атаки (хакерские атаки на вычислительную систему с целью довести её до отказа);

– несанкционированный доступ к конфиденциальной информации;

– мошеннические SMS и звонки;

– вредоносное программное обеспечение (ПО).

Направлений может быть больше, вплоть до поиска уязвимостей в инфраструктуре отдельных банков [4].

Предполагается, что специалисты FinCERT будут проводить мониторинг ситуации в интернете, СМИ, по любым открытым и закрытым источникам, оперативно получать информацию от профильных силовых структур, получать информацию от банков, которые подверглись атакам. На основании собранной информации должны формироваться рекомендации по борьбе с этими атаками и инцидентами, а также оперативно рассылаться по всем, кто будет подключен к системе.

Однако по–прежнему сохраняются те же проблемы.

Во-первых, не ясно, как эффективно консолидировать информацию, поскольку нет уверенности, что в этом согласятся участвовать специалисты по расследованию преступлений против информационной безопасности и интеллектуальной собственности главного следственного управления СК Республики Беларусь или Оперативно-аналитического центра при Президенте (ОАЦ), да и банки будут крайне неохотно предоставлять информацию об инцидентах.

Во-вторых, кадровый вопрос. Хороший специалист по кибербезопасности стоит на рынке 2–3 тыс. у.е., профильный руководитель – около 5 тыс. у.е. Даже если найдутся молодые талантливые кадры или эти места займут представители спецслужб, то их придется обучать и мотивировать. Но нельзя исключать того, что через некоторое время эти работники начнут уезжать в западном или восточном направлении, туда, где спрос на таких специалистов и их заработки выше.

Таким образом, кибербезопасность – понятие комплексное. Для ее обеспечение необходима специальная работа, в том числе через законодательство и реализацию политики безопасности.

Литература

1. Measuring the Information Society ICT Opportunity Index and World Telecommunication/ICT Indicators – 2017 – Сайт Международного союза электросвязи [Электронный ресурс] – Режим доступа: http://www.itu.int/en/publications/Pages/default.aspx. – Дата доступа: 4.07.17.

2. Информационная безопасность бизнеса [Электронный ресурс]. – Режим доступа: http://media.kaspersky.com/pdf/it_risk_report_russia_2014.pdf. – Дата доступа: 5.07.17.

3. «Безопасность в Интернете» Форум по управлению интернетом (Belarus IGF–2017) –

[Электронный ресурс] – Режим доступа: https://igf.by/BelarusIGF–2017.pdf. – Дата доступа: 24.09.17.

4. XIV Международный форум по банковским информационным технологиям "БанкИТ'2017")

– [Электронный ресурс] – Режим доступа: http://bankit.it–event.pro/. – Дата доступа: 24.09.17.