Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

Анализ киберугроз и перспективы информационной безопасности для бизнеса в России

Научный руководитель – Крючкова Кристина Юрьевна

Омарова Милана Вугаровна

Студент (специалист)

Российская правовая академия МЮ РФ, Северо-Кавказский филиал, Юридический факультет, Махачкала, Россия

E-mail: omarovamilana333@gmail.com

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере от случайных или преднамеренных воздействий, которые могут нанести неприемлемый ущерб субъектам информационных отношений, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Результаты исследований, проведенных "Лабораторией Касперского" совместно с агентством "B2BInternational" в 14 странах мира, показали, что уровень угроз в сфере информационной безопасности крайне высок. В России доля компаний, сталкивающихся с киберугрозами, достигает 98%. Внешние и внутренние атаки приводят к риску и фактической потере интеллектуальной собственности, данных об осуществленных платежах, личной информации о сотрудниках.

Еще одной причиной низкой степени защищенности от киберугроз, помимо нежелания уделять им внимание, является несоответствие выбранных мер защиты характеру опасности.

Согласно мнению участников опроса, информационная стратегия должна являться частью глобальной стратегии организации, наряду с финансовой, кадровой и маркетинговой. А главной задачей IT-департамента должно быть обеспечение бесперебойной работы качественной системы информационной безопасности[1].

Наиболее опасными действиями пользователей в России считаются активности в социальных сетях и создание общего доступа к файлам[2]. Компания Group-IB, специализирующаяся на предотвращении киберпреступлений, 9 октября представила отчет , согласно которому годовой ущерб финансовой сферы России от таких инцидентов составил 2,96 млрд руб.

Затраты на обеспечение корпоративной информационной безопасности составляют в среднем 8 000 долл. в год для малого бизнеса, 80 000 долл. для среднего бизнеса и 3,2 млн долл. для крупных компаний. Большинство участников опроса считают бюджет, выделяемый на информационную безопасность, недостаточным и требующим увеличения.

В России только 36% опрошенных считают уровень вложений достаточным, причем имеет место нехватка не только финансовых, но и кадровых и системных ресурсов. В мире этот показатель достигает 55%. По мнению 95% сотрудников IT-департаментов, инвестиции в информационную безопасность необходимо увеличить на четверть и более. Одно из громких киберпреступлений последнего времени «Международная группировка хакеров (Carbanak) из России, Китая и стран Европы похитила со счетов клиентов банков около $300 млн, в феврале 2015 года. Жертвами хакеров стали клиенты более 100 банков и других финансовых институтов в 30 странах мира. Согласно сообщению издания, большинство пострадавших банков находится в России, хакерам также удалось взломать

системы финансовых организаций Японии, Соединенных Штатов и Европы. Это мошенничество может оказаться одной из крупнейших банковских краж в истории, совершенной «без обычных признаков ограбления».[3]
Для улучшения ситуации в будущем потребуются существенные инвестиции, увеличение численности IT-персонала и использование новейших технологий.[4]

Мы полагаем , что при управлении системами безопасности в России большая часть мероприятий связана с потерями из-за киберугроз. Для решения данных проблем компании ориентируются на сотрудничество с интегратором комплексных решений, антивирусного, антиспамового и антифишингового назначения и обучения персонала для предотвращения риска потерь. Выступавший на конгрессе глава Сбербанка Герман Греф предупредил, что в 2022 году общие потери от кибератак могут достигнуть $8 трлн.

Учитывая постоянный транснациональный рост и масштабность киберугроз, а также глобальность негативных последствий в информационной сфере от их проведения, считаем, тенденции по созданию информационно-коммуникационных систем ограниченного доступа будут только нарастать. В результате количество государств, вводящих различные законодательные ограничения на «проникновение» в их информационное пространство неизбежно приведет к разработке еще более эффективных технологий хакерских атак[5].

Поэтому полагаем, в целях обеспечения национальной безопасности государств, сокращение количества и разрушительной силы киберугроз, особенно в части, касающейся экономической инфраструктуры, в первую очередь критически важных объектов других государств необходима консолидация усилий международного сообщества, направленная на решение проблемы по разработке и принятию в рамках ООО Конвенции информационной безопасности.

Если этого не произойдет, то данное, на наш взгляд, обстоятельство станет дополнительным основанием для создания в развитых с точки зрения внедренных IT-технологий странах национальных систем обеспечения информационной безопасности и разделения сети Интернет на отдельные части.

Уважаемые участники конференции, для выхода на новый уровень развития нам нужны собственные передовые разработки и научные решения. А для этого необходимо сосредоточиться на направлениях, где накапливается мощный технологический потенциал будущего, а это цифровые технологии.

Ведь вопрос национальной безопасности и технологической независимости России, в полном смысл этого слова- наше будущее.

Источники и литература

1) Баранова Е.К. Информационная безопасность и защита информации: М.: РИОР; Инфра-М, 2014.

2) Башелханов И.В. Кибервойны будущего - к чему готовиться законодателям и корпорациям // Информационная безопасность. 2014.

3) ТелеканалRBC:https://www.rbc.ru/technology_and_media/15/02/2015/54dffd599a79473e130611994.

4) Мельников В.П. Информационная безопасность: М.: Академия, 2013

5) Оганесян А.Г. Финансовая выгода VS информационная безопасность при ИТ-аутсорсинге: как найти баланс? // Банковское дело. 2011.