Секция «Особенности аудита организации с цифровыми ресурсами: угрозы и информационная безопасность»

Киберпреступность в банковской сфере как угроза экономической безопасности

Научный руководитель – Долбилов Алексей Владимирович

Зинченко Дарья Игоревна

Студент (специалист)

Московский университет Министерства внутренних дел Российской Федерации, Москва, Россия

E-mail: zinchenko-dashulya@mail.ru

Мы живем в период информационного общества, когда компьютеры и телекоммуникационные системы охватывают все сферы жизни людей и стран. Но человечество, используя телекоммуникации и глобальные компьютерные сети, не представляет, какие возможности для злоупотребления создают данные технологии. На сегодняшний день потерпевшими от злоумышленников, орудующих в пространстве Интернета, становятся не только люди, но и целые экономические системы государств. При этом безопасность огромного числа пользователей оказывается в зависимости от нескольких преступников. Число киберпреступлений растет пропорционально числу пользователей компьютерных сетей, и, по данным Интерпола, темпы роста преступности, например, в глобальной сети Интернет, являются самыми быстрыми на планете.

Угрозу атак киберпреступников как для всего мира, так и для России признают и российские органы охраны правопорядка. Так, согласно данным Главного управления специальных технических мероприятий МВД России, преступность в сфере высоких технологий в настоящее время является одной из значимых угроз национальной безопасности Российской Федерации в сфере информации.

Также эксперты Центра информационной безопасности ФСБ России прогнозируют рост количества киберпреступлений в отношении российских финансовых учреждений. К примеру, в конце 2015 и в начале 2016 года отметился рост хищений денежных средств путем заражения вредоносным программным обеспечением автоматизированных рабочих мест. В результате пострадало свыше ста банков и нанесен ущерб более десяти миллиардов рублей. Эксперты ФСБ отмечают, что в целом по миру количество взломов банковских систем и хищений тоже увеличилось. Однако, по оценкам международных экспертов, основное количество подобных преступников находится на территории Российской Федерации и стран СНГ.

Оценим ущерб, который приносят преступления в сфере информационных технологий. Если смотреть на цифры, то ущерб всей российской экономике от киберпреступников в 2015 году составил 0,25% от ВВП. Это в 2 раза больше всего российского рынка интернет-рекламы, почти половина капитализации компании "Яндекс", треть отечественного ИТ-рынка и почти половина всех расходов на здравоохранение, выделенных из бюджета РФ в 2015 году! Потери от киберпреступлений достигли 22,8% от бюджетных ассигнований на исследовательскую деятельность. Это фантастические цифры. Маленькие компании из-за действий преступников недополучают выручку и теряют репутацию, крупный бизнес - теряет деньги, что негативно влияет на их инвестиции в развитие. Киберугрозы серьезным образом сдерживает развитие отечественных инноваций.

Для того, чтобы обеспечить кибербезопасность Российской Федерации в стране действует Доктрина Информационной безопасности, для организации предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере высоких технологий, а

также защиты российских военных систем управления и связи от кибертерроризма функционируют специальные подразделения МВД и Министерства обороны, в свою очередь для регулирования, контроля и надзора в сфере информационных технологий осуществляют свою деятельность ФСБ, ФСТЭК, Министерство связи, Роскомнадзор и ЦБ РФ. Но несмотря на все меры, принимаемые государством для предотвращения преступлений в сфере высоких технологий, существует ряд проблем обеспечения кибербезопасности в России, такие как: несовершенность законодательной базы и правоприменительной практики, несоответсвие системы подготовки кадров существующим трендам и угрозам, отсутствие сертификации специалистов и институтов, низкая компьютерная грамотность и осведомленность массовых категорий населения и менеджмента о киберугрозах, которая создает благодатную основу для их реализации в масштабах, угрожающих устойчивости страны.

Поэтому деятельность государственных органов в области кибербезопасности требует координации и налаживания партнёрства с бизнесом - постоянный обмен с поставщиками услуг, банками, ИТ-компаниями информацией, необходимой для отражения кибератак. Также необходимо совершенствование правовой базы в области информационной безопасности, в силу значимости проблемы кибератак имеет место выделение отдельного раздела закона. Для обеспечения кибербезопасности частных пользователей необходимо планирование и развёртывание обучения специалистов, сертификация специалистов, а также информирование интернет-пользователей об угрозах. Эффективная борьба с киберпреступностью возможна только при взаимодействии государства, бизнеса и гражданского общества.

Источники и литература

1) Доктрина информационной безопасности Российской Федерации (Утверждена Указом Президента Российской Федерации от 05.12.2016 № 646)
2) Официальный сайт Центрального банка Российской Федерации // www.cbr.ru
3) Сайт Лаборатории Касперского // http://www.kaspersky.ru
4) Сайт РИА Новости // https://ria.ru/economy