УДК 681.3.67

ТЕНДЕНЦИИ В СТРУКТУРЕ УГРОЗ И РИСКОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фильштинский С.В. (Мельбурн, Австралия)

Считается общепризнанным, что в настоящее время целью большинства атак на системы информационной безопасности являются, в конечном итоге, деньги, в то время как несколько лет назад основной целью атак был престиж в узких кругах хакеров.

Это изменение произошло несколько лет назад. С одной стороны большое количество уязвимых систем в Интернете породило рынок предложений на украденную информацию, и в первую очередь на легко превращаемые в реальные деньги номера кредитных карточек. С другой стороны появление торговых платформ для торговли такой информацией привлекло любителей быстрых денег со всего мира и тем самым создало огромный спрос. Это обстоятельство до сих пор поддерживает чрезвычайную устойчивость криминальных торговых площадок, несмотря на непрерывную охоту на них со стороны мощнейших государственных спецслужб, структур безопасности ведущих платежных систем и корпораций.

Система торговых площадок, созданная для операций с краденными кредитными карточками привлекла к себе другие виды мошенничества – фишинг (phishing), кража личной информации с целью мошенничества (identity theft), шантаж.

Торговые площадки изменили те виды мошенничества, которые ранее требовали объединения в

одной группе лиц специалистов разного профиля, таких как

- хакеры
- спамеры
- программисты
- специалисты в банковском деле
- специалисты по отмыванию денег.

Возникло разделение труда, специализация, рынок услуг. Компьютерное мошенничество вошло в индустриальных век.

Это важно понимать, оценивая уровни рисков в области информационной безопасности.

Если раньше, к примеру, база данных клиентов компании представляла интерес только для прямых конкурентов, то теперь любая ценная информация превратилась в высоколиквидный товар, который можно с легкостью продать за реальные деньги.

В докладе предлагается:

- оценивать риски с учетом повышения вероятности их реализации;
- искать меры защиты, которые бы работали против используемой киберпреступниками бизнес - модели;
- не ограничивать способы защиты техническими методами, а также применять меры организационного характера.