Секция «Аудит организаций с цифровыми ресурсами и использующих криптовалюты: сетевые угрозы и информационная безопасность»

Организационно-правовые основы повышения культуры информационной безопасности личности в условиях интенсификации угроз новейшего типа

Научный руководитель – Морозов Андрей Витальевич

Козырева Анна Александровна

Аспирант

Академия гражданской защиты Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Московская область, Россия

E-mail: a.kozyreva@amchs.ru

В условиях интенсивного развития информационного пространства, а именно в условиях динамичности и трансграничности процесса обмена информацией, открываются широкие возможности для интенсификации угроз и вызовов новейшего типа, направленных на уязвимый субъект информационных отношений - личность.

В связи с этим, актуальным является рассмотрение вопроса формирования организационно-правовых основ обеспечения личной информационной безопасности и повышения правовой грамотности личности, как субъекта информационных отношений. Изучением данного вопроса, занимаются различные гуманитарные и технические науки, каждая со своей стороны. Но основные концептуальные моменты заложены в политико-правовых документах, принятых за последние годы. Одним из таких документов является Доктрина информационной безопасности (далее - Доктрина), утвержденная Указом Президента РФ от 5 декабря 2016 г. №646, в которой отмечаются основные национальные интересы в информационной среде, основные информационные угрозы и состояние информационной безопасности, определяются стратегические цели, основные направления и организационные основы обеспечения информационной безопасности. Впервые в данном документе акцентируется внимание на том, что состояние информационной безопасности в области образования характеризуется низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности [1]. Следующим основополагающим документом стала Стратегия развития информационного общества на 2017-2030 годы (далее - Стратегия), утвержденная Указом президента 10 мая 2017 года [2]. В данном документе, изложены цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и телекоммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Одной из основных угроз информационной безопасности в данных документах признана киберпреступность. На сегодняшний день надо признать тот факт, что масштабы компьютерной преступности возрастают прежде всего в кредитно-финансовой сфере, зачастую нарушении прав и свобод человека и гражданина в области защиты персональных данных, при этом способы и средства совершения преступных деяний становятся все изощрённее. По данным Лаборатории Касперского финансовое мошенничество стало одной из наиболее распространенных угроз информационной безопасности, что указано в работе Тарасова А.М.: «примерно 20 % российских интернет-пользователей при совершении банковских операций и онлайн-покупок как минимум два раза становились жертвами киберпреступников, теряя при этом денежные средства» [3]. Подобная проблема существует и при обработке персональных данных использовании различных сервисов в сети Интернет.

Для предотвращения подмены, искажения или блокирования информации новая Стратегия предполагает использование российских криптоалгоритмов и средств шифрования при взаимодействии органов власти между собой, а также с гражданами и организациями. Предполагается, что для предоставления безопасных услуг и программного обеспечения в отечественных информационно-телекоммуникационных системах будут использоваться встроенные средств защиты информации.

Классификация вызовов и угроз информационной безопасности личности представлена в диссертационном исследовании доктора юридических наук Чеботаревой А.А., в основу которой положены такие критерии как цель, источник угрозы, характер воздействия. В отдельную категорию угроз выделены угрозы новейшего типа, к которым относятся:

- угрозы, исходящие от специальных файлов куки (от англ. Cookie);

- угрозы, направленные на трафик виртуальной валюты Bitcoin;

-угрозы конфиденциальности данных вследствие новейших технологий онлайн- рекламы Real-TimeBidding (RTB).

Данный список не является исчерпывающим, т.к. разнообразие вызовов и угроз пополняется вследствие развития цифровой экономики, к которым можно отнести фишинг, кардинг, скимминг. Также особого внимание заслуживают формы информационной угрозы личности, такие как кибербуллинг (киберзапугивание), целенаправленное дезинформирование, интернет-моббинг[5]. Молодежный парламент при Государственной Думе РФ выступил с инициативой установить административную ответственность за массовую травлю в общественных местах и социальных сетях. Председатель Молодежного парламента при Государственной думе Мария Воропаева пояснила, что предлагаемая мера направлена в первую очередь против таких явлений, как кибербуллинг и интернет-моббинг. Под этими терминами подразумевают организованную травлю, оскорбления, угрозы и публикацию компрометирующих материалов о человеке в виртуальном пространстве. Так как агрессия распространяется в сети, ее тяжело ограничить, в нее вовлекается множество людей, а установить личности обидчиков зачастую невозможно.

Данная инициатива безусловно является актуальной и в случае принятия поправок к действующему законодательству позволит минимизировать данный вид информационной угрозы личности, но нет гарантии, что на смену кибербуллингу и интернет-моббингу не придет еще более современный, не подпадающий по регулирование нормами права способ воздействия на личность, при котором не возможно будет чувствовать себя в безопасности в сети. Именно поэтому, формирование правовой культуры информационной безопасности личности является приоритетным направлением в развитии безопасного информационного пространства.

В условиях закрепленных правовых основ в Концепции информационной безопасности детей (далее - Концепция)[6] , предполагается, что в 2020 году в России сформируется поколение молодых граждан, которые смогут свободно и самостоятельно ориентироваться в современном информационном пространстве и будут осознанными и ответственными субъектами информационных отношений. В связи с этим создание новых механизмов партнерства с участием всех институтов общества призваны выработать систему доверия в сети "Интернет", гарантирующую конфиденциальность и личную безопасность пользователей, конфиденциальность их информации и исключающую анонимность, безответственность пользователей и безнаказанность правонарушителей в сети Интернет . Стратегические политико-правовые документы позволяют переходить из состояния «догоняющего» нарушителей в состояние «предвосхищающих» правонарушения, путем формирования правовой культуры информационной безопасности личности, повышая уровень правосознания личности в информационной сфере.

Источники и литература

1) Доктрина информационной безопасности, утверждена Указом Президента РФ от 5 декабря 2016 года №646
2) Стратегия развития информационного общества на 2017-2030 годы, утверждена Указом Президента РФ от 10 мая 2017 года №203
3) Тарасов А.М. Киберугрозы, прогнозы, предложения // Информационное право. – 2014. - №3. – С.12.
4) Чеботарева А. А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе / докторская диссертация по специальности 12.00.13 - «Информационное право» [Электронный ресурс] Режим доступа: http://www.igpran.ru/prepare/board/4381/?id=3465?id=3465(дата обращения 15.02.2018)
5) В Госдуме предложили установить ответственность за травлю в соцсетях. [Электронный ресурс]Режим доступа: https://inetsafety.ru/v-gosdume-predlozhili-ustanovit-otvetstvennost-za-travlju-v-socsetjah/ (дата обращения 07.03.2018)
6) Концепция информационной безопасности детей, утвержденная Распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р / Официальный интернет-портал правовой информации http://www.pravo.gov.ru (дата обращения 11.03.2018)