Д. В. Денисов, *канд. экон. наук, доцент, Университет «Синергия», г. Москва, Ddenisov@mfpa.ru*

Безопасность в Интернете: защита от внешних угроз

В данной статье рассматриваются актуальные внешние угрозы, связанные с использованием Интернета, при этом делается акцент на «криминализации» глобальной сети и угрозах, представляющих опасность для финансов, жизни, здоровья и психического состояния пользователей. Далее рассматриваются основные активы пользователей, подвергающиеся угрозам, и соответствующие средства защиты: программные, организационные и правовые.

Ключевые слова: Интернет, спам, фишинг, угроза, сетевая атака, компьютерный вирус, DDOS, интернет-мошенничество, троллинг, кибербуллинг, секстинг, груминг, социальная сеть, пароль, аккаунт, антивирус, родительский контроль, управление «К» МВД РФ.

Введение

Говоря о способах, методах и средствах обеспечения безопасности в Интернете, следует определиться с основными понятиями и их трактовкой. В данной статье будет использоваться самое широкое понимание термина *безопасность* как состояния защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз. Поскольку *угроза* представляет собой потенциально или реально существующие воздействия, приводящие к материальному или моральному ущербу, то логично начать с определения угроз, присущих Интернету. Принято выделять внешние и внутренние угрозы. Данный материал будет посвящен анализу и определению способов противодействия внешним угрозам, а следующая публикация — внутренним.

Особое внимание уделим относительно новым внешним угрозам, связанным с активным развитием социальных сетей, средств социальной инженерии, а также «криминализацией» Интернета.

Выделяют следующие способы защиты информации:

- *предупреждение угроз* — превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
- *выявление угроз* выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;
- *обнаружение угроз* имеет целью определение реальных угроз и конкретных преступных действий;
- *локализация* преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;
- *ликвидация* последствий угроз и преступных действий и восстановление статус-кво.

В данной статье рассмотрены действия по обнаружению внешних угроз в Интернете, их локализации и ликвидации последствий.

Условно внешние угрозы можно разделить на «традиционные» и «новые». К «традиционным» внешним угрозам можно отнести спам, фишинг, компьютерные вирусы, троянские программы и сетевые атаки [1]. В рамках данной статьи будут рассматриваться только «новые» внешние угрозы.