ОСОБЕННОСТИ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ «СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Лыньков Л.М., Борботько Т.В., Тимофеев А.М.
Учреждение образование «Белорусский государственный университет информатики и радиоэлектроники» (г. Минск)

В настоящее время весьма сильное влияние на формирование и развитие современного информационного общества оказывают системы социальных отношений, управление которыми осуществляется посредством оказания информационно-психологического воздействия. Применение социально-психологических средств и методов воздействия с использованием современных технических каналов связи и телекоммуникаций привело к тому, что информационное пространство социальных систем является одним из основных инструментов как для обмена социально значимой информацией, так и для несанкционированного доступа к ней [1-3]. В этой связи при подготовке специалистов в области информационной безопасности представляется весьма важным не только изучение теоретических основ, но и получение практических навыков обеспечения информационной безопасности в социально-психологической сфере, что являлось целью данной работы.

Определены основные направления и технологии социально-психологических воздействий на различные слои человеческого общества, изучение которых позволит специалистам в области информационной безопасности получить навыки, необходимые для выработки методов и средств их противодействию.

Изучение в рамках практических занятий системы обеспечения национальной безопасности Республики Беларусь позволяет установить внутренние и внешние источники угроз национальной безопасности в социальной и информационной сферах, а также основные направления нейтрализации этих угроз.

Проведение диагностик по установлению различных особенностей нервной системы человека, а также его поведения, психического состояния, личностных качеств, логичности мышления, темперамента и эмоциональной устойчивости позволяет развить механизмы информационно-психологической защиты личности.

Разрабатываемые в рамках самостоятельной работы студентов программные комплексы могут быть использованы для диагностики силы, уравновешенности и подвижности нервной системы личности, а также для оценки уровня ригидности, конфликтности/тактичности и потребностей в саморазвитии.

Литература

1. Кузнецов, М.В. Социальная инженерия и социальные хакеры / М.В. Кузнецов, И.В. Симдянов. – СПб.: БХВ-Петербург, 2007. – 368 с.

2. Астахова, Л.В. Критическое мышление как средство обеспечения информационно-психологической безопасности личности: монография / Л.В. Астахова, Т.В. Харлампьева; под ред. Л.В. Астаховой. – М.: РАН, 2009. – 136 с.

3. Гафнер, В.В. Информационная безопасность: учеб. пособие / В.В. Гафнер. – Ростов н/Д: Феникс, 2010. – 324 с.

АНАЛИЗ УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Маликов В.В., Лившиц И.И.
Учреждение образования «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь (г. Минск)

В настоящее время деятельность всех кредитно-финансовых организаций (КФО) в той или иной степени включает процесс удаленного взаимодействия с потребителями их услуг на основе использования каналов сопряжения и коммуникации (КСиК). Наиболее распространенными вариантами дистанционного банковского обслуживания (ДБО) физических лиц являются интернет-банкинг, мобильный банкинг, SMS-банкинг. Проведение значительного числа безналичных электронных платежей способствует активизации деятельности криминального сообщества по разработке и внедрению противоправных схем, позволяющих удаленно атаковать пользователей финансовых услуг и получать несанкционированный доступ (НСД) к управлению их устройствами и/или счетами.

В рамках исследования проведен анализ моделей и методов, используемых для организации атак на системы ДБО (компоненты: КСиК, электронное устройство конечного пользователя и/или конечный пользователь), а также исследован уровень информационной безопасности таких систем на примере 18 белорусских КФО из реестра Национального банка Республики Беларусь, имеющих специальные разрешения (лицензии) на