УДК 376.1

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ОБУЧЕНИЯ ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЦ С ОСОБЫМИ ПОТРЕБНОСТЯМИ

Власова Г.А., Шпак И.И.

Институт информационных технологий БГУИР, Минск, Республика Беларусь

g.vlasova@bsuir.by, shpak@bsuir.by

Важнейшей предпосылкой получения перспективной профессии для лиц с особыми потребностями является использование информационно-коммуникационных технологий. Однако наряду с большими возможностями новые технологии генерируют и новые угрозы. В подавляющем большинстве случаев угрозы информационным ресурсам реализуются из-за человеческого фактора с применением методов социальной инженерии. Формирование социально-психологических навыков противостояния угрозам информационной безопасности является необходимым условием для развития инклюзивного образования.

Ключевые слова: инклюзивное образование, лица с особыми потребностями, информационно-коммуникационные технологии, информационная безопасность, социальная инженерия, профессиональное образование, образовательные технологии.

Обеспечение всеохватного и справедливого качественного образования является одной из целей устойчивого развития (ЦУР) Республики Беларусь [1]. В этой связи к 2030 году планируется обеспечить равный доступ к образованию и профессионально-технической подготовке всех уровней для уязвимых групп населения, в том числе инвалидов (цель 4). Предполагается также уменьшение неравенства, в том числе путем поощрения активного участия всех людей в социальной, экономической и политической жизни независимо от их инвалидности (цель 10). К 2030 году предполагается обеспечить достойную работу для всех, в том числе молодых людей и инвалидов (цель 8).

В полном соответствии с указанными целями Концепцией развития системы образования Республики Беларусь до 2030 года «признана необходимость включения (инклюзии) лиц с особенностями психофизического развития … в образовательный процесс с учетом их особых образовательных потребностей» [2]. Инклюзия в образовании является одним из ведущих принципов государственной политики в сфере образования [2].

Для многих уязвимых категорий использование информационно-коммуникационных технологий является важнейшей, а в ряде случаев единственной возможностью получения образования и достойной работы. Однако новые возможности связаны с новыми угрозами. Президент Республики Беларусь А.Г.Лукашенко на VI Всебелорусском народном собрании сказал: «Не умаляя преимуществ, возможностей и перспектив, которые открыл человеку информационный мир, мы должны обратить внимание и на его обратную сторону. На искусственную реальность, которая дала зеленый свет манипуляциям, обману, преступлениям…» [3]. В 2023 году в Беларуси зафиксировано более 10 тысяч киберпреступлений. «Из них 90% (чуть более 9 тыс.) – это мошенничество и хищение

денежных средств … Таких преступлений в сравнении с прошлым годом стало в два раза больше», – сообщил начальник управления по раскрытию киберпреступлений главного управления по противодействию киберпреступности Министерства внутренних дел [4].

К компьютерной преступности относят: преступления против информационной безопасности (модификация компьютерной информации, несанкционированный доступ к компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети и др.); изготовление и распространение порнографических материалов; хищения путем использования средств компьютерной техники; иные преступления, связанные с использованием компьютерной техники (доведение до самоубийства путем систематического унижения личного достоинства через распространение каких-либо сведений в сети Интернет, разглашение врачебной тайны, незаконное собирание либо распространение информации о частной жизни, клевета, оскорбление и т.д.). При этом средства компьютерной техники являются орудиями совершения преступления.

Среди тенденций развития информационных технологий, способствующих киберпреступлениям, выделяют следующие: развитие сети Интернет в Республике Беларусь; предоставление электронных услуг (включая оборот товаров и денежных средств); дистанционная занятость и обучение (вызванные, в том числе распространением коронавирусной инфекции); отставание уровня компьютерной грамотности от скорости внедрения компьютерных технологий [5].

В этой связи особую значимость приобретает построение взаимосвязанных моделей профессиональной области и обучаемого [6].

Известно, что взлом систем защиты информации в 80% случаев происходят из-за человеческого фактора. Сегодня одним из основных инструментов хакеров стала социальная инженерия – хакерство с использованием человеческого фактора. Под социальной инженерией понимают манипулирование человеком или группой людей с целью взлома систем безопасности и похищения важной информации [7]. В данном случае человек понимается как часть компьютерной системы. Методы социальной инженерии следует отличать от социального программирования, которое реализуется без использования вычислительной техники и применяется не только для взлома, но и для других целей: обуздания толпы, победы на выборах и т.д.

Психологические предпосылки воздействия на объект согласно схеме белорусского психолога и социолога В.П. Шейнова следующие [7]: формирование цели воздействия на объект; сбор информации об объекте воздействия; обнаружение наиболее удобных мишеней воздействия; аттракция (от лат. attralure – привлекать, притягивать) – создание нужных условий для воздействия на объект; понуждение к нужному действию; нужный итог.

В ряде случаев возможно создание условий, при которых объект сам просит придти мошенника (хакера). При этом имеет место обратная социальная инженерия.

Области применения социальной инженерии разнообразны: финансовые махинации; конкурентная разведка, в том числе информация о маркетинговых планах организации, воровство клиентских баз данных, информация о наиболее перспективных сотрудниках, информация об организации с целью последующего уничтожения конкурента; фишинг и другие способы кражи паролей с целью доступа к персональным банковским данным частных лиц; фарминг – изменение адресов так, чтобы страницы, которые посещает пользователь, были не оригинальными, а фишинг-страницами; общая дестабилизация работы организации; рейдерские атаки (методы социального инжиниринга применяются на первом этапе – сбора информации).

В ряде случаев в силу физического и эмоционального состояния лиц с особыми потребностями им труднее распознать обман и манипуляцию. Так, лицам, имеющим проблемы со зрением, сложнее отличить фишинговую страницу от истинной либо обнаружить незначительные изменения в написании ссылки на страницу в Интернете. Лицам, имеющим проблемы со слухом, сложнее уловить интонацию говорящего с ним

человека и распознать мошенника. Лица с нарушениями опорно-двигательного аппарата могут случайно коснуться внезапно появившегося на экране компьютера предложения от хакера. Кроме того, лицам с особыми потребностями сложнее обнаружить враждебные намерения, поскольку они привыкли к доброжелательному к себе отношению.

Обучающимся следует разъяснять, что, работая на предприятии, избежать подобных угроз позволит соблюдение следующих правил:

1) ни один из сотрудников предприятия не должен знать больше, чем ему полагается знать по должности;

2) в трудовом контракте обязательно должен быть пункт об ответственности сотрудника.

Однако настройка «человеческого брандмауэра» требует постоянного внимания. Обеспечение информационной безопасности и защита информации – это непрерывная системная работа [8].

Как было сказано выше, в Республике Беларусь люди с особыми потребностями окружены вниманием государства, а также поддержкой граждан. Поэтому часто бывают уязвимы к обманщикам. Кроме того, большинство киберпрестулений в отношении граждан нашей страны совершается из-за границы. В этой связи следует уделять особое внимание обучению основам информационной безопасности лиц с особенностями психофизического развития.

Литература

1. Цели устойчивого развития в Беларуси // [Электронный ресурс]. – Режим доступа: https://sdgs.by/targets. – Дата доступа: 19.11.2023.

2. Концепция развития системы образования Республики Беларусь до 2030 года [Электронный ресурс]. – Режим доступа: https://edu.gov.by/kontseptsiya-do-2030-goda. – Дата доступа: 19.11.2023.

3. Доклад Президента Беларуси на VI Всебелорусском народном собрании // Администрация Президента Республики Беларусь. [Электронный ресурс]. – Режим доступа: https://president.gov.by/ru/events/shestoe-vsebelorusskoe-narodnoe-sobranie. – Дата доступа: 19.11.2023.

4. В Беларуси в 2023 году зафиксировано более 10 тыс. киберпреступлений // Белта. [Электронный ресурс]. – Режим доступа : http:// https://www.belta.by/society/view/v-belarusi-v-2023-godu-zafiksirovano-bolee-10-tys-kiberprestuplenij-585322-2023. – Дата доступа: 19.11.2023.

5. Власова, Г.А. Обучение – необходимое условие обеспечения информационной безопасности в период цифровизации. / Власова Г.А., Войтехович С.А. // Дистанционное обучение – образовательная среда XXI века: материалы X Междунар. науч.-метод. конф., Минск, 7–8 декабря 2017г. – Мн.: БГУИР, 2017. – С.196.

6. Шпак, И.И. Применение ИКТ и адаптивных образовательных технологий для развития и совершенствования инклюзивного образования. / Шпак И.И., Охрименко А.А., Скудняков Ю.А., Шпилевская В.В. // Непрерывное профессиональное образование лиц с особыми потребностями: сб. ст. IV Междунар. науч.-практ. конфе., Минск, 9-10 декабря 2021г. – Мн.: БГУИР, 2021. – С.328-330.

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

8. Власова, Г.А. Аспекты изучения процессной модели при подготовке специалистов по информационной безопасности. / Г.А. Власова // Технические средства защиты информации: тезисы докладов XVIII Белорусско-российской научно-технической конференции, Минск, 9 июня 2020г. – Мн.: БГУИР, 2020. – С.18.

SOCIO-PSYCHOLOGICAL ASPECTS OF EDUCATION OF THE BASICS OF INFORMATION SECURITY FOR PERSONS WITH SPECIAL NEEDS

Vlasova G.A., Shpak I.I.

Institute of information technologies BSUIR, Minsk, Republic of Belarus

The most important prerequisite for obtaining a promising profession for persons with special needs is the use of information and communication technologies. However, along with great opportunities, new technologies generate new threats. In the vast majority of cases, threats to information resources are realized due to the human factor using social engineering methods. The formation of socio-psychological skills to counter information security threats is a prerequisite for the development of inclusive education.

Keywords: inclusive education, persons with special needs, information and communication technologies, information security, social engineering, professional education, educational technologies.