Заключение. При интерпретации результатов по двум разным тестам не удалось найти связь между типом родительского отношения и видом психологической защиты. Однако удалось подтвердить, что у большинства людей психологическим механизмом защиты является проекция.

Результаты данного исследования существования связи между родительским отношением и психологической защитой можно использовать при коммуникации. Если большинство людей используют проекцию – это нужно учитывать. Не додумывать, не приписывать, не достраивать слова другого человека, а также снижать эффект использования проекции.

1. Психология счастливой жизни [Электронный ресурс]. – Режим доступа: https://psycabi.net/. – Дата доступа: 11.05.2022.

НЕИНФОРМИРОВАННОСТЬ ПОДРОСТКОВ О КИБЕРПРЕСТУПНОСТИ КАК СОЦИАЛЬНАЯ ПРОБЛЕМА

Шаршнёва В.В.,
студентка 2 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – ***Михайлова Е.Л.,*** *канд. пед. наук, доцент*

Ключевые слова. Киберпреступление, вишинг, смишинг, кибератака.
Keywords. Cybercrime, vishing, smishing, cyberattack.

Киберпреступление – это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства [1]. На сегодняшний день очевидно снижение числа преступлений в сфере информационных технологий: если в 2020 году следователями возбуждено 25 571 уголовное дело, то в 2021 году – 15 503, что на 10 068 уголовных дел меньше. Что касается цифровых показателей первого квартала 2022 года, то Следственным комитетом зарегистрировано вдвое меньше преступлений по ст.212 (хищение путем модификации компьютерной информации) Уголовного кодекса – 2 тыс. 833. За аналогичный период 2021 года установлено 5 тыс. 734 таких преступлений. В целом, несмотря на плодотворную работу правоохранительных органов, нельзя говорить о том, что на сегодняшний день киберпреступность побеждена. Ведь кибермошенники используют различные способы социальной инженерии: пишут от имени друзей, используют фишинговые ссылки, звонят от имени сотрудников банка и правоохранительных органов [2].

Именно это доказывает актуальность темы в данный момент среди подростков. Кроме того, одним из индикаторов актуальности проблемы, по мнению Ю.П. Беженарь, является то, что «вся жизнь молодых людей, включая учебную, внеаудиторную, профессиональную и досуговую деятельность, проходит в условиях информационного многообразия» [3, с.19].

Цель исследования – изучить степень информированности подростков о киберпреступности.

Материал и методы. Материалы: научные статьи по теме исследования, анкетные опросники. Методы исследования: метод теоретического анализа литературы, анкетирование, математическая обработка результатов исследования. В исследовании приняли участие учащиеся ГУО «Средняя школа №4 г. Витебска» в количестве 22 человек, из них 19 девушек и 3 юноши в возрасте 14-15 лет.

Результаты и их обсуждение. Зная, что такое киберпреступление, можно говорить о самых популярных его формах. Одной из них является вишинг (англ. vishing – voice + phishing) – это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль (как правило, сотрудника банка, технического специалиста и т.д.), вынуждают человека сообщить им свои конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой [4]. Различают также такой вид мошенничества как смишинг (англ. SmiShing) – мошенничество при помощи SMS-сообщений. В этом случае ссылка на поддельный сайт отправляется через SMS, либо мошен-

ники просят прислать им необходимую информацию о банковской карте в ответном сообщении [5, с. 25]. Эти и многие другие формы мошенничества можно назвать таким действием как кибератака. Как указывает в своей научной работе французский автор Д. Вентре, «кибератака является современной формой агрессии, совершаемой отдельными лицами, либо целой группой лиц, целью которой является подрыв информационной системы безопасности, подрыв работы какой-либо инфраструктуры, компьютерной сети и/или подрыв работы персональных компьютеров и других приспособлений, произведенный любыми способами. Кибератаки совершаются злоумышленниками анонимно, что не освобождает лиц, совершивших ее, от ответственности; кибератаки являются нелегальным проникновением в чужую компьютерную систему, что может послужить причиной подрыва национальной системы безопасности. В хакерской атаке (кибератаке) могут принимать участие один или несколько высококлассных специалистов (хакеров)» [6].

Анализ результатов эмпирического исследования показал, что большинство подростков (86%) знакомы с определением киберпреступности. Все респонденты (100%) ответили, что необходимо знать правила безопасного поведения в Интернете.

На вопрос об известных подросткам формах мошенничества наиболее популярными были «вишинг» (мошенничество с помощью телефонных звонков) (28%) и мошенничество в виде объявления о победе в лотерее или выигрыше айфона (28%); «смишинг» (вид мошенничества с помощью SMS-сообщений) (18%), распространение личной информации (18%), такие направления, как кибератака и кибертерроризм были отмечены только 8% респондентов.

Отвечая на вопрос о том, оставляют ли подростки свои личные данные на незнакомых сайтах, 77% респондентов ответили отрицательно, 18% ответили утвердительно, 5% ответили, что делают это иногда.

Стоит отметить, что исходя из ответов, большинство подростков (65%) за последний год не сталкивались со случаями мошеннических действий в отношении них. Однако оставшиеся 35% оказывались в ситуации следующих мошеннических действий: мошенничество в интернет-магазине; мошенничество на торговой платформе «Куфар»; смишинг; вишинг (где мошенник представляется сотрудником банка).

Также 57% школьников отмечают в анкете, что отвечают на незнакомые номера. Но в то же время 78% из них не переходят по незнакомым ссылкам.

Говоря о единой биометрической системе, 56% подростков не знают о ней и не готовы предоставлять свои биометрические данные для упрощённой системы идентификации. В качестве наиболее эффективного способа защиты личных данных школьники предложили двухэтапную аутентификацию (85%). Также все респонденты (100%) готовы обратиться в милицию в случае хищения денежных средств в сети Интернет.

Чтобы не попасть в руки мошенников, рекомендуется создавать уникальные пароли к различным Интернет-сервисам, не отвечать на незнакомые номера или установить определитель номера, не переходить по незнакомым ссылкам, использовать только проверенные Wi-Fi источники, не оставлять персональные данные и данные банковских карт в Интернет приложениях, использовать двухэтапную аунтефикацию.

Заключение. Таким образом, результаты свидетельствуют о том, что опрошенные респонденты имеют верное представление о киберпреступности как преступлении, а также о правилах безопасного поведения в сети Интернет. Но в то же время они склонны попадать в руки мошенников, отвечая на незнакомые номера. Положительным фактом является то, что подростки готовы общаться за помощью в милицию.

1. Советы по защите от киберпреступников [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime. – Дата доступа: 30.05.2022 г.

2. Число киберпреступлений снизилось почти вдвое. Зампред СК о тенденциях в области IT-преступлений [Электронный ресурс]. – Режим доступа: https://www-belta-by.cdn.ampproject.org/v/s/www.belta.by/amp/society/view/chislo-kiberprestuplenij-snizilos-pochti-vdvoe-zampred-sk-o-tendentsijah-v-oblasti-it-prestuplenij-496880-2022. – Дата доступа: 30.05.2022 г.

3. Певзнер, М.Н. Диалоговый подход к противодействию молодежному экстремизму в условиях информационного многообразия / М.Н. Певзнер, П. А. Петряков, Ю. П. Беженарь // Гражданское образование молодежи в современном медиапространстве: возможности и риски информационного общества: материалы международной научно-практической конференции, Витебск, 23 марта 2022 г. – Витебск: ВГУ имени П.М. Машерова, 2022. – С. 13–26. – https://rep.vsu.by/handle/123456789/32482. – Дата доступа: 30.05.2022 г.

4. Мошенничество с использованием технологий социальной инженерии (вишинг) [Электронный ресурс]. – Режим доступа: https://oac.gov.by/phishing/fighting-telecom-fraud/vishing. – Дата доступа: 30.05.2022 г.

5. Бахтеев, Д.В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц / Д.В. Бахтеев // Российское право: Образование. Практика. Наука. – 2016. – № 3. – С. 24–26.

6. Ventre, D. Cyberespace et acteurs du cyber conflict. – Hermes-Lavoisier, 2011.