С.Н. Фазульянова,
Самарский университет

КОМПЕТЕНТНОСТЬ НАСЕЛЕНИЯ В ВОПРОСАХ КИБЕРБЕЗОПАСНОСТИ: ПРАКТИКИ ИЗМЕРЕНИЯ И ОПЫТ СОЦИОЛОГИЧЕСКОГО ИССЛЕДОВАНИЯ В САМАРСКОЙ ОБЛАСТИ

Тезисы посвящены результатам исследования, цель которого – выявление уровня компетентности жителей Самарской области в сфере кибербезопасности через анализ цифровой грамотности и культуры поведения в киберпространстве. Приводится классификация респондентов по уровням компетентности и сравнение полученных результатов с похожими замерами по РФ. Отмечается, что уровень компетентности в вопросах кибербезопасности жителей региона принимает относительно высокие и средние значения. Однако в сознании граждан недостаточно сформирован ряд важных правил безопасности и главное, навыков реагирования на киберугрозы.

Ключевые слова: кибербезопасность, киберугроза, информационная грамотность, уровень компетентности, социальный профиль группы.

S.N. Fazulianova,
Samara University

CYBERSECURITY COMPETENCE: MEASUREMENT PRACTICES AND EXPERIENCE OF A SOCIOLOGICAL SURVEY IN THE SAMARA REGION

The thesis is devoted to the results of the study, which aims to identify the level of cybersecurity competence of Samara region residents through the analysis of digital literacy and culture of behavior in cyberspace. It classifies respondents by competence levels and compares the results with similar measures in the Russian Federation. It is noted that the level of cybersecurity competence of the region's residents takes on relatively high and average values. However, a number of important security rules and, most importantly, skills for responding to cyberthreats have not been sufficiently formed in the minds of citizens.

Keywords: cybersecurity, cyberthreat, information literacy, level of competence, group social profile

Роль кибербезопасности в устойчивости бизнеса и государства за последние два-три года стремительно вышла на первый план. В прошедшем 2022 году в РФ зафиксировано трехкратное увеличение общего числа кибератак по сравнению с предыдущим годом, при этом в открытый доступ попали более 460 млн учетных записей пользователей [1]. По данным МВД РФ в абсолютном выражении количество киберпреступлений превысило отметку в 522,1 тыс. [2]

Главными мишенями кибератак остаются бизнес-корпорации, коммерческие и государственные организации. Тем не менее, количество атак на частных лиц в последние годы имеет тенденцию к росту. В 2022 году на обычных пользователей пришлось 17 % от числа всех атак, что на 3 % выше, чем в предыдущий год [3]. И в текущем 2023 году эксперты прогнозируют увеличение числа атак на пользователей в социальных сетях и мессенджерах, кражи учетных данных с атаками на второй фактор аутентификации с использованием фишинговых инструментов, социальной инженерии и вредоносных программ с функциями кражи SMS и пуш-уведомлений.

Нельзя забывать при этом, что всё больше личных устройств обычных пользователей становятся точками доступа в корпоративные информационные системы. Среднее количество приложений на наших смартфонах варьируется и по разным оценкам может доходить до 67 [4]. Это заставляет задуматься о безопасности такого соседства.

В связи с этим особую актуальность и важность приобретают вопросы понимания населением принципов поведения и управления своими данными и личными финансами в онлайн-среде. Готовы ли рядовые пользователи к высоким темпам цифровизации? Способны ли они противостоять угрозам киберпреступников? Каков реальный уровень компетентности населения в сфере кибербезопасности?

Эти вопросы побуждают исследователей во всем мире перевести фокус своих исследований с корпоративной информационной безопасности на обычных пользователей и потребителей информации и услуг в онлайне. Появляются различные по масштабам проекты, объединенные общим стремлением выразить в одном емком интегральном показателе специфику знаний и компетенций населения в цифровом пространстве.

Так, аналитический центр НАФИ (г. Москва) произвел первый в России замер «индекса цифровой финансовой грамотности жителей», эмпирическим объектом которого выступили жители РФ. Предметом выступил уровень цифровой грамотности, который измерялся по 100-бальной шкале. В основе измерения лежит методика ОЭСР [5].

В отличие от московских коллег, в нашем исследовании, эмпирический объект уже – жители Самарской области. Но предмет сформулирован более широко – уровень компетентности в сфере кибербезопасности. Это ключевое для нашего исследования понятие складывается из совокупности признаков, измеряющих цифровую грамотность и соблюдение мер безопасности в киберпространстве[5].

Высокий уровень компетентности в вопросах кибербезопасности означает, что человек имеет достаточно знаний и опыта, чтобы принимать правильные решения и предотвращать инциденты в области кибербезопасности, знает о видах киберугроз и способах их предотвращения, а также осведомлен о последних технологических разработках в области кибербезопасности. Низкий уровень компетентности в сфере кибербезопасности приводит к тому, что люди недооценивают риски и не используют достаточно мер предосторожности, чтобы защитить себя от киберугроз.

Исследование показало, что правила «цифровой гигиены» на базовом уровне известны большинству опрошенных. В целом население Самарской области представляет, что:

– неправильно заводить один и тот же пароль для всех учетных записей;

– нельзя использовать простые пароли типа своего имени, дня рождения или места проживания;

– неправильно записывать пароли от разных сайтов и приложений в заметки на телефоне.

Однако если «копнуть» немного глубже, то тут знания значительной части населения сильно ограничены. О двухфакторной аутентификации знает только каждый второй опрошенный, о безопасном хранилище паролей еще меньше (41 %), менее трети опрошенных регулярно меняют пароли. Нет уверенных знаний и о том, какие данные с банковской карты безопасно передавать посторонним лицам.

Достаточно легкомысленно опрошенные относятся и к соблюдению мер безопасности в отношении личного компьютера: далеко не все регулярно обновляют ПО, устанавливают лицензионные, а не пиратские версии программ, устанавливают пароль при запуске. Такое поведение упрощает жизнь мошенникам, повышает уязвимость домашних компьютеров, легко превращая их в потенциальный источник атак.

[5] Исследование проведено в апреле-ноябре 2022 года, базировалось на классической количественной методологии. Метод сбора информации - онлайн опрос. Генеральная совокупность – взрослое (старше 18 лет) население Самарской области, объем выборки – 1347 чел. Контролируемые выборочные параметры: пол, возраст и тип поселения.

Умение распознать киберугрозы сформировано у значительной части респондентов. Но они не составляют большинство. И особенно тревожен тот факт, что при реальном столкновении с киберугрозой, например, с телефонным мошенником, распространен паттерн избегания «брошу трубку», как крайняя форма этого паттерна – «не беру трубку с незнакомых номеров». Такую модель поведения выбирает примерно каждый третий опрошенный, опасаясь и не зная, как себя вести при столкновении с мошенниками.

На основе замеров по отдельным индикаторам цифровой грамотности и поведения в прожективных ситуациях нами был сформирован интегральный показатель «уровень компетентности в сфере кибербезопасности», измеряемый в баллах. Всего для его измерения использовалось 20 индикаторов в виде групп вопросов в тестовой форме и форме прожективных ситуаций. За каждый ответ присваивались баллы по определенной логике.

В итоге была осуществлена типология (классификация) пользователей по уровням компетентности в сфере информационной безопасности. Всего выделены 5 уровней/типов компетентности: от низкого до «продвинутого».

Показательно, что, несмотря на различия в методике и масштабах исследований, полученные нами результаты схожи с замерами НАФИ. В своем исследовании специалисты НАФИ выделили 3 уровня цифровой финансовой грамотности и получили, что большинство жителей России (87 %) имеют средний или высокий уровень цифровой финансовой грамотности [5]. По данным нашего исследования, 89 % опрошенных жителей Самарской области демонстрируют средний, относительно высокий и «продвинутый» уровень компетентности в сфере кибербезопасности (Рис. 1). Не могу изменить данные в рисунке

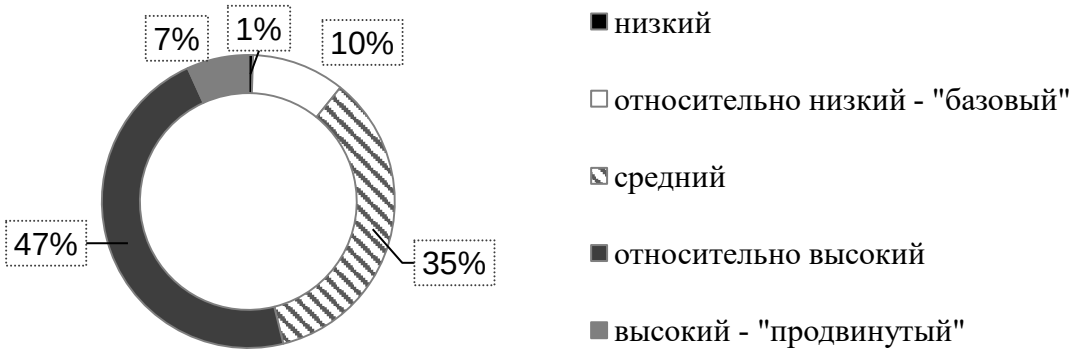

Рис. 1. Распределение опрошенных по уровням компетентности в сфере кибербезопасности (N=1347)

Результаты нашего опроса позволили не просто зафиксировать долю респондентов определенного типа (уровня), но и ответить на вопрос: какие социальные группы преимущественно входят в каждый тип? Для этого выявлялся так называемый «социальный портрет» или профиль групп.

Обращает на себя внимание заметная поляризация социальных профилей разных групп по уровню компетентности в сфере кибербезопасности, а именно:

– «базовый» уровень компетентности имеет «женское лицо», а «продвинутый» – мужское;

– у продвинутой группы и группы с относительно высокой компетентностью более молодежный профиль, и в них преобладают проживающие в крупных городах;

– отличаются эти группы и родом занятий, интересами и предпочитаемыми источниками информации.

Резюмируя результаты исследования, отметим, что уровень компетентности в вопросах кибербезопасности жителей Самарской области принимает относительно высокие и средние значения. Это означает, что опрошенное население в целом демонстрирует адекватное и правильное поведение при взаимодействии с цифровыми продуктами в интернете, однако в сознании граждан недостаточно сформирован ряд важных правил безопасности и, главное, навыков реагирования на потенциальные киберугрозы.

Наше исследование указывает на необходимость информационной работы с населением, направленной не только на упреждение возможных рисков, повышение осведомленности о киберугрозах в целом, но и на вооружение населения техниками и приемами распознавания и отражения киберугроз.

В целях повышения уровня компетентности населения в сфере кибербезопасности необходима разработка программ обучения и образовательных мероприятий, направленных на различные возрастные группы и слои населения. Например, по аналогии с существующими картами компетенций заместителя генерального директора по информационной безопасности и специалиста по информационной безопасности в бизнесе, можно разработать карту компетенций для рядовых пользователей и обучать этому в вузах и школах. Актуальна организация семинаров, тренингов и других интерактивных форм обучения, связанных с кибербезопасностью, которые способствуют освоению безопасных практик в сети, формированию умений распознавать киберугрозы и применять меры противодействия им.

Список литературы:

1. Киберугрозы 2022. Аналитический отчет экспертов Jet CSIRT («Инфосистемы Джет») // https://jetcsirt.su/upload/Otchet%20JetCsirt%20o%20kiberugrozah%202022.pdf

2. Число экстремистских преступлений в России в 2022 году выросло // Информационная группа Интерфакс, 31.01.2023 // https://www.interfax.ru/russia/884032

3. Актуальные киберугрозы: IV квартал 2022 года // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/

4. Лобач Д.В., Смирнова Е.А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. 2019. № 4 // https://cyberleninka.ru/article/n/sostoyanie-kiberbezopasnosti-v-rossii-na-sovremennom-etape-tsifrovoy-transformatsii-obschestva-i-stanovlenie-natsionalnoy-sistemy

5. НАФИ провел первый замер Индекса цифровой финансовой грамотности жителей России // https://nafi.ru/analytics/nafi-provel-pervyy-zamer-indeksa-tsifrovoy-finansovoy-gramotnosti-zhiteley-rossii/