– әлеуметтік-гуманитарлық пәндер болашақ маманның кәсіби мобильділігін дамыту үшін қажетті танымдық іс-әрекет формалары мен әдістерінің кең спектрін қамтиды;

– әлеуметтік-гуманитарлық пәндер тұлғаның өзін-өзі білім алуға және өзін-өзі жетілдіруге саналы қатынасын қалыптастыруда ерекше маңызға ие [6].

Жоғарыда айтылғандарды қорытылай келсек, келесі түйіедеме жасауға болады деп ойлаймыз.

Қазіргі кезеңде әлеуметтік-гуманитарлық білім мен ғылым адамдардың санасы мен өзіндік санасын жаңғыртуға бағытталған ақпараттық күрестің алдыңғы қатарында тұр. Олардың құндылықтық және дүниетанымдық бағдарлары мемлекеттік қауіпсіздіктің басты факторларының бірі болып табылады және жаңғыртылған қоғамдық сана жағдайында болашақ мамандардың кәсіби құзыреттілігін қалыптастырудың шешуші құрамдас бөлігі ретінде қызмет етеді.

Пайдаланылған әдебиеттер тізімі

1. Ясперс К. Смысл и назначение истории. - М.: Изд. Полит.лит., 1991.

2. Санникова О.В. Трансформация содержания профессионального социально-гуманитарного образования: социологический анализ. [Электронды ресурс]. – URL: https://www.dissercat.com/content/transformatsiya-soderzhaniya-professionalnogo-sotsialno-gumanitarnogo-obrazovaniya-sotsiolog

3. Манхейм К. Диагноз нашего времени. - М.: Изд. Юрист,1994.

4. Миллс Ч. Социологическое воображение. - М.: Изд. Стратегия. 1998.

5. Пузиков В. Социологическое образование в вузе: задачи и проблемы // Высшее образование в России. - 2008. - № 6 - С. 106 - 109.

6. Роль социально-гуманитарных дисциплин в формировании и развитии социально-личностных компетенций студентов. [Электронды ресурс]. – URL: http://bibliofond.ru/view.aspx?id=564963

УДК 372.851.02

НЕКОТОРЫЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ В КАЗАХСТАНЕ

Жумагалиева А.Б., Карагандинский университет имени академика Е.А. Букетова, Караганда, Казахстан

Термин «кибербезопасность» (согласно опубликованному Международной организацией по стандартизации и Международной электротехнической комиссией стандарту в области кибербезопасности ISO/IEC 27032:2012) характеризуется как безопасность в киберпространстве или как сохранение конфиденциальности, целостности, доступности и других важных свойств активов пользователей и организаций типа аутентичности, учетности и надежности в киберпространстве [1].

В стандарте ISO/IEC 27032:2012 также охарактеризована взаимосвязь терминов «кибербезопасность», «сетевая безопасность», «безопасность приложений, «безопасность в Интернете» и «безопасность ключевых систем информационной инфраструктуры», которая отражена на рисунке 1.

Кибербезопасность – это деятельность, нацеленная на обеспечение защиты пользователей, их информационных систем, сетей, и программ от цифровых атак.

Основной целью таких кибератак может являться как получение конфиденциальной информации пользователя для дальнейшего злоупотребления этой информации в собственных целях хакера, так и нарушение работы целого бизнес-процесса.

Поэтому, в особенности контекста государственных подразделений и больших частных организаций, для Казахстана, как и для других стран мира одной из основных задач для эффективного и безопасного присутствия в интернете является именно развитие сферы кибербезопасности.

Рисунок 1. Взаимосвязь кибербезопасности с другими видами безопасности в соответствии со стандартом ISO/IEC 27032:2012

П р и л о ж е н и е- составлено автором по источнику [1]

В современном цифровом мире киберпреступность является ключевой угрозой роста мировой экономики. Повышение культуры поведения граждан в Интернете, информационная безопасность, а также распространение понятных общемировых правил борьбы с киберпреступностью могут помочь в борьбе с такими преступлениями. Ежегодно эксперты Международного союза электросвязи ООН (International Telecommunication Union) составляют рейтинг стран по уровню кибербезопасности под названием «Глобальный индекс кибербезопасности» (Global Cybersecurity Index).

Глобальный индекс кибербезопасности (GCI) — это совместный проект ITU-ABI research, призванный оценить возможности государств в области кибербезопасности . GCI измеряет приверженность стран кибербезопасности на глобальном уровне для повышения осведомленности о важности проблем кибербезопасности [2].Согласно новой методике, Казахстан занял место во второй группе (Tier 2 – Advancing), набрав 94,04 балла из 100 возможных., показанный на рисунке 11. Новая методика оценивает работу за 2023 год. Обновляется индекс 1 раз в два года. В отчете 2024 года используется обновленный пятиуровневый анализ, позволяющий более точно оценить достижения стран в области кибербезопасности. Уровни включают Tier 1 — Role-modelling, Tier 2 — Advancing, Tier 3 — Establishing, Tier 4 — Evolving и Tier 5 — Building. (Рисунок 2).

Рейтинг GCI формируется на основе 83 параметров, охватывающих пять ключевых направлений кибербезопасности: юридический, технический, организационный аспекты, развитие потенциала и международное сотрудничество. Казахстан в рамках новой методики выполнил все требования в направлениях «юридический» и «сотрудничество», а также продемонстрировал достаточный технический уровень.

Данный рейтинг оценивает готовность 194 стран к кибератакам. В этом году Казахстан продемонстрировал значительный прогресс, заняв место во втором уровне — Tier 2, что подтверждает его успешное развитие в области кибербезопасности.

В 2024 году произошли изменения в оценочной системе индекса — конкретные места были заменены на распределение стран по уровням, от Tier 1 лидеры в кибербезопасности до Tier 5. Казахстан вошел во второй уровень Tier 2, что подчеркивает его устойчивый прогресс и приверженность к развитию инфраструктуры кибербезопасности. Однако для дальнейшего повышения рейтинга необходимо усилить организационные меры, развить потенциал, а также усилить меры области международного сотрудничества в сфере кибербезопасности".

В 2024 году в первой группе рейтинга МСЭ доминируют европейские страны и США. В этот список также входят Гана, Кения, Маврикий, Марокко, Руанда и другие страны. Второй уровень, известный как «передовые» страны, включает Казахстан, Китай, Россию, а также Швейцарию и Канаду.

В целях определения уровня осведомленности населения об угрозах информационной безопасности (кибербезопасности с октября по ноябрь 2024 года было проведено социологическое исследование среди населения.

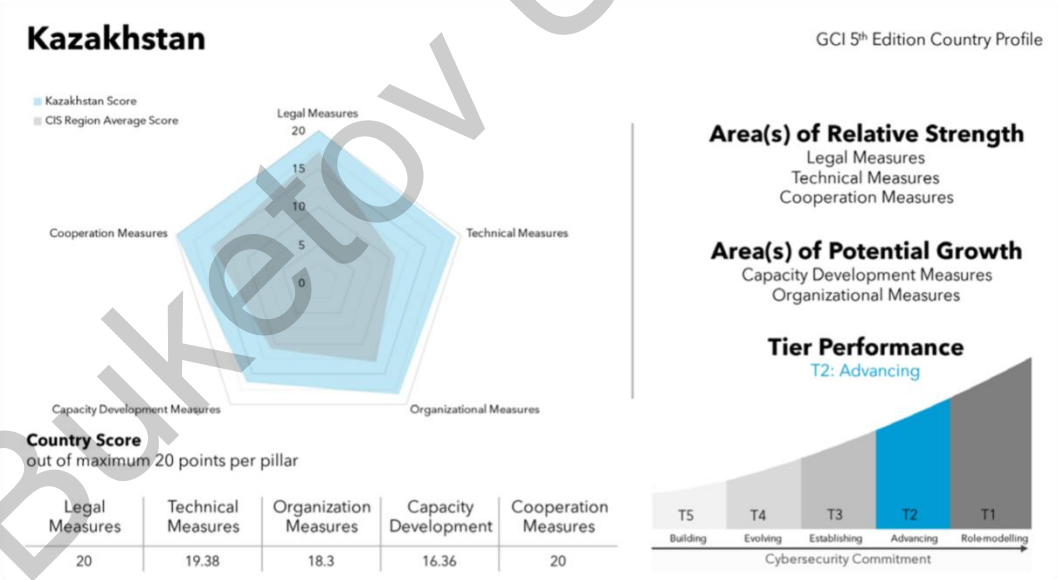

Рисунок 2. Место Казахстана в Глобальном индексе кибербезопасности в 2024 г.
П р и л о ж е н и е- составлено автором по источнику [3]

В процессе исследования было охвачено:
- 3 города республиканского значения;
- 17 областей, райцентры, 11371 респондент.

Показатели осведомленности населения об угрозах информационной безопасности (кибербезопасности) и защиты персональных данных, представлен на рисунке 3.

Из рисунка 2 видно, что государство проводит работу по осведомлению населения об угрозах кибербезопасности. В 2022 году процент осведомленности населения составил 77,4%, то в 2024 году на 4,9% больше, что составило 82,3%.

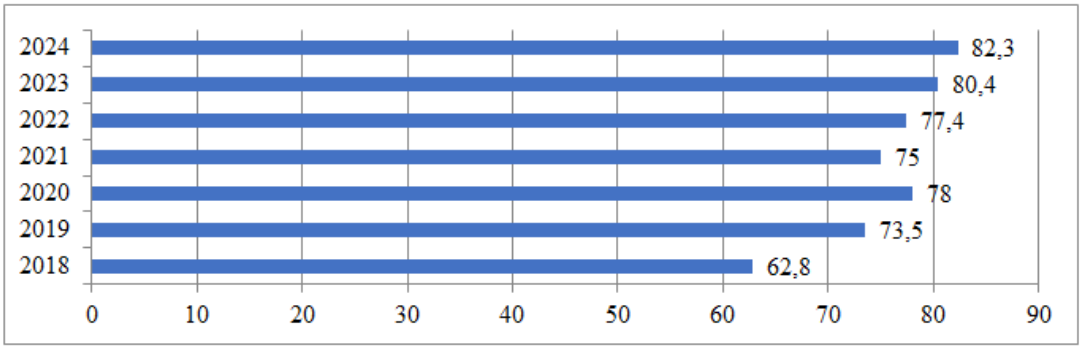

Рисунок 3. Динамика показатели осведомленности населения об угрозах информационной безопасности (кибербезопасности) и защиты персональных данных (на основе социологического опроса) за 2018-2024 гг., %

П р и л о ж е н и е- составлено автором по источнику [4]

По результатам социологического опроса, большинство респондетов были осведомлены об киберугрозах:

- получают знания о защите личной информации при использовании социальных сетей – 90,52%;
- осведомлены при использовании цифровой подписи – 85,06%;
- знают о потенциальных рисках детей при использовании интернета – 76,65%.

Вопросам развития сферы информационной безопасности в Казахстане уделяется значительное внимание. И результат работы, проводимой совместно органами, неправительственными организациями и бизнесом — это тенденция последних лет, когда наша страна стремительно улучшает свои позиции в глобальном индексе кибербезопасности.

В 2024 году количества этих атак снизилась на 35 единиц, что составила 117. При этом 35 % зафиксированных DoS/DdoS-атак были направлены на банки второго уровня РК и 22 % на государственный сектор. DdoS – это действия, направленные на перегрузку трафиком, когда на атакуемый ресурс отправляется большое количество злонамеренных запросов, из-за чего полностью «забиваются» все каналы сервера или вся полоса пропускания. При этом передача легитимного трафика на сервер затрудняется или становится невозможной. Угрозы информационной безопасности от ОЦИБ за 2024 г. показан на рисунке 4.

Из рисунка 4 видно, что наибольшая угроза продолжает представлять вредоносное ПО, на долю которого приходится 49% от всех зарегистрированных инцидентов ИБ, полученных от ОЦИБ. В первую очередь, это программы-вымогатели, вирусы и трояны, которые используются для блокировки данных и промышленного шпионажа.

Второе место среди угроз занимает эксплуатация уязвимости, которая составляет 32% от всех инцидентов. Хакеры активно используют слабые места в устаревших системах и уязвимости нулевого дня, что позволяет им проникать в сети организаций до выхода необходимых обновлений безопасности.

Спам с вредоносными вложениями, несмотря на более низкие показатели (6%), остаётся стабильным источником угроз на протяжении всего года. Основной вектор атаки – распространение вредоносного ПО через электронные письма и ссылки, нацеленные на человеческий фактор.

Несанкционированный доступ занимает четвёртое место с долей 5% от общего числа инцидентов. Пик активности был зафиксирован в феврале и марте, после чего наблюдается значительный спад, связанный с более активным внедрением многофакторной аутентификации и усилением контроля доступа во многих организациях РК, что позволило снизить количество успешных атак.

Замыкают список Brute-force атаки (4%), направленные на подбор паролей методом перебора. Они остаются опасными для слабо защищённых учётных записей и систем с простыми паролями.

Анализ угроз информационной безопасности за 2024 год демонстрирует, что Казахстан продолжает сталкиваться с растущей сложностью угроз. Особенно заметным становится активный рост атак на информационные системы, которые не успели адаптироваться к современным вызовам, что подчёркивает необходимость своевременного обновления программного обеспечения и внедрения более надёжных защитных мер.

Казахстан имеет отдельные законодательные акты в части кибербезопасности, а именно, Концепция Кибербезопасности РК ("Киберщит Казахстана") от 30 июня 2017 г., Стратегия кибербезопасности финансового сектора Республики Казахстан на 2020-2022 годы, Концепция развития цифровой экосистемы на 2022-2027 года («Киберщит-2»).

Кроме того, в планах разработать единую техническую политику в сфере ИКТ, в рамках которой предприятия и организации можно будет определять по уровням безопасности. И появится новая методика экономической системы информационной безопасности.

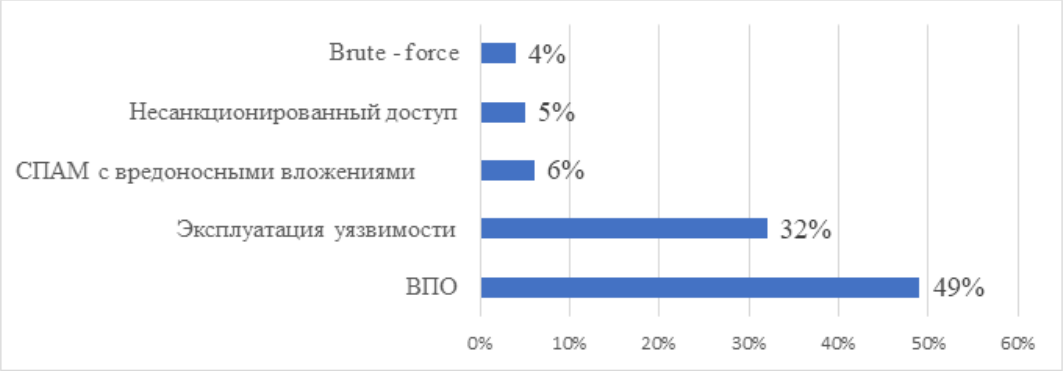

Рисунок 4. Угрозы информационной безопасности от ОЦИБ за 2024 г.
П р и л о ж е н и е- составлено автором по источнику [5]

Также рассмотрят возможность создания резервного Национального координационного центра информационной безопасности, "Киберполигона" по подготовке специалистов.

Отмечается, что в вопросе кибербезопасности уже был реализован ряд важных проектов. Например, в законе появилось понятие "киберстрахование", которое позволяет возмещать имущественный вред организации, причиненный в результате компьютерных инцидентов, а также моральный вред физическому лицу, причиненный в результате утечки данных.

Также был создан Комитет по ИБ, появились профстандарты в IT и запущен "пилот" частной платформы выявления уязвимостей BugBounty. Там уже зарегистрировано более 1,1 тыс. независимых экспертов, от которых получено более 1,2 тыс. отчетов с сообщениями об уязвимостях.

В настоящее время, Казахстан, как и многие другие страны, осуществляет свое развитие с акцентом на внедрение передовых технологий, стремясь повысить эффективность государственного управления.

Список использованной литературы

1. Модуль 2 «Основные виды киберпреступности». Управление Организации Объединенных Наций по наркотикам и преступности https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_2_General_Types_of_Cybercrime_RU.pdf

2. Аллахвердиева Л.А., Бахшалиев Ф.Р. Кибербезопасность как фактор развития цифровой экономики // Вестник ИЭ РАН. №6. - 2019. - С. 41–50

3. Казахстан укрепил позиции в Глобальном индексе кибербезопасности 2024 // https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

4. Данные социологического опроса/ среди населения, проведенны по заказу Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан//www.gov.kz/memleket/entities/infsecurity/press/article/details/109499?lang=ru

5. КИБЕРКОД 2024: вызовы цифровой эпохи// https://sts.kz/storage/media/%C3%90%C2%BA%C3%90%C2%B8%C3%90%C2%B1%C3%90%C2%B5%C3%91%C3%90%C2%B4%C3%90%C2%B0%C3%90%C2%B9%C3%90%C2%B4%C3%90%C2%B6%C3%90%C2%B5%C3%91%C3%91%20%C3%91%C3%90%C2%B8%C3%90%C2%BD%C3%90%C2%B0%C3%90%C2%BB%201402%20%C3%90%C2%B2%C3%90%C2%B5%C3%90%C2%B1_compressed_MgA8leK.pdf

УДК 316.3

ЛИЧНОСТНЫЕ И ПРОФЕССИОНАЛЬНЫЕ ОРИЕНТАЦИИ БУДУЩИХ СОЦИАЛЬНЫХ РАБОТНИКОВ КАК ОТРАЖЕНИЕ ГУМАНИТАРНЫХ И СОЦИАЛЬНЫХ ТЕНДЕНЦИЙ

Жебеген З.Б., Евразийский национальный университет им.Л.Н.Гумилева, Астана, Казахстан
Азаматова Н.А., Евразийский национальный университет им.Л.Н.Гумилева, Астана, Казахстан
Урузбаева Г.Т Евразийский национальный университет им.Л.Н.Гумилева, Астана, Казахстан

Аннотация. В статье представлены результаты исследования взаимосвязи карьерных ориентиров, смысложизненных ориентаций, самоотношения и психологического благополучия студентов гуманитарного профиля, в частности будущих социальных работников ЕНУ. В исследовании использовались методики Е.А. Климовой «Личные профессиональные планы» и Д.А. Леонтьева «Смысложизненные ориентации». Показано, что