УДК 004.056

ВЫЗОВЫ ЦИФРОВОМУ ОБЩЕСТВУ: ПРОБЛЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Мансуров Александр Валерьевич

Алтайский государственный университет, г. Барнаул
e-mail: mansurov.alex@gmail.com

CHALLENGES TO DIGITAL SOCIETY: PROBLEMS OF TRAINING INFORMATION SECURITY SPECIALISTS

Mansurov Alexander V.

Altai State University, Barnaul

Аннотация: В работе идентифицируются и рассматриваются актуальные вызовы и угрозы современному цифровому обществу с позиции, осуществляемой специалистами по защите информации профессиональной деятельности. Отмечается, что для эффективного преодоления этих вызовов и угроз специалистам очень важно иметь адекватный уровень компетенций, которые должны быть обеспечены в ходе их подготовки согласно учебным планам направлений и специальностей подготовки «Информационная безопасность» в высших учебных заведениях. Выполненный сравнительный анализ учебных планов подготовки специалистов в области информационной безопасности в университетах и колледжах ряда стран БРИКС (прежде всего России, Китая и Индии) позволил установить отсутствие в явном виде в учебных планах специализированных дисциплин, непосредственно отвечающих за формирование требуемых компетенций. В заключении сформирован ряд критичных вопросов, необходимых для дальнейшего обсуждения в ходе разработки и формирования обновленных учебных программ, соответствующих современным вызовам и реалиям.

Работа представлена в форме доклада на Международном круглом столе БРИКС «Цифровое общество: тенденции, возможности и риски», который состоялся

Abstract: The paper discusses pressing problems and challenges to the modern digital society from the viewpoint of cybersecurity specialists and their professional activities. It is stated that cybersecurity specialists need an adequate level of the required specific professional competences to successfully overcome the noted problems and challenges. Therefore, such competences should be managed by the necessary study courses and modules in the cybersecurity and information security curricula of universities, colleges, and other institutions of higher education. A comparative analysis of cybersecurity curricula of several universities and colleges of BRICS countries (namely, Russia, China, and India) conducted in the paper reveals the lack of such study courses in the analyzed curricula. The paper concludes with several pivotal questions on prospective designs of the cybersecurity curricula that should help form and develop the required professional competences.

This work was presented as a speaker paper at the International BRICS Roundtable «Digital Society: Trends, Opportunities & Risks», held on August 22, 2024, at the Altai State University, Barnaul, Russia.

Keywords: information security, technological leadership, educational technology, competences, study curriculum, active learning.

22 августа 2024 года в Алтайском государственном университете, г. Барнаул, Россия.

Ключевые слова: информационная безопасность, технологическое лидерство, образовательные технологии, компетенции, учебные программы, активное обучение.

Для цитирования: Мансуров А.В. Вызовы цифровому обществу: проблемы подготовки специалистов по защите информации // Проблемы правовой и технической защиты информации. 2024. №12. С.52-57.

For citation: Mansurov A.V. Challenges to Digital Society: Problems of Training Information Security Specialists // Legal and Technical Problems of Information Protection. 2024. No. 12. P.52-57.

Современное цифровое общество, связанные с ним сервисы и информационные системы испытывают целый ряд очень непростых вызовов, которые связаны с самыми разными сторонами и сферами жизни и деятельности современного человека и общества. Развитие информационно-телекоммуникационных технологий, совершенствование средств и решений, применяющихся в современных информационных системах, а также быстро меняющиеся условия цифровизации формируют проблемное поле для деятельности специалистов в области информационной безопасности [1-3]. Среди наиболее актуальных вызовов и угроз можно определить следующие:

1) Широкое распространение и насыщенность всевозможными «ботами» современных сервисов и систем. Здесь идет речь о уже сложившейся практике использования чат-ботов как первой линии взаимодействия человека с цифровым сервисом или информационной системой, а также использование ботов как основы для построения несложных интерактивных информационных систем, например, простые обучающие сервисы, или же сервисы интерактивной помощи и решения проблем. Не следует также забывать о том, что большое количество ботов активно участвует в формировании и перераспределении информационных потоков в различных системах обмена сообщениями и сервисов социальных сетей, таких как Телеграм, Фейсбук, ВКонтакте и т.п. Это стало возможным за счет большого количества открытых и доступных для использования сторонних бот-платформ, которые можно интегрировать в свои собственные информационные системы или сторонние цифровые платформы и сервисы при помощи доступного для использования API-интерфейса.

Привлечение сторонних бот-платформ привело к открывшемуся «окну возможностей» для осуществления взломов и целенаправленных атак злоумышленников на функционирование таких бот-сервисов. Это, в свою очередь, приводит к некорректному функционированию и деградации работы интерфейсов информационных систем, дает возможность для злоумышленников вбрасывать и распространять заведомо ложные информационные сообщения, а также получать доступ к различной «чувствительной» информации, такой как персональные данные, конфиденциальная информация. В частности, одна из последних атак злоумышленников на бот-платформу FleetBot привела к рассылке заведомо ложной информации по множеству новостных и информационных каналов популярной системы обмена сообщениями Телеграмм [4].

2) Популяризация и массовое упрощение в использовании систем искусственного интеллекта и искусственных нейронных сетей (ИНС). В настоящее время достаточного много

«юзер-френдли» сервисов на базе ИНС ЧатГПТ, в открытом доступе есть возможность поработать с сервисами Яндекс.Шедеврум и набором готовых к использованию уже обученных ИНС от компании Яндекс. Активно внедряются и используются технологии искусственного интеллекта наряду или совместно с чат-ботами в различных интерфейсах современных информационных систем, позволяя тем самым выстраивать сложные диалоговые взаимодействия с пользователями. При помощи ИНС и технологий искусственного интеллекта, машинного обучения в настоящее время можно создавать не только различные красивые изображения или видео, в руках злоумышленников эти технологии и решения открывают бесконечные просторы для манипулирования искаженной и заранее фальшивой информацией, а также подделки голоса, внешности и иных биометрических данных, что ставит под вопрос надежность работы этапа биометрической идентификации и аутентификации в современных системах [5]. Нередки на сегодня случаи, когда при помощи т.н. «дипфейкинга» обычных граждан и сотрудников компаний заставляют выполнять определенные действия, полностью подделывая голоса собеседников или (как в случае с сотрудником Гонгконгской международной компании) целую видеоконференцию, в которой кроме него были искусственно созданы весь остальной руководящий персонал [6].

3) Доступность «Интернета вещей» (IoT). Очень многие устройства из числа IoT используются сейчас повсеместно, зачастую без адекватной оценки того, насколько надежно и защищено от взлома и последующего неправомерного использования такое эксплуатируемое устройство, насколько качественно выполнена программная составляющая таких устройств и насколько сложно будет злоумышленнику подключиться к таким устройствам и проэксплуатировать возможные существующие уязвимости.

Отдельно надо заметить, что значительная часть современных устройств из мира IoT позиционируются как интеллектуальные, с возможностью распознавания голоса. Но при этом остается совершенно неясным, насколько такие интеллектуальные возможности могут быть использованы в совершенно незапланированных режимах и сформированных злоумышленниками схемах. В частности, использование популярных в России СмартТВ с голосовым интерфейсом или звуковых систем «Яндекс.Алиса» с голосовым помощником Алиса от компании Яндекс не гарантирует однозначно того, что возможности для получения голосовых команд нельзя использовать для записи звука, речи, переговоров и т.п. с последующей отправкой записанных данных нужному получателю (т.е. злоумышленнику). Да и наличие т.н. «базы знаний» для работы интеллектуальных помощников где-то далеко в облаке или в сети на площадках компаний не гарантирует отсутствие утечек данных или, наоборот, принципиальное использование компаниями-производителями таких возможностей своих решений с какими-либо корыстными намерениями.

4) «Базированность» бизнес-процессов и рабочих алгоритмов компаний на популярные и доступные решения сторонних производителей. К таковым относятся популярные мессенджеры, службы и приложения для работы с социальными сетями и средства для организации удаленной работы и видеоконференций. Принудительный запрет на использование уже «полюбившегося» или устоявшегося в рабочих цепочках и бизнес-процессах стороннего решения (как это сложилось, например, в результате зарубежных санкций для предприятий России) приводит к последствиям, на преодоления которых приходится тратить не запланированные на подобное силы и средства. К тому же, нет никаких гарантий использования сторонних продуктов и решений в т.н. «шпионских» целях со стороны силовых структур и производителей таких программных продуктов и решений, что немаловажно для

предотвращения случаев промышленного шпионажа или иных утечек данных.

Учитывая обозначенные проблемы и вызовы, важным является понимание того, насколько к ним подготовлена образовательная составляющая процесса подготовки специалиста по защите информации и формирования требуемых актуальных компетенций. В частности, для образовательных учреждений критичными являются следующие моменты:

– Получение обучаемыми специалистами по защите информации необходимых компетенций, чтобы предвидеть, понимать, анализировать и решать проблемы и вызовы современности.

– Наличие специализированных учебных дисциплин (модулей, курсов, …) в программах подготовки специалистов по информационной безопасности, которые адресно охватывают и изучают обозначенные ранее проблемы с формированием требуемых компетенций.

В ходе данного исследования был проведен сравнительный анализ содержимого учебных программ подготовки специалистов по информационной безопасности (или кибербезопасности) уровня бакалавриата (как программ подготовки основной группы специалистов) в странах БРИКС. Наиболее детально анализировались учебные программы вузов Российской Федерации, и двух самых близких к России стран БРИКС – Китая и Индии, на основании данных открытых источников – журнальных публикаций [7-9] и веб-сайтов учебных заведений, осуществляющих подготовку специалистов и публикующих содержимое своих образовательных программ.

В соответствии с рисунком 1, программы подготовки специалистов по информационной безопасности в России, Индии и Китае (основные страны БРИКС) во многом схожи. В России, в Китае и в Индии программы формируют значимый фундаментальный естественно-научный базис знаний и содержат в своей основной ядерной части необходимые дисциплины, которые «отвечают» за конкретные направления деятельности будущего специалиста. В частности, это криптография, обеспечение безопасности информационных систем, сетевая безопасность, нормативы и регулирование в области защиты информации. В качестве неотъемлемого элемента ядерной части присутствуют также дисциплины, формирующие знания и компетенции в области машинного обучения и искусственного интеллекта (ИНС), чтобы специалист по защите информации имел представление о том, как работают и как используются современные достижения технологического прогресса.

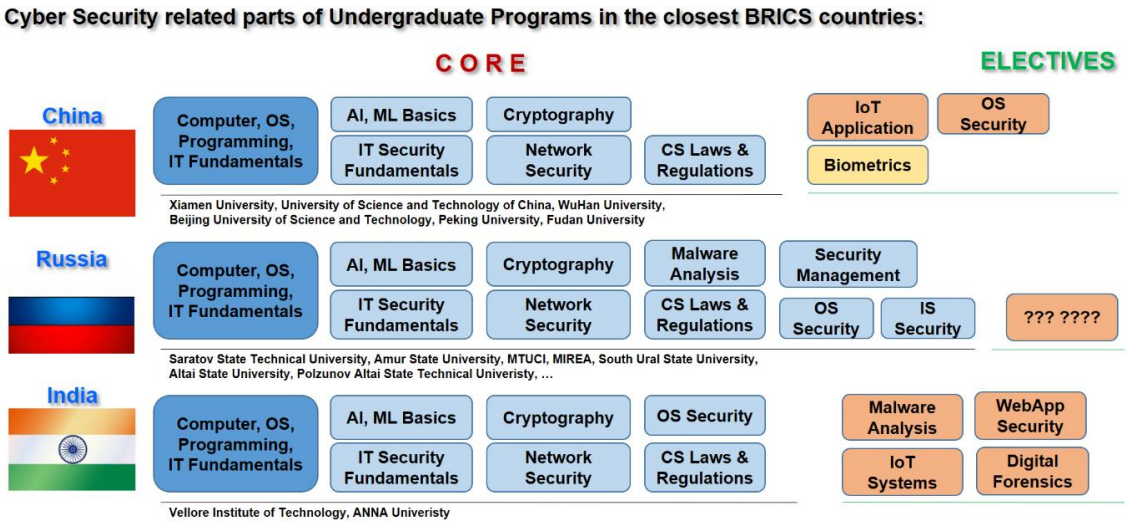

Рисунок 1. Компоненты образовательных программ в области информационной безопасности стран БРИКС – России, Китая и Индии

В то время как элективная составляющая в России пока что достаточно однозначно и четко не представлена, и очень часто заполнена дисциплинами, напрямую не связанными с вопросами защиты информации, в программах китайских и индийских вузов элективная часть представлена теми вариантами дисциплин, которые необходимы для узкопрофильной деятельности специалиста-безопасника. В частности, можно увидеть основы функционирования систем «Интернета вещей», цифровую форензику, биометрию и т.п.

К сожалению, детальных составляющих учебных планов по университетам и колледжам Бразилии и Южной Африки в открытом доступе найти не удалось, либо же в этих вузах ведется базовая подготовка специалистов в области компьютерных наук (бакалавр Computer Science) с рядом элективов в виде курсов, связанных с вопросами безопасности и защиты информации.

Резюмируя изложенную информацию, можно сделать вывод, что специализированная подготовка и специализированные дисциплины, так или иначе связанные с обозначенными в статье проблемами, в актуальных образовательных программах в своей основной массе отсутствуют. Подготовленный на сегодняшний момент специалист по защите информации вынужден либо получать недостающие знания и компетенции самостоятельно, либо использовать те небольшие фрагменты, которые могут содержаться в какой-либо из учебных дисциплин основной программы или электива.

Актуальными на повестке дня для учебных заведений, осуществляющих подготовку специалистов в области информационной безопасности, остаются следующие вопросы:

1) Необходимы ли специализированные дисциплины, содержащие необходимые знания и формирующие требуемые компетенции, для ответа на указанные ранее вызовы и проблемы?

2) Должны ли такие дисциплины, если таковые должны быть в учебных программах, быть включены как элективы или же являться непосредственно ядерными (обязательными) дисциплинами учебных программ?

3) Целесообразно ли, учитывая собственную специфику каждой из стран БРИКС в формировании учебных программ, организовать и поддерживать ежегодный обмен студентами (обучающимися по программам информационной безопасности) между университетами и колледжами стран БРИКС и поможет ли такой обмен более эффективно решать уже существующие и потенциально возможные проблемы и вызовы цифровому обществу и его информационным системам?

Ответы на данные вопросы помогут обеспечить формирование эффективной учебной программы подготовки специалистов в области информационной безопасности в условиях актуальных вызовов современности с формированием необходимых компетенций для последующей профессиональной деятельности специалистов.

Библиографический список

1. *Минакова Н.Н., Поляков В.В. Модель практико-ориентированной подготовки специалистов по информационной безопасности в Алтайском государственном университете. Сб. науч. статей VII Междунар. научно-практ. конф. «Многоядерные процессоры, параллельное программирование, ПЛИС, системы обработки сигналов». Барнаул, 10-11 марта 2017 г. Барнаул. 2017. С. 251-256.*

2. *Минакова Н.Н., Поляков В.В., Мансуров А.В. Подготовка специалистов по информационной безопасности в условиях трансформации университета в центр инновационного, технологического и социального развития региона. Доклады VII Пленума СибРОУМО и матер. XVI Междунар. научно-практич. конф. «Проблемы информационной безопасности государства,*

общества и личности». Томск, 6-10 июня 2018 г. Томск: В-Спектр, 2018. С. 13-14.

3. Минакова Н.Н., Мансуров А.В., Поляков В.В. Подготовка специалистов по информационной безопасности в условиях формирования технологического лидерства // Проблемы правовой и технической защиты информации. 2023. №11. С. 35-39.

4. Хакеры взломали чат-бот в Telegram и начали массово рассылать сообщения // РБК: сайт. URL: https://www.rbc.ru/technology_and_media/21/07/2024/669cce1c9a7947034b974cb9 (дата обращения: 10.09.2024)

5. Cybersecurity threatscape: Q1 2024 // Positive Technologies: сайт. URL: https://global.ptsecurity.com/analytics/cybersecurity-threatscape-2024-q1 (дата обращения: 10.09.2024)

6. Chen H., Magramo K. Finance worker pays out $25 million after video call with deepfake 'chief financial officer' // CNN: сайт. URL: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html (дата обращения: 10.09.2024)

7. Yang S. C. A Curriculum Model of Cybersecurity Bachelor's Programs in AACSB-Accredited Business Schools in the US. // Journal of Information Systems Education, Vol. 35, N. 3, pp. 313-324. URL: https://doi.org/10.62273/FRJE33 (дата обращения: 10.09.2024)

8. Djedjiga M., Sohail A., Madjid M. Cybersecurity Curriculum Design: A Survey // In: Pan Z., Cheok A., Müller W., Zhang M., El Rhalibi A., Kifayat K. (eds) Transactions on Edutainment XV. Lecture Notes in Computer Science, Vol. 11345. Springer, Berlin, Heidelberg. URL: https://doi.org/10.1007/978-3-662-59351-6_9 (дата обращения: 10.09.2024)

9. Huaying Chen H., Maynard S., Ahmad A. A comparison of information security curricula in China and the USA. // Proceedings of the 11th Australian Information Security Management Conference, ISM 2013. URL: https://www.researchgate.net/publication/264898151_A_comparison_of_information_security_curricula_in_China_and_the_USA (дата обращения: 10.09.2024)