DOI: 10.24412/2076-1503-2021-10-334-338
NIION: 2018-0076-10/21-288
MOSURED: 77/27-023-2021-10-486

УДК 343

АНУРЬЕВА Мария Сергеевна,
старший преподаватель
кафедры математического моделирования
и информационных технологий Института математики,
физики и информационных технологий ФГБОУ ВО
«Тамбовский государственный университет
им. Г.Р. Державина»,
e-mail: anuryeva@mail.ru

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО РАССЛЕДОВАНИЮ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ В РОССИИ И ЗАРУБЕЖНЫХ СТРАНАХ

Аннотация. *В статье рассматривается возрастание масштабов компьютерной преступности, прежде всего, в кредитно-финансовой сфере, что отражено в Доктрине информационной безопасности Российской Федерации. Одним из перспективных направлений в компьютерной криминалистике, по мнению зарубежных экспертов, является модернизация профессиональной подготовки и сертификации специалистов по расследованию цифровых преступлений. Потребность общества в специалистах, способных проводить компьютерную экспертизу и обладающих навыками расследования цифровых преступлений, чрезвычайно высока. Сделан вывод о том, что имеется необходимость расширения подготовки по компьютерной экспертизе, в т.ч. увеличения набора по соответствующему профилю образовательной программы, а также внедрения дисциплин по расследованию цифровых преступлений в учебные планы всех образовательных программ по информационной безопасности.*

Ключевые слова: *информационная безопасность, защита информации, подготовка специалистов, расследование цифровых преступлений, компьютерная экспертиза.*

ANUR'EVA Mariya Sergeevna,
Senior Lecturer at the Department of Mathematical Modeling
and Information Technology of the Institute of Mathematics,
Physics and Information Technology,
Derzhavin Tambov State University

TRAINING OF SPECIALISTS IN THE INVESTIGATION OF DIGITAL CRIMES IN RUSSIA AND FOREIGN COUNTRIES

Annotation. *The article examines the increasing scale of computer crime, primarily in the credit and financial sphere, which is reflected in the Information Security Doctrine of the Russian Federation. One of the promising areas in computer forensics, according to foreign experts, is the modernization of professional training and certification of specialists in the investigation of digital crimes. The need of society for specialists capable of conducting computer expertise and having the skills to investigate digital crimes is extremely high. It is concluded that there is a need to expand training in computer expertise, including increasing enrollment in the relevant profile of the educational program, as well as the introduction of disciplines on the investigation of digital crimes in the curricula of all educational programs on information security.*

Key words: *information security, information protection, training of specialists, investigation of digital crimes, computer expertise.*

В июле 2021 г. Указом Президента РФ была утверждена Стратегия национальной безопасности РФ, пришедшая на смену ранее действовавшей Стратегии. Новая Стратегия выделяет национальные интересы РФ и стратегические национальные приоритеты, среди которых развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия, стоят наравне со сбережением народа и развитием человеческого потенциала, защитой конституционного строя, поддержанием гражданского мира и согласия в стране [12].

Другой основополагающий документ в сфере информационной безопасности и защиты инфор-

мации – Доктрина информационной безопасности – характеризуя основные информационные угрозы и состояние информационной безопасности, указывает на возрастание масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличение число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в т.ч. в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений, становятся все изощреннее [13].

Вместе с тем, в Доктрине отмечается, что состояние информационной безопасности в области науки, технологий и образования характеризуется низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности [13].

Компьютерная преступность, безусловно, общемировая угроза, масштабам которой характерен экспоненциальный рост. Так, в 2017 г. доля таких преступлений от числа всех зарегистрированных в России преступных деяний составляла 4.4% [3]. В отчете МВД России о состоянии преступности по итогам пяти месяцев 2021 г. сообщается, что в данном отчетном периоде удельный вес преступлений в сфере высоких технологий увеличился до 26.8%, а в январе-мае 2020 г. этот же показатель составлял 21.7% [7].

В США ежегодно только 3 из 1000 совершенных киберпреступлений (что составляет менее 1%) раскрываются и доходят до обвинительного приговора в суде (для сравнения: показатель раскрытия преступлений против собственности составлял примерно 18%, за насильственные преступления - 46%) [20].

Число успешных кибератак продолжает расти, угрожая финансовой и личной безопасности во всем мире [19]. Цифровая криминалистика переживает смену парадигмы, в которой доказательства часто имеют весомую значимость и при низкой квалификации специалиста, проводящего экспертизу и поиск цифровых доказательств, могут оказаться некорректными для предоставления в суде. Зарубежные специалисты отмечают, что в целях оптимизации распределения ресурсов и более эффективного определения приоритетов киберкриминалистики, необходима работа в следующих перспективных направлениях:

- модернизация профессиональной подготовки и сертификации специалистов по расследованию цифровых преступлений;
- поддержка и совершенствование облачной и мобильной криминалистики;
- поддержка и совершенствование инструментов с открытым исходным кодом;
- исследования в области шифрования, вредоносных программ и запутывания следов;
- обновление нормативно-правового регулирования;
- эффективное взаимодействие лабораторий, осуществляющих расследование цифровых преступлений с правоохранительными органами;
- увеличение числа соответствующих специалистов и объёмов финансирования [21].

Исходя из вышеизложенного, потребность общества в специалистах, способных проводить компьютерную экспертизу и обладающих навыками расследования цифровых преступлений, чрезвычайно высока.

Ранее проведенное исследование системы подготовки специалистов в области информационной безопасности в США и Великобритании показывает высокую популярность программ по компьютерной экспертизе и расследованию цифровых преступлений [2; 16]. Так, к самым популярным образовательным программам бакалавриата среди всех программ по информационной безопасности относятся программы по расследованию цифровых преступлений (т.е. именно такие программы встречаются даже чаще, чем программы по обеспечению безопасности в компьютерных системах и сетях).

Образовательные программы по информационной безопасности во Франции [17] и Германии [18] не так распространены, как в вышерассмотренных странах, однако и в этих государствах все соответствующие программы включают в себя дисциплины и темы, связанные с обучением навыкам компьютерной экспертизы и поиска цифровых доказательств.

В отечественной системе подготовки профессионального образования в области информационной безопасности федеральными государственными образовательными стандартами высшего образования (далее – ФГОС ВО) предусмотрен профиль «Компьютерная экспертиза» направления подготовки специалистов 10.05.05 «Безопасность информационных технологий в правоохранительной сфере». Вместе с тем, указанный профиль не получил широкого распространения в отечественных вузах. В этой связи, ежегодно выпускается весьма незначительное количество специалистов по проведению компьютерной экспертизы и расследованию преступлений в цифровой среде.

Вместе с тем, ФГОС ВО по другим направлениям подготовки УГСНП 10.00.00 «Информационная безопасность» не подразумевает наличие общепрофессиональных компетенций по форми-

рованию способностей проведения компьютерной экспертизы и поиску цифровых доказательств, что означает тот факт, что включение соответствующей дисциплины в учебный план образовательных программ по информационной безопасности возможно только по желанию образовательной организации, реализующей данную программу.

Такое различие с зарубежными образовательными программами по информационной безопасности, вероятно, обусловлено историческим аспектом: подготовка будущих специалистов по компьютерной экспертизе в рассматриваемых зарубежных странах раньше, чем в России перестала иметь «закрытый» характер, и сегодня многие вузы предоставляют свои образовательные ресурсы в данном направлении.

Другим отличием в содержании отечественных и зарубежных образовательных программ по информационной безопасности, вытекающим из выше обозначенного, является небольшой объём дисциплин в отечественных образовательных программах, связанных с правоприменительными технологиями в области информационной безопасности.

Вместе с тем, все отечественные образовательные программы содержат дисциплины по правовой защите информации, в рамках которых рассматривается базовое законодательство в сфере информационной безопасности, однако, продолжает остро стоять проблема правоприменительных технологий в информационной сфере, в частности, в области информационной безопасности. При этом отмечается, что трансформация образовательного пространства в условиях цифровой экономики сопровождается появлением новых угроз конституционным правам и свободам граждан, а также национальной безопасности страны в целом [8 -10].

Специалист по обеспечению информационной безопасности в процессе профессиональной деятельности постоянно обязан ориентироваться на регламентирующие нормативно-правовые акты. Правовая компетентность, будучи неотъемлемой составляющей общей культуры современного специалиста, позволяет ему успешно выполнять различные виды профессиональной деятельности [11]. Правовое обучение стало обязательной важной составной частью общей подготовки любого специалиста, когда без знания правовых норм, регулирующих профессиональную деятельность, современный специалист не может на должном уровне выполнять свои служебные обязанности [11].

Так, специалист по информационной безопасности свою профессиональную деятельность, помимо федерального законодательства, должен ориентировать на требования регуляторов. Зачастую такие требования могут вызвать ряд сложностей и противоречий (например, в выполнении требований Федерального закона «О персональных данных» [6] и других нормативно-правовых актов [5].

Законодательство в сфере информационных правоотношений и защиты информации претерпевает постоянные изменения: принимаются новые законы, например, регулирующие вопросы защиты информации в критической инфраструктуре; ранее принятые претерпевают существенные корректировки:

- в части защиты персональных данных [15];
- лицензировании деятельности в сфере информационной безопасности [14];
- требований Роскомнадзора по ограничению интернет-ресурсов, содержащих информацию, распространение которой в РФ запрещено [4] и др.

Эти корректировки достаточно динамичны и, с одной стороны, диктуют необходимость знаний и понимания причин, направленности и тенденций происходящих изменений законодательства; с другой – необходимость формирования умений и навыков в применении действующих норм и своевременного реагирования на новые редакции нормативно-правовой базы.

В данном аспекте будет полезен опыт Великобритании. Отметим, что Великобритания – это единственная страна из рассмотренных, в которой возможно получение степени магистра права после успешного завершения образовательной программы в области информационной безопасности. Образовательные программы бакалавриата по законодательству в сфере информационных систем, как правило, являются комбинированными [1].

Учебный план условно можно разделить на две части:

- в первую включают дисциплины базовой программы по юриспруденции («Контракты», «Юридические методы и навыки», «Государственное и муниципальное право», «Коммерческое законодательство», «Международное законодательство в области электронной коммерции»);
- во вторую – дисциплины, связанные как общими вопросами информатики («Принципы программирования», «Базы данных», «Разработка веб-приложений»), так и конкретными областями информационной безопасности («Киберпреступность» и др.).

Таким образом, назрела объективная потребность общества в специалистах, способных проводить поиск цифровых доказательств и расследовать компьютерные преступления. На данный момент реализуемые в России образова-

тельные программы по информационной безопасности не готовят соответствующих специалистов в необходимом объёме. Необходимо расширять подготовку по профилю «Компьютерная экспертиза» направления подготовки специалистов 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», а также внедрять дисциплины по расследованию цифровых преступлений в учебные планы образовательных программ УГСНП 10.00.00 «Информационная безопасность».

Список литературы:

[1] Анурьева М.С. Подходы к формированию содержания дисциплин по правовой защите информации за рубежом // Гаудеамус. – 2014. – № 2 (24). – С. 124 - 129.

[2] Анурьева М.С., Чванова М.С. Система образования в области информационной безопасности в Великобритании // Преподавание информационных технологий в Российской Федерации: материалы IX Всеросс. конф. – Саратов, 2011. – С. 67 - 70.

[3] Дерюгин Р.А. Киберпреступность в России: современное состояние и актуальные проблемы // Вестник Уральского юридического института МВД России. – 2019. – № 2. – С. 46 - 49.

[4] Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено [Электронный ресурс]. URL: https://eais.rkn.gov.ru. (дата обращения: 27.08.2021).

[5] Лукацкий А.В. Регулирование безопасности в России усиливается // Директор информационной службы. – 2011. – № 07 [Электронный ресурс]. URL: https://www.osp.ru/cio/2011/07/13009726/ (дата обращения: 27.08.2021).

[6] Материалы вебинара «Сложности и спорные вопросы реализации закона «О персональных данных» [Электронный ресурс]. URL: https://youtu.be/WKUueUAKfS8 (дата обращения: 27.08.2021).

[7] МВД России публикует данные о состоянии преступности по итогам пяти месяцев 2021 года [Электронный ресурс]. URL: https://мвд.рф/news/item/24738876 (дата обращения: 27.08.2021).

[8] Морозов А.В. Проблема информационной безопасности личности в условиях цифрового образовательного пространства // Учёные записки ИУО РАО. – 2018. – № 4 (68). – С. 90 - 94.

[9] Морозов А.В. Проблема национальной безопасности России в условиях цифровизации образовательного пространства // Профессиональное образование в современном мире. – 2019. – Т. 9. – № 2. – С. 2663 - 2673.

[10] Морозов А.В. Трансформация образовательного пространства в условиях цифровой экономики // В сб.: Электронное обучение в непрерывном образовании 2019: VI Междунар. науч.-практ. конф., посвященная памяти А.Н. Афанасьева. – Ульяновск, 2019. – С. 338 - 345.

[11] Морозов А.В., Анучкин В.А. Правовое обучение современной молодёжи как одна из важнейших составляющих её духовно-нравственного развития // Социально-экономические и технические системы. – 2016. – № 5 (72). – С. 251 - 261.

[12] Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 27.08.2021).

[13] Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 27.08.2021).

[14] Федеральный закон «О лицензировании отдельных видов деятельности» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_113658/ (дата обращения: 27.08.2021).

[15] Федеральный закон «О персональных данных» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 27.08.2021).

[16] Чванова М.С., Анурьева М.С. Подготовка кадров в области информационной безопасности в США // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2012. – № 8 (112). – С. 126 - 133.

[17] Чванова М.С., Анурьева М.С. Подготовка специалистов в области информационной безопасности во Франции // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2012. – № 7 (111). – С. 159 - 165.

[18] Чванова М.С., Анурьева М.С. Система высшего образования в ФРГ. Подготовка специалистов в области информационной безопасности // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2012. – № 6 (110). – С. 78 - 84.

[19] Ibragimov I.D., Neif N.M., Nikolaeva Y.V., etc. Strategy And Tactics of Students Readiness Formation to Counter Cyber Extremist Activities // Modern journal of language teaching methods. – 2018. – Т. 8. – Вып. 5. – Pp. 127 - 140.

[20] Gaskew B. Cyber Enforcement in Four Key States. – Third Way. – 2019 [Электронный ресурс].

URL: http://www.jstor.org/stable/resrep20152 (дата обращения: 27.08.2021).

[21] Harichandran V., Breitinger F., Baggili I., Marrington A. A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later // Computers & Security. – 2016. – № 57. – Pp. 1 - 13.

Spisok literatury:

[1] Anur'eva M.S. Podhody k formirovaniyu soderzhaniya disciplin po pravovoj zashchite informacii za rubezhom // Psihologo-pedagogicheskij zhurnal Gaudeamus. – 2014. – № 2 (24). – S. 124 - 129.

[2] Anur'eva M.S., Chvanova M.S. Sistema obrazovaniya v oblasti informacionnoj bezopasnosti v Velikobritanii // Prepodavanie informacionnyh tekhnologij v Rossijskoj Federacii: materialy IX Vseros. konferencii. – Saratov, 2011. – S. 67 - 70.

[3] Deryugin R.A. Kiberprestupnost' v Rossii: sovremennoe sostoyanie i aktual'nye problemy // Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii. – 2019. – № 2. – S. 46 - 49.

[4] Edinyj reestr domennyh imen, ukazatelej stranic sajtov v seti Internet i setevyh adresov, pozvolyayushchih identificirovat' sajty v seti Internet, soderzhashchie informaciyu, rasprostranenie kotoroj v Rossijskoj Federacii zapreshcheno [Elektronnyj resurs]. URL: https://eais.rkn.gov.ru. (data obrashcheniya: 27.08.2021).

[5] Lukackij A.V. Regulirovanie bezopasnosti v Rossii usilivaetsya // Direktor informacionnoj sluzhby. – 2011. – № 07 [Elektronnyj resurs]. URL: https://www.osp.ru/cio/2011/07/13009726/ (data obrashcheniya: 27.08.2021).

[6] Materialy vebinara «Slozhnosti i spornye voprosy realizacii zakona «O personal'nyh dannyh» [Elektronnyj resurs]. URL: https://youtu.be/WKUueUAKfS8 (data obrashcheniya: 27.08.2021).

[7] MVD Rossii publikuet dannye o sostoyanii prestupnosti po itogam pyati mesyacev 2021 goda [Elektronnyj resurs]. URL: https://mvd.rf/news/item/24738876 (data obrashcheniya: 27.08.2021).

[8] Morozov A.V. Problema informacionnoj bezopasnosti lichnosti v usloviyah cifrovogo obrazovatel'nogo prostranstva // Uchyonye zapiski IUO RAO. – 2018. – № 4 (68). – S. 90 - 94.

[9] Morozov A.V. Problema nacional'noj bezopasnosti Rossii v usloviyah cifrovizacii obrazovatel'nogo prostranstva // Professional'noe obrazovanie v sovremennom mire. – 2019. – T. 9. – № 2. – S. 2663 - 2673.

[10] Morozov A.V. Transformaciya obrazovatel'nogo prostranstva v usloviyah cifrovoj ekonomiki // V sbornike: Elektronnoe obuchenie v nepreryvnom obrazovanii 2019: VI Mezhdunar. nauch.-prakt. konf., posvyashchennaya pamyati A.N. Afanas'eva. – Ul'yanovsk, 2019. – S. 338 - 345.

[11] Morozov A.V., Anuchkin V.A. Pravovoe obuchenie sovremennoj molodyozhi kak odna iz vazhnejshih sostavlyayushchih eyo duhovno-nravstvennogo razvitiya // Social'no-ekonomicheskie i tekhnicheskie sistemy. – 2016. – № 5 (72). – S. 251 - 261.

[12] Ukaz Prezidenta Rossijskoj Federacii ot 02.07.2021 № 400 «O Strategii nacional'noj bezopasnosti Rossijskoj Federacii» [Elektronnyj resurs]. URL: http://www.kremlin.ru/acts/bank/47046 (data obrashcheniya: 27.08.2021).

[13] Ukaz Prezidenta Rossijskoj Federacii ot 05.12.2016 № 646 «Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii» [Elektronnyj resurs]. URL: http://www.kremlin.ru/acts/bank/41460 (data obrashcheniya: 27.08.2021).

[14] Federal'nyj zakon RF «O licenzirovanii otdel'nyh vidov deyatel'nosti» // [Elektronnyj resurs]. URL: http://www.consultant.ru/document/cons_doc_LAW_113658/ (data obrashcheniya: 27.08.2021).

[15] Federal'nyj zakon RF «O personal'nyh dannyh» [Elektronnyj resurs]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (data obrashcheniya: 27.08.2021).

[16] Chvanova M.S., Anur'eva M.S. Podgotovka kadrov v oblasti informacionnoj bezopasnosti v SSHA // Vestnik Tambovskogo universiteta. Seriya: Gumanitarnye nauki. – 2012. – № 8 (112). – S. 126 - 133.

[17] Chvanova M.S., Anur'eva M.S. Podgotovka specialistov v oblasti informacionnoj bezopasnosti vo Francii // Vestnik Tambovskogo universiteta. Seriya: Gumanitarnye nauki. – 2012. – № 7 (111). – S. 159 - 165.

[18] Chvanova M.S., Anur'eva M.S. Sistema vysshego obrazovaniya v FRG. Podgotovka specialistov v oblasti informacionnoj bezopasnosti // Vestnik Tambovskogo universiteta. Seriya: Gumanitarnye nauki. – 2012. – № 6 (110). – S. 78 - 84.

[19] Ibragimov I.D., Neif N.M., Nikolaeva Y.V., etc. Strategy And Tactics of Students Readiness Formation to Counter Cyber Extremist Activities // Modern journal of language teaching methods. – 2018. – T. 8. – Vyp. 5. – Pp. 127 - 140.

[20] Gaskew B. Cyber Enforcement in Four Key States. – Third Way. – 2019 [Elektronnyj resurs]. URL: http://www.jstor.org/stable/resrep20152 (data obrashcheniya: 27.08.2021).

[21] Harichandran V., Breitinger F., Baggili I., Marrington A. A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later // Computers & Security. – 2016. – № 57. – Pp. 1 - 13.