СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

CONTEMPORARY TENDENCIES IN PROFESSIONAL EDUCATION DEVELOPMENT

УДК/UDC 378

М. С. Анурьева

M. Anurieva

ИСТОРИКО-ЛОГИЧЕСКИЙ АНАЛИЗ СТАНОВЛЕНИЯ СИСТЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

HISTORICAL AND LOGICAL ANALYSIS OF THE FORMATION OF THE TRAINING SYSTEM OF SPECIALISTS IN THE FIELD OF THE INFORMATION SECURITY

Введение. Компоненты образовательной среды и профессиональной деятельности специалистов по защите информации непрерывно трансформируются под влиянием процессов развития информационного общества. В статье проведен анализ влияния становления деятельности по обеспечению информационной безопасности (ИБ) на формирование современной образовательной среды, прежде всего на содержание образования, для подготовки специалистов по защите информации.

Методология. Историческая хронология событий, связанная с подготовкой специалистов в области информационной безопасности, рассматривается с точки зрения историко-логического подхода. Анализ дает возможность сделать вывод о том, что развитие системы подготовки специалистов по ИБ зависит от исторически сложившейся национальной системы, сформированной в той или иной стране.

Результаты. В статье проанализированы подходы к периодизации деятельности по защите информации в России и за рубежом. На основе анализа работ отечественных ученых, ретроспективного анализа государственных образовательных стандартов и перечней направлений и специальностей высшего образования в области подготовки специалистов по защите информации выделены пять этапов развития системы подготовки специалистов по ИБ в России. Рассмотрены отдельные аспекты исторического развития зарубежных систем ИБ (США, Великобритания, Франция) и их влияние на становление современной системы подготовки специалистов.

Заключение. Автором выявлен ряд соответствий в развитии национальной системы защиты информации и содержании современной подготовки специалистов.

Introduction. Components of the educational environment and professional activities of information security professionals are continuously transformed under the influence of the development of the information society. The article analyzes the impact of the development of activities

to ensure state information security (IB) on the formation of a modern educational environment, primarily on the content of education, for the training of information protection professionals.

Materials and Methods. The historical chronology of events, connected with the training of specialists in the field of information security, is considered from the point of view of the historical-logical approach. The analysis makes it possible to conclude that the development of the system of training specialists in information security depends on the historically established national system formed in a particular country.

Results. The article analyzes the approaches to the periodization of the formation and development of information protection activities in Russia and abroad. Based on the analysis of the domestic scientists' work, a retrospective analysis of state educational standards and lists of directions and specialties of higher education in the field of training specialists in the protection of information, five stages of the development of the system of training specialists in information security in Russia are identified. Separate aspects of the historical development of foreign IS systems in the state (the USA, Great Britain, France) and their influence on the formation of a modern system of training specialists are considered.

The conclusions. The author identified a number of correspondences between the development of the national information protection system and the content of modern training of specialists.

Ключевые слова: информационная безопасность, защита информации, подготовка специалистов, историко-логический подход.

Keywords: information security, protection of information, training of specialists, historical and logical approach.

Введение

Одной из составляющих государственной политики в области информационной среды является подготовка специалистов в сфере информационной безопасности (ИБ). Сегодня отмечена необходимость глубокого анализа интеграционных процессов в различных направлениях подготовки по ИБ в связи с развитием ИТ-отрасли и ее проникновением как в ключевые компоненты профессиональной деятельности, так и компоненты образовательной среды самого вуза. Специфика формирования образовательной среды будущего специалиста определяется прежде всего особенностями его будущей профессиональной деятельности. Она в настоящее время трансформируется под влиянием процессов развития информационного общества. Рассмотрим с этой позиции влияние становления деятельности по обеспечению государственной информационной безопасности на формирование современной образовательной среды, прежде всего на содержание образования, для подготовки специалистов по защите информации.

Методология

Рассмотрение исторической хронологии событий, связанных с подготовкой специалистов в области ИБ, целесообразно с точки зрения историко-логического подхода. Предполагается, что историко-логический подход позволит выявить этапы и основные закономерности взаимозависимости системы образования в области ИБ и развития деятельности по защите государственных интересов в информационной сфере.

В то же время не было целью связывать этапы развития подготовки специалистов в области ИБ с точной хронологией. Такие процессы в различных странах не могли формироваться одинаково — отсутствует синхронизация. При этом в настоящее время отдельные тенденции синхронизации наблюдаются как следствие проникновения информационных технологий. Все же наш анализ дает возможность сделать вывод о том, что развитие системы подготовки специалистов по ИБ зависит от исторически сложившейся национальной системы, сформированной в той или иной стране.

Результаты

С целью рассмотрения периодизации системы подготовки специалистов в области ИБ необходимо проанализировать этапы становления развития деятельности по защите информации в России и за рубежом. В.И. Аверченков выделяет три относительно самостоятельных периода, причем в основе деления на этапы лежит эволюция видов носителей информации [6, с. 10].

Первый этап (с древнейших времен) — ученый выделяет развитие криптографических и стенографических методов защиты информации, которые определяются появлением возможности фиксации сообщений на носителях (появление письменности).

Второй этап характеризуется появлением «технических средств обработки информации и передачи сообщений с помощью электрических сигналов и электромагнитных полей» с середины XIX в. и обусловливает развитие инженерно-технических методов обеспечения информационной безопасности.

Третий этап (с середины XX в.) связан с появлением компьютеров и массовой информатизацией общества.

Анализ зарубежных источников показал, что развитие деятельности по защите информации начинается только с середины XX в., то есть с появлением компьютеров. Так, американский исследователь Майк Линетт в статье «История информационной безопасности от прошлого до настоящего времени» [4] первый этап защиты информации относит к 1960-м гг., когда организации начинают защищать свои компьютеры, при этом для защиты терминалов к устройствам были добавлены пароли и несколько уровней защиты, то есть использованы первые программные средства идентификации и аутентификации, а также появляется принцип программного разграничения доступа. Второй этап, 1970-е гг., характеризуется первыми попытками нарушения целостности и конфиденциальности информации, передающейся с помощью информационно-коммуникационных сетей, и появлением единичных компьютерных преступников (хакеров). В 1980-е гг. (третий этап) компьютерные преступления приобретают массовый характер, и правительство принимает более активные меры по борьбе с киберпреступностью, что ведет к развитию правовых мер защиты информации на государственном уровне. Последующие этапы (девяностые, нулевые, десятые годы) Майк Линетт рассматривает с позиции развития компьютерных правонарушений и борьбы правительства с ними.

Аналитик, эксперт в области ИБ Тед Джулиан подходит к выделению этапов деятельности по защите информации с точки зрения реагирования на создание и развитие деструктивных программ (компьютерных вирусов) [3]. Так, первый этап, с точки зрения Теда Джулиана, начинается в конце 1980-х — начале 1990-х гг. и связан с появлением первой вредоносной программы компьютерного вируса («компьютерный червь»), что стало первым распространенным примером атаки на отказ в обслуживании (DoS-атака). Это привело к развитию первых сертификатов безопасности, а также к появлению профилактических и детективных продуктов безопасности (антивирусных программ). Второй этап (1990-е гг.) характеризуется массовыми поражениями компьютерных систем деструктивными программами, в это время активно продолжают развиваться антивирусные технологии, появляются новые методы обнаружения вредоносных программ и борьбы с ними. На третьем этапе (в конце 2000-х гг.) кибератаки стали более целенаправленными в ответ на обнаруженные первые нарушения серийных номеров кредитных карт. В этот период организации стали применять более сложные системы безопасности, использовать комплексный подход к обеспечению ИБ. Четвертый этап (современный) характеризуется тем, что атаковать системы стало намного сложнее за счет усиления мер ИБ.

Таким образом, рассмотренные выше подходы [1; 5] к выделению периодов позволяют сделать вывод о том, что исследователи, прежде всего американские, к деятельности по обеспечению ИБ относят и защиту компьютерных систем и сетей, в отличие от отечественных исследователей, которые до «компьютерной эры» рассматривают становление криптографических и инженерно-технических методов защиты информации.

Подготовка специалистов по защите информации, как и по любым другим направлениям, не может рассматриваться как отдельный элемент вне системы. Развитие технологий, методов, средств обеспечения ИБ оказывает существенное влияние не только на предметную область подготовки специалистов, но и на образовательные технологии. Одновременно с этим этапы становления деятельности по защите информации невозможно рассматривать вне международной системы безопасности в целом и глобальных информационных противоборств в частности.

Мы полагаем, что выделение отдельных событий в мировой истории, оказывающих влияние на развитие системы национальной безопасности (в том числе в информационной сфере) и являющихся ответом на вновь сформированные угрозы безопасности (в том числе информационные), поможет более подробно рассмотреть предметную область историко-логического анализа и выделить этапы становления системы подготовки специалистов по ИБ в России (табл. 1).

Таблица 1

Развитие взаимосвязи в триаде «ситуация в мире» — «развитие методов защиты информации» — «развитие системы подготовки специалистов по информационной безопасности»

Этапы развития системы подготовки специалистов по ИБ	Период	Характеристика этапа в контексте событий в мире	Методы защиты информации	Характеристика системы образования в России
Этап подготовки в закрытых ведомственных учреждениях	До 1940-х гг.	– Развитие разведывательной и контрразведывательной деятельности; — появление технических средств обработки и передачи информации (телефон, телеграф, радио)	– Появление и развитие криптографических методов защиты информации; — появление и развитие инженерно-технических методов защиты информации	Образование в области защиты информации ведется в рамках подготовки агентов только в закрытых ведомственных (чаще военных) государственных учреждениях
Этап подготовки в вузах по закрытым программам	1940-е — 1985 гг.	– Глобальное информационное противоборство («холодная война»); — появление и развитие компьютеров и компьютерных сетей	Появление и развитие программно-аппаратных методов защиты информации	– Появляется совместная закрытая образовательная программа по криптографии ведомственного государственного учреждения (КГБ СССР) и гражданского вуза (МГУ имени М.В. Ломоносова) в 1949 г.; — в 1970-е г. образовательные программы включают отдельные темы по программно-аппаратным методам защиты информации; — в образовательные программы включают дисциплины по техническим и организационно-правовым методам обеспечения безопасности
Этап единичных открытых программ по ИБ в отдельных вузах	1985 — конец 1990-х гг.	– Окончание «холодной войны»; — массовая информатизация всех сфер деятельности общества	Начало становления научно-методологического базиса ИБ	– Появляются единичные открытые программы по ИБ в отдельных вузах; — с 1995 г. появляются первые государственные образовательные стандарты подготовки специалистов в области ИБ
Этап массового внедрения образовательных программ в вузах	2000–2010-е гг.	– Прорыв во внимании к решению проблем ИБ бизнеса и государства как ответ на международный терроризм; — поддержка безопасности информационной составляющей бизнеса; — обострение гуманитарных проблем ИБ	– Активное развитие научно-технических методов защиты информации; — формирование методологических основ обеспечения гуманитарной составляющей ИБ	– Массовое развитие открытых образовательных программ в области ИБ; — в 2000 г. впервые выделяется отдельный блок в Перечне направлений подготовки и специальностей ВПО 075000 «Специальности в области ИБ», куда были включены и общедоступные и «закрытые» специальности

Окончание таблицы 1

Этапы развития системы подготовки специалистов по ИБ	Период	Характеристика этапа в контексте событий в мире	Методы защиты информации	Характеристика системы образования в России
Переход на двухуровневую систему образования; этап подготовки по отраслям	С 2010 г. по настоящее время	– Активизация информационного противоборства на международном уровне; — обогащение методов информационного противоборства как следствие изменения средств интерактивного воздействия	– Активное развитие научно-технических методов защиты информации; — формирование методологических основ обеспечения гуманитарной составляющей ИБ	– 2010–2011 гг.— переход на двухуровневую систему подготовки; — появление новых специальностей в области ИБ по отраслям деятельности

Анализ работ отечественных ученых, ретроспективный анализ государственных образовательных стандартов и перечней направлений и специальностей высшего профессионального образования (позже — высшего образования) в области подготовки специалистов по ИБ позволили нам выделить пять этапов образования по защите информации в России. Следует отметить, что содержательно первые два этапа совпадают с зарубежным развитием систем обучения специалистов в виду равномерности развития общества в информационной сфере. Дальнейшее развитие систем подготовки зарубежных специалистов по защите информации (особенно в США и Великобритании) вырвалось вперед, как результат высокой интенсивности информатизации общества, инновационного развития, создания собственного программного и аппаратного обеспечения и, как следствие, завоевания лидерских позиций в мире в сфере информационных технологий.

Первым этапом подготовки специалистов по защите информации целесообразно, по нашему мнению, выделить ***этап подготовки специалистов по ИБ в закрытых ведомственных учреждениях*** (до 1940-х гг. XX в.). Определение нижней временной границы данного этапа представляет некоторую сложность, так как элементы этой системы зарождались достаточно давно (например, в рамках передачи специализированных знаний по секретным шифрам одного служащего к другому). Позже, с формированием государственной системы обеспечения национальной безопасности, в том числе в информационной сфере, обучение специалистов в области защиты информации проводилось в рамках подготовки агентов в закрытых ведомственных государственных учреждениях.

Второй этап (1940-е — 1985 гг. XX в.), как мы полагаем,— ***этап подготовки специалистов по ИБ в вузах по закрытым программам.*** Следует отметить, что этот период характеризуется важными мировыми событиями в информационном пространстве: с одной стороны, это глобальное информационное противоборство («холодная война») двух стран-лидеров — СССР и США — и их союзников; с другой — появление и развитие компьютеров и компьютерных сетей. Так, в 40-е гг. американский ученый Дж. фон Нейман и другие [2] впервые определили основные принципы создания универсальной электронно-вычислительной машины (ЭВМ), и, как следствие, к концу 1940-х гг. стали появляться ЭВМ первого поколения.

Появление первых компьютерных сетей ученые связывают с событиями 1969 г., когда Министерство обороны США реализовало проект объединения оборонных и университетских основных компьютерных узлов в общую сеть ARPANET. При этом, как отмечает Ю. А. Савостицкий, «отечественные сети оборонного назначения создавались, видимо, одновременно с американскими... Но наши сети общественного пользования появились с почти десятилетним отставанием от Запада и базировались не на отечественных оборонных технологиях, а создавались совершенно независимо. Это десятилетнее отставание сохранялось до конца 1980-х — начала 1990-х гг.: ведь зарубежная сетевая технология не стояла на месте, а передача ее в нашу страну (особенно программного обеспечения) была жестко ограничена КОКОМом»[1] [13, с. 61]. С начала 1990-х гг. такое

[1] КОКОМ – международный Координационный комитет по экспортному контролю.

«отставание» сократилось не за счет собственных разработок в области компьютерных систем и сетей, а за счет возможности использования западных технологий: «...в самом начале 90-х гг. в нашей стране обозначился взрывообразный рост количества сетей общего пользования, создававшихся в основном как частные сети совместных предприятий с участием крупных иностранных телекоммуникационных операторов. Одновременно расширялся обмен информацией с зарубежными странами» [13, с. 61].

Все эти события не могли не повлиять на становление системы подготовки специалистов в области ИБ. В СССР с 1949 г. технический факультет Высшей школы КГБ СССР совместно с закрытым отделением механико-математического факультета МГУ начинает подготовку специалистов-криптографов. При этом «подготовка и переподготовка осуществлялись по ведомственным учебным планам и программам, утверждаемым Госкомвузом и КГБ СССР» [12, с. 17]. Несколько позже, в 1970-е гг., в учебные планы были введены дисциплины, касающиеся программно-аппаратных методов обеспечения безопасности информации.

Третий этап (1985 — конец 1990-х гг.) — ***этап единичных открытых программ по ИБ в отдельных вузах.*** Этап характеризуется, с одной стороны, «потеплением» отношений в биполярном мире, началом открытого диалога, который оказал существенное влияние на общую обстановку в мире, а также положил начало сотрудничеству, в том числе в информационной сфере, между СССР и США. С другой стороны — массовой информатизацией всех сфер деятельности, в первую очередь — в военной и образовательной отраслях. Б. А. Погорелов, И. В. Мацкевич отмечают, что в конце 1980-х — начале 1990-х гг. подготовку специалистов в области ИБ стали осуществлять и гражданские вузы. Так, в 1980-х гг. в РГГУ стали готовить специалистов по организации комплексной защиты информации, с 1991 г. в МИФИ ввели отдельные темы в области ИБ в рамках специальности «прикладная математика».

Анализ нормативно-правовой документации позволил заключить, что первые три специальности по ИБ были включены в Классификатор направлений и специальностей высшего профессионального образования в 1994 г.[2] Весной 1995 г. было предложено дополнить классификатор новой специальностью — 013200 «Криптография»[3] [12, с. 17].

В течение 1995–1997 гг. были приняты государственные образовательные стандарты высшего профессионального образования (ГОС ВПО), государственные требования к минимуму содержания и уровню подготовки специалистов, прошедших подготовку по образовательным программам в области ИБ.

В 1996 г. приказом Государственного комитета Российской Федерации по высшему образованию № 613 «Об учебно-методическом объединении (УМО) по образованию в области ИБ» основано Учебно-методическое объединение вузов по образованию в данной сфере, его основной целью стала координация работы вузов по подготовке кадров в области ИБ.

Таким образом, все это демонстрирует повышенный интерес к данному направлению подготовки в этот период, что взаимосвязано с началом становления научно-методологического базиса ИБ и способствовало дальнейшему активному развитию отечественной системы подготовки специалистов в области ИБ.

В то же время, как полагают эксперты [10, с. 190], развитие компьютерных технологий и информатизация общества в 1990-х гг. проходили наиболее интенсивно, нежели индустрия средств защиты информации, а также «в 90-х гг. еще не существовало такой угрозы, как международный высокотехнологичный терроризм, поэтому создаваемые системы и не рассчитывались на функционирование в условиях воздействия поражающих факторов хакеров-террористов», что, как мы полагаем, послужило качественному изменению системы подготовки специалистов по ИБ.

Четвертый этап (2000–2010 гг.) — ***этап массового внедрения образовательных программ в вузах.*** На этот период приходится прорыв во внимании к решению проблем ИБ бизнеса и государства как ответ на международный терроризм. Террористические акты в США 11 сентября 2001 г. стали «точкой отсчета не только для целого ряда специальных служб и правоохранитель-

[2] Приказ от 5.03.1994 № 180 «Об утверждении государственного образовательного стандарта в части Классификатора направлений и специальностей высшего профессионального образования».

[3] Приказ от 15.06.1995 № 911 «О дополнении Классификатора направлений и специальностей высшего профессионального образования». http://docs.cntd.ru/document/456058142.

ных органов, но и для разработчиков информационных систем и производителей средств защиты информации» [10, с. 190].

Также этому периоду характерно активное расширение границ понимания ИБ и потребителей средств защиты информации в мировом пространстве. Если раньше ИБ отожествлялась с государственной безопасностью в информационной сфере, то теперь проблемы кибербезопасности и угрозы конфиденциальности, целостности и доступности стали насущными и для бизнес-структур. Если до этого времени вузы и ведомственные образовательные учреждения готовили специалистов для различных спецслужб, то с начала XXI в. потребность в специалистах по защите информации стала ощутима и в организациях различных форм собственности. Так, в Перечне направлений и специальностей высшего профессионального образования 2000 г.[4] уже был выделен отдельный блок 070000 (075000) «Специальности в области ИБ», в него входили 6 специальностей, по которым в течение 2000 г. были также приняты образовательные стандарты.

Несколько позже, в 2002 г., была создана новая специальность «противодействие техническим разведкам». Следует отметить, что специальности 075100 «Криптография» и 075700 «Противодействие техническим разведкам» в виду своей специфичности до настоящего времени носят закрытый характер.

С 2002–2003 гг. в отечественных вузах по всей стране начали готовить специалистов по образовательным программам в области ИБ. На 2004 г. уже более 100 вузов России ввели в перечень своих образовательных программ программы в сфере ИБ [11, с. 125].

В 2005 г. был принят новый перечень направлений подготовки (специальностей) ВПО — Общероссийский классификатор специальностей по образованию (ОКСО)[5]. В соответствии с ОКСО специальности по защите информации выделялись в блок 090000 «Информационная безопасность». При этом сам перечень образовательных программ и утвержденные ГОС ВПО не менялись.

Помимо разработки учебно-методологического базиса образования в сфере ИБ, через несколько лет после начала массового внедрения открытых образовательных программ в вузах к преподавательской деятельности стали привлекаться специалисты с системным представлением предметной области. С момента открытия специальностей по защите информации (ориентировочно 2002–2005 гг.) в гражданских вузах России к преподаванию специализированных дисциплин привлекались специалисты смежных областей, прежде всего физики, информатики, инженеры.

Конец четвертого периода характеризуется началом оснащения гражданских университетов материально-технической базой, в том числе открываются лаборатории и специализированные центры технической и программно-аппаратной защиты информации, необходимые для формирования учебно-образовательной базы с целью организации обучения студентов практическим навыкам работы в сфере обеспечения ИБ.

Пятый этап (с 2010 г. и по настоящее время) характеризуется ***переходом на двухуровневую систему образования, а также началом подготовки специалистов в области информационной безопасности по отраслям.*** Для современного периода характерно активное развитие научно-технических методов защиты информации, а также формирование методологических основ обеспечения гуманитарной составляющей ИБ.

Для обеспечения перехода на двухуровневую систему образования в 2009 г. были приняты федеральные государственные образовательные стандарты высшего профессионального образования (ФГОС ВПО) с кодом 090900 «Информационная безопасность» и присвоением квалификации (степени) бакалавра и магистра[6]. Новые стандарты предусматривали компетентностный подход к квалификации будущих специалистов по защите информации.

---

[4] Приказ Минобразования РФ от 02.03.2000 № 686 «Об утверждении государственных образовательных стандартов высшего профессионального образования».

[5] Приказ Минобрнауки России от 12.01.2005 № 4 «Об утверждении перечня направлений подготовки (специальностей) высшего профессионального образования».

[6] Приказ от 28.10.2009 № 496 «Об утверждении и введении в действие Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 «Информационная безопасность (квалификация (степень) «бакалавр»)»; Приказ от 28.10.2009 № 497 «Об утверждении и введении в действие Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 «Информационная безопасность (квалификация (степень) «магистр»)».

В 2011 г. аналогичные ФГОС ВПО (третьего поколения) приняты для ряда специальностей группы 090000, причем перечень открытых программ изменился. Ранее популярные специальности «организация и технология защиты информации» и «комплексная защита объектов информации» не сохранились как отдельные направления подготовки, но могли реализовываться в образовательной организации, например как профиль подготовки бакалавров. Появилось два новых направления подготовки специалистов «Информационно-аналитические системы безопасности» и «Безопасность информационных технологий в правоохранительной сфере», ориентированных на конкретные отрасли обеспечения ИБ. Первая специальность направлена на защиту информации различных информационно-аналитических систем, на безопасность финансовых и экономических структур (систем электронного документооборота, современных платежных систем и т.п.). Вторая — обеспечивала безопасность информационных технологий в правоохранительных органах, в том числе технологии защиты информации в данной сфере, информационное обеспечение правоохранительной деятельности и проведение компьютерной экспертизы при расследовании преступлений.

Помимо историко-логического анализа подготовки специалистов по защите информации в России, необходимо рассмотреть отдельные аспекты исторического развития зарубежных систем ИБ и их влияние на становление современной системы подготовки специалистов. За основу государственной политики в ответ на информационную войну возьмем труды доктора технических наук, ведущего эксперта в области ИБ С.Н. Гриняева [9–10], который проанализировал развитие теории, средств и методов информационной войны в ряде стран.

Подходя к вопросу истории развития деятельности в условиях информационного противоборства, С.Н. Гриняев отмечает, что «деятельность американской администрации в области защиты критической инфраструктуры берет свое начало с формирования Президентской комиссии по защите критической инфраструктуры (President's Commission for Critical Infrastructure Protection) в 1996 г. » [9].

Одной из наиболее важных выполненных Министерством обороны США работ по защите информации в критической инфраструктуре выделено «существенное продвижение по пути совершенствования приемов и методов работы с доказательствами компьютерных преступлений, что имеет большое значение при проведении расследований любых инцидентов, связанных с применением вычислительной техники». Вследствие чего 24 сентября 1999 г. была открыта Компьютерная судебная лаборатория Министерства обороны США (Defense Computer Forensics Laboratory, DCFL). Сегодня в США существует не только государственная, но и множество подобных других лабораторий, чаще это частные центры или центры при частных вузах страны, осуществляющие независимую деятельность. Подобные центры и лаборатории предназначены для обработки компьютерных доказательств преступлений и мошенничеств с последующим предоставлением этих доказательств в суде.

Востребованность специалистов по расследованию компьютерных преступлений повлияла на социальный заказ для вузов США. Данный факт нашел свое отражение в современной системе подготовки специалистов в области ИБ. Направления подготовки бакалавров в области расследования компьютерных инцидентов в США — самые популярные среди образовательных программ в области ИБ и составляют значительный процент от общего числа таких программ (17 %) [15, с. 128]. Это говорит о том, что общество заинтересовано в привлечении таких специалистов не только в государственный, но и частный сектор, в том числе в сфере электронной коммерции.

В то же время в России расследованием компьютерных преступлений занимаются подразделения ФСБ и МВД, и практически нет, в отличие от зарубежных стран, частных практикующих лабораторий по компьютерной экспертизе, результаты которых могли бы использоваться в качестве доказательств в суде. Исключение составляет компания Group-IB, основанная студентами кафедры ИБ МГТУ имени Н.Э. Баумана в 2003 г. Генеральный директор Group-IB И.К. Сачков отмечает, что изучение и сравнение зарубежного и отечественного рынков компьютерной экспертизы позволили сделать вывод о том, «что в России этим никто не занимается, несмотря на то, что в США и Европе это развитая отрасль ИБ» [14].

Аналогичная ситуация возникает и при подготовке специалистов в области ИБ. В перечне направлений подготовки и специальностей в данной сфере по ФГОС ВО существует специальность 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» со спе-

циализацией «компьютерная экспертиза». Однако подготовкой по такому направлению занимается минимальное количество вузов. Автор уже указывала [7, с. 14], что всего 5 % от общего числа образовательных программ по ИБ — это программы по направлению подготовки 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», при этом специализация «компьютерная экспертиза» среди них практически не встречается.

Следующей важнейшей отраслью обеспечения государственной системы защиты информации в США С. Н. Гриняев [9] выделяет защиту компьютерных сетей: «С целью улучшения способности активно защищать информационные системы и компьютеры была создана Объединенная оперативная группа по защите компьютерной сети Министерства обороны». Важность защиты компьютерных сетей на государственном уровне также отражена в системе подготовки специалистов: образовательные программы в области защиты компьютерных сетей составляют более 10 % от общего числа программ, что сопоставимо с количеством образовательных программ по защите телекоммуникационных систем и сетей в России. Также следует отметить, что отдельные темы по расследованию компьютерных преступлений и защите компьютерных сетей входят во все направления подготовки по защите информации [15].

С. Н. Гриняев также отмечает, что «представление британских аналитиков об ИБ и информационной войне аналогично тому, что характерно для американских: информационная война определяется как воздействие на информационные системы противника при одновременной защите собственных. Вместе с тем британские специалисты активно используют юридический нормативный акт (Regulation of Investigatory Powers Act, принят в 2000 г.), который в значительной степени может быть применим к действиям в киберпространстве». Также схожи укрупненные блоки направлений подготовки специалистов в области информационной безопасности Великобритании и США: «Информационная безопасность», «Компьютерная безопасность», «Расследование компьютерных инцидентов», «Безопасность компьютерных сетей», «Менеджмент ИБ» [8, с. 67–68; 16, с. 127].

Наиболее активное использование юридической составляющей в области обеспечения информационной безопасности в Великобритании создает одну из самых жестких из существующих национальных систем защиты информации. Серьезный упор со стороны Великобритании на юридические аспекты ИБ и защиту информации также наблюдается в системе подготовки специалистов по защите информации. Так, Великобритания — единственная из рассматриваемых стран, где студенты после успешного окончания обучения имеют возможность получить академическую степень магистра права в области ИБ. Также вузы Великобритании имеют самое большое количество различных образовательных программ по законодательству в области ИБ [8, с. 68–69].

Относительно мнения французских и немецких экспертов в области информационной безопасности С. Н. Гриняев отмечает, что они в целом совпадают с принятым в США и Великобритании, однако отдельно выделяют экономические (гражданские) аспекты информационной войны. Так, французская система подготовки специалистов по защите информации в изобилии включает в себя образовательные программы, связанные с управлением безопасности, информационным менеджментом, корпоративной информационной безопасностью. «В то же время во Франции активно формируются структуры по контролю граждан в киберпространстве с тенденцией на перехват сообщений во французских (и не только) линиях электронных коммуникаций. Перехват информации в телекоммуникационных линиях способствует развитию криптографических методов ИБ» [9]. Эта тенденция видна в системе подготовки специалистов в области ИБ: внедряется большое количество образовательных программ, связанных с математическими методами защиты информации, а также дисциплин по криптографии в другие непрофильные направления подготовки специалистов по защите информации [16, с. 160–162].

Заключение

Таким образом, историко-логический анализ становления системы подготовки специалистов по защите информации позволил выявить этапы ее развития в России, которые рассматривались в контексте совершенствования мирового сообщества в информационной сфере и развития методов защиты информации за рубежом.

Анализ научных источников и интернет-пространства позволил прийти к выводу о том, что сегодня отечественная ИТ-отрасль существенно отстает от западной ИТ-индустрии. Пока еще Россия находится в «цифровой зависимости» от западных разработок. Так, повсеместно исполь-

зуются зарубежные аппаратные платформы (сетевые, мобильные, персональные компьютеры) и программные средства (операционные системы, офисные технологии, поисковые механизмы и др.).

На современном этапе международных отношений крайне важно укреплять собственный цифровой суверенитет. В последнее время активизировались процессы по созданию отечественных ИТ-разработок, аппаратных и программных платформ, осуществляется политика по их внедрению. Мы полагаем, что обобщение ситуации в зарубежных системах подготовки (прежде всего в странах-лидерах по подготовке ИТ-специалистов) становится почвой для дальнейших исследований, в том числе для выявлений направлений развития и разработок прорывных технологий в России. Развернуты процессы по генерированию проектов в рамках развития Национальной технологической инициативы (НТИ). Среди приоритетных направлений НТИ выделяют рынок SafeNet (новых персональных систем безопасности), развиваются идеи и механизмы квантовой криптографии, появляются первые протоколы стриминга биоданных и идеи первых стандартов передачи и обработки биоданных и связанных с ними систем безопасности.

Анализ содержательных компонентов показал, что независимо от ментальности и традиций формирования содержания образовательных программ в разных странах им присуще общее: во-первых, ориентация на динамичные изменения профессиональной среды; во-вторых, на образовательную среду накладываются новые задачи, порожденные динамикой развития информационного общества. Вместе с тем на современном этапе университет становится не столько местом передачи знаний, сколько местом, где происходит генерация инновационных идей.

Литература

1. A history of Internet security [Electronic resource]. URL: https://www.washingtonpost.com/graphics/national/security-of-the-internet/history/ (дата обращения: 29.03.2017)
2. John von Neumann. First Draft of a Report on the EDVAC / University of Pennsylvania // Contract № W-670-ORD-4926. Between the United States Army Ordnance Department and the University of Pennsylvania. Moore School of Electrical Engineering, University of Pennsylvania, June 30, 1945.
3. Julian Ted. Defining Moments in the History of Cyber-Security and the Rise of Incident Response [Electronic resource].URL: https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/ (дата обращения: 29.03.2017).
4. Lynett Mike. A History of Information Security From Past to Present [Electronic resource]. URL: http://blog.mesltd.ca/a-history-of-information-security-from-past-to-present (дата обращения: 29.03.2017).
5. Timberg Craig. A history of Internet security [Electronic resource].URL: https://www.washingtonpost.com/graphics/national/security-of-the-internet/history/ (дата обращения: 29.03.2017)
6. Системы защиты информации в ведущих зарубежных странах / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. Брянск : БГТУ, 2007. С. 225.
7. Анурьева М. С. Современная система образования в области информационной безопасности в РФ // Информационные технологии в образовании и социальной сфере. Тамбов, 2017. С. 13–20.
8. Анурьева М. С., Чванова М. С. Система образования в области информационной безопасности в Великобритании // Преподавание информационных технологий в Российской Федерации : материалы IX Всерос. конф. Саратов : Наука, 2011. С. 67–70.
9. Гриняев С. Н. Информационная война: история, день сегодняшний и перспектива [Электронный ресурс]. URL: http://www.agentura.ru/equipment/psih/info/war/ (дата обращения: 29.03.2017)
10. Гриняев С. Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. Минск : Харвест, 2004. 448 с.
11. Коваленко А. П., Белов Е. Б. Концепция подготовки кадров в области обеспечения информационной безопасности (проблемы, анализ, подходы) // Научные и методологические проблемы информационной безопасности : сб. ст. М. : МЦНМО, 2004. С. 117–133.
12. Погорелов Б. А., Мацкевич И. В. О подготовке кадров в области информационной безопасности // Информационное общество. 1997. Вып. 1. С. 17–22.
13. Савостицкий Ю. А. История развития глобальных компьютерных сетей // Информационное общество. 2000. Вып. 4. С. 59–65.
14. Царев Е. О. Расследование инцидентов информационной безопасности [Электронный ресурс]. URL: https://www.tsarev.biz/news/rassledovanie-incidentov-informacionnoj-bezopasnosti/.
15. Чванова М. С., Анурьева М. С. Подготовка специалистов в области информационной безопасности в США // Вестник Тамбовского университета. Сер. Гуманитарные науки. 2012. Вып. 8 (112). С. 126–133.
16. Чванова М. С., Анурьева М. С. Подготовка специалистов в области информационной безопасности во Франции // Вестник Тамбовского университета. Сер. Гуманитарные науки. 2012. Вып. 7 (111). С. 159–165.

References

1. A history of Internet security. Available at: https://www.washingtonpost.com/graphics/national/security-of-the-internet/history/ (accessed 29.03.2017).
2. John von Neumann. First Draft of a Report on the EDVAC. University of Pennsylvania. *Contract No. W-670-ORD-4926. Between the United States Army Ordnance Department and the University of Pennsylvania. Moore School of Electrical Engineering, University of Pennsylvania, June 30, 1945*

3. Julian Ted. Defining Moments in the History of Cyber-Security and the Rise of Incident Response. Available at: https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/ (accessed 29.03.2017).
4. Lynett Mike. A History of information security from past to present. Available at: http://blog.mesltd.ca/a-history-of-information-security-from-past-to-present (accessed 29.03.2017).
5. Timberg Craig. A history of Internet security. Available at: https://www.washingtonpost.com/graphics/national/security-of-the-internet/history/ (accessed 29.03.2017).
6. Averchenkov V. I., Rytov M. Yu., Kondrashin G. V., Rudanovsky M. V. Sistemy zashchity informacii v vedushchih zarubezhnyh stranah [Information security systems in leading foreign countries]. Bryansk, BSTU, 2007, 225 p. (In Russian).
7. Anurieva M. S. Sovremennaya sistema obrazovaniya v oblasti informacionnoj bezopasnosti v RF [The modern system of education in the field of information security in the Russian Federation]. *Information technologies in education and social sphere.* Tambov, 2017, pp. 13–20. (In Russian).
8. Anurieva M. S., Chvanova M. S. Sistema obrazovaniya v oblasti informacionnoj bezopasnosti v Velikobritanii [The information security education system in the UK]. *Teaching of information technologies in the Russian Federation. Proceedings of the IX All-Russian Conference.* Saratov, Science, 2011, pp. 67–70. (In Russian).
9. Grinjaev S. N. Informacionnaya vojna: istoriya, den' segodnyashnij i perspektiva [Information war: history, today's day and perspective]. Available at: http://www.agentura.ru/equipment/psih/info/war/ (accessed 29.03.2017). (In Russian).
10. Grinjaev S. N. Pole bitvy – kiberprostranstvo: Teoriya, priemy, sredstva, metody i sistemy vedeniya informacionnoj vojny [The battlefield – cyberspace: Theory, methods, means, methods and systems of information warfare]. Minsk, Harvest, 2004, 448 p. (In Russian).
11. Kovalenko A. P., Belov E. B. Koncepciya podgotovki kadrov v oblasti obespecheniya informacionnoj bezopasnosti (problemy, analiz, podhody) [The concept of training personnel in the field of information security (problems, analysis, approaches)]. *Scientific and methodological problems of information security. Collection of articles.* Moscow, MCNMO, 2004, pp. 117–133. (In Russian).
12. Pogorelov B. A., Mackevich I. V. O podgotovke kadrov v oblasti informacionnoj bezopasnosti [On the training of personnel in the field of information security]. *Information society,* 1997, iss. 1, pp. 17–22. (In Russian).
13. Savostickij Ju. A. Istoriya razvitiya global'nyh komp'yuternyh setej [History of the development of global computer networks]. *Information society,* 2000, iss. 4, pp. 59–65. (In Russian).
14. Carev E. O. Rassledovanie incidentov informacionnoj bezopasnosti [Investigation of incidents of information security]. Available at: https://www.tsarev.biz/news/rassledovanie-incidentov-informacionnoj-bezopasnosti/ (accessed 29.03.2017). (In Russian).
15. Chvanova M. S., Anur'eva M. S. Podgotovka specialistov v oblasti informacionnoj bezopasnosti v SShA [Training of specialists in the field of information security in the USA]. *Tambov University Review. Series Humanities,* 2012, iss. 8 (112), pp. 126–133. (In Russian).
16. Chvanova M. S., Anur'eva M. S. Podgotovka specialistov v oblasti informacionnoj bezopasnosti vo Francii [Training of specialists in information security in France]. *Tambov University Review. Series Humanities,* 2012, iss. 7 (111). pp. 159–165. (In Russian).

УДК/UDC 37.013.83:101

И. А. Грешилова

I. Greshilova

АНДРАГОГИЧЕСКИЕ ПРИНЦИПЫ НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ: ФИЛОСОФСКО-АНТРОПОЛОГИЧЕСКИЙ АСПЕКТ

ANDRAGOGICAL PRINCIPLES OF CONTINUING EDUCATION: PHILOSOPHICAL-ANTROPOLOGICAL ASPECT

Введение. В статье представлено исследование проблемы непрерывного образования как социальной системы, характеризующейся наличием таких инвариантных качеств, как динамичность и вариативность, приобретающих особую значимость в современных социально-экономических условиях. В настоящее время роль андрагогических принципов непрерывного образования возрастает, что обусловлено инновационными тенденциями, связанными с необходимостью подготовки человека к быстро меняющимся условиям жизни.

Методология. В центре внимания исследования — проблема непрерывного образования как проблема личностного роста, напрямую связанная с путями и средствами получения образования, их практической направленности. В статье рассматривается ценностно-смысловое содержание непрерывного образования в контексте запуска механизмов процесса самоактуализации.

Результаты исследования представлены анализом андрагогических принципов, выступающих в органической взаимосвязи и дополняющих друг друга, образующих целостную совокуп-