Об актуальных проблемах образования в области информационной безопасности

И.И. Лившиц (НИУ ИТМО (Университет ИТМО)

«Как вы все это можете объяснить?
Недомыслием.
Как? Повторите!
Пожалуйста, недомыслием.»
(«Укрощение огня»)

В настоящее время во многих вузах нашей страны проводится подготовка по специальностям 10.03.01 «Информационная безопасность» (программа бакалавриата) и 10.04.01 «Информационная безопасность» (программа магистратуры). Безусловно, подготовка по данным специальностям крайне важна для всех отраслей экономики (даже без учета современных «прорывных» технологий IoT, блок-чейн, Web 4.0 и пр.) в первую очередь – для обеспечения стабильности государства и сохранения национального суверенитета [1, 2].
При всех положительных моментах существующих программ подготовки по указанным специальностям существуют проблемы, проявляющиеся в процессе преподавания ряда дисциплин в течение длительного периода. Отмечено, что эти проблемы могут привести к рискам при выпуске готовых специалистов, незнакомых с существующими международными стандартами в области безопасности ИТ и, как следствие, не способных обеспечить требуемый уровень безопасности. В наихудшем сценарии этот риск может быть реализован на государственном уровне и привести к критическим проблемам при обеспечении национальной безопасности.

Ключевые слова: бакалавриат, магистратура, информационная безопасность, обучение, проблемы, направление подготовки, международные стандарты, соответствие.

Часть 1. Актуальные стандарты

В настоящее время в РФ разработаны и применяются Федеральные государственные образовательные стандарты высшего образования (ФГОС ВО) по направлениям подготовки 10.04.01 Информационная безопасность (программа магистратуры) и 10.03.01 Информационная безопасность (программа бакалавриата) (www.fgosvo.ru). В дальнейшем будем рассуждать только о программе подготовки магистров 10.04.01. Отметим, что в Программе в Разделе 4 «Характеристика профессиональной деятельности выпускников, освоивших программу магистратуры» в п. 4.4 указана, в частности, готовность решения следующих профессиональных задач (выборочно):

- системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем;
- обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;
- аудит информационной безопасности информационных систем и объектов информатизации;
- организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами ФСБ России и ФСТЭК России.

В полном перечне профессиональных задач (п. 4.4 Программы), очевидно, не упомянуты риски (они вообще, к сожалению, не упомянуты в этом разделе, встречаются только один раз в разделе 5 «Требования к результатам освоения программы магистратуры» в п. 5.4 при описании компетенции ПК-1). И это обстоятельство дает основание для формирования первого риска — невозможности обеспечения информационной безопасности (ИБ) только исключительно на основании нормативно-методических документов (НМД) Федеральной службы безопасности (ФСБ России) и Федеральной службы технического и экспертного контроля (ФСТЭК России). Эта проблема имеет на данный момент исключительную актуальность по причине того, что, во-первых, противоборствующая сторона не всегда учитывает при организации атак требования упомянутых выше национальных регуляторов, а во-вторых, все национальные стандарты в системе ГОСТ Р ИСО (ИСО/МЭК) не успевают обновляться синхронно с международными. Например, по сайту ФАТРиМ (https://www.gost.ru/portal/gost/home/standarts/cataloginter) наблюдаем, что основной межгосударственный стандарт ГОСТ Р ИСО/МЭК серии 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» утвержден еще в 2006 г. Актуальной версией международного стандарта этой серии является ISO/IEC 27001:2013 с дополнением Corr 2:2015, опубликованным в декабре 2015 г. (https://www.iso.org/standard/69378.html).

Похожая ситуация наблюдается и в области стандартов для систем управления промышленной автоматизации, в частности, для семейства стандартов ISA/IEC 62443 Industrial communication networks. Network and system security. В этом семействе к настоящему времени выпущено 12 стандартов и еще 9 готовятся к изданию или находятся на рассмотрении (https://webstore.iec.ch/). В частности, стандарт IEC/TS 62443-1-1:2009 «Industrial communication networks. Network and system security. Part 1–1. Terminology, concepts and models» выпущен еще в 2009 г., но принят в качестве ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищен-

ность (кибербезопасность) сети и системы» только в 2014 г. К сожалению, и требования к промышленным сетям также никак не упомянуты в Программе (http://fgosvo.ru/news/8/2127), как будто все современные проблемы обеспечения безопасности в области промышленной автоматики уже успешно решены и не представляют никакого научного интереса.

Более серьезное отставание демонстрируют ведомственные (отраслевые) системы стандартизации, где запаздывание идет уже на два и более поколения (например, стандарт СТО Газпром 4.2-3-003-2009 СОИБ «Анализ и оценка рисков» содержит ссылку на отмененный британский стандарт BS серии 7799) [3]. На многих научных и научно-практических конференциях давно обсуждается вопрос о необходимости поддержки нескольких раздельных ведомственных стандартов по конкретной тематике, в частности, в области ИТ и ИБ. Даже на уровне собственных центров (например, Газпром ВНИИГАЗ) идет обсуждение длительного и серьезного запаздывания в области стандартизации, что подтверждается, кстати, и публикациями в ведомственных журналах (например, статья «Актуализация стандартов ПАО «Газпром» на системы менеджмента качества СТО Газпром серии 9000») [4]. Также отметим, что принятие нового СТО в области системы менеджмента качества (СМК) выполнено только в августе 2018 г, в конце 3-х летнего переходного периода СМК (считая с даты утверждения ISO 9001 версии 2015 г.), с принятием приказа ПАО Газпром № 508 от 20.08.2018 новых СТО Газпром 9000-2018 и СТО Газпром 9001-2018.

Соответственно при наличии фундаментальных изменений в системе требований обеспечения ИБ на международном уровне в РФ более 13 лет на национальном уровне доступен только конкретный стандарт как перевод уже устаревшего международного. Эти изменения никак не отражены в Программе, и преподавателям нужно самостоятельно разрабатывать комплекс компенсирующих мер: искать обновления, закупать актуальные стандарты (часто выложенные в сети Internet версии неполные), выполнять перевод (часто выложенные в сети Internet переводы некорректны), обновлять учебные материалы и состав практических занятий.

Часть 2. Роль независимой оценки (аудита)

Следующей актуальной проблемой по степени значимости является понимание роли аудита ИБ. Однако и в этом важном аспекте нет оснований для оптимизма, — все современные «целевые» стандарты по аудиту ИБ (в частности, ГОСТ Р ИСО/МЭК серии 27006 и 27007) в РФ также не соответствуют по актуальности международным ISO/IEC, и даже «общие» стандарты для выполнения аудитов (в частности, ГОСТ Р ИСО 19011-2012 «Руководящие указания по аудиту систем менеджмента» и ГОСТ Р ИСО/МЭК 17021-2012 «Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента», отражают уже прошедший этап. Подобная практика может привести к риску невозможности получения студентами в рамках обучения по Программе актуальных знаний, соответствующих текущему уровню требований к обеспечению и/или аудиту ИБ на тех предприятиях, куда они могут трудоустроиться после окончания вуза. В тоже время крайне немногие преподаватели хотят и делают дополнительные усилия для своевременной компенсации подобных рисков — готовят новые учебные материалы, получают новые стандарты и авторизованные переводы.

В одном из вузов Санкт-Петербурга каждый год перед стартом обучения по дисциплине «Нормативно-методическое обеспечение ИБ» проводится несколько добровольных публичных исследований, цель которых — оценить степень информированности студентов, закончивших бакалавриат. За прошедшие 3 года только один раз на потоке отозвались несколько студентов, знавших хотя бы один (!) актуальный международный стандарт и/или их национальный аналог в системе сертификации ГОСТ Р ИСО (ИСО/МЭК) по ИБ. Заметим, что эти знающие студенты уже работали в компании, выполняющей, в том числе работы по сертификации информационных систем по требованиям «Общих критериев». Следующий опрос касался знаний хотя бы одного стандарта по аудиту ИБ. Здесь также только один студент (прошедший ранее обучение в одном из известных университетов Казахстана) смог назвать один из стандартов. Вызывает удивление и такой факт — практика аудита известна несколько столетий, и к настоящему моменту опубликованы десятки «целевых» стандартов самых разных организаций — National Institute of Standards and Technology (NIST, https://www.nist.gov), профессиональных сообществ Critical Infrastructure Protection (CIP, https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx), в том числе и в области аудита ИТ и/или ИБ — Control Objectives for Information and Related Technologies (Cobit5, https://www.isaca.org/cobit/pages/default.aspx). В этой ситуации тотальное незнание методов аудита, особенно методов формальной оценки соответствия, хорошо и давно известных, применимых и к объектам критичной информационной инфраструктуры (КИИ) на соответствие требованиям ФЗ «О безопасности критической информационной инфраструктуры РФ» от 26.07.2017 N 187-ФЗ, например, на базе IEC (ГОСТ Р МЭК) серии 61508 и/или IEC (ГОСТ Р МЭК) серии 61511, в известном техническом вузе вызывает значительную тревогу.

Кроме того, нужно отметить различия в преподавании предметов по Программе, в первую очередь, преподавателями старшего возраста. Известно, что до определенного времени вопросы безопасности и, в частности, вопросы ИБ, преподавались только в определенных вузах в системе ФСБ и Министерства обороны. Конечно, это прекрасная научная школа, в которой значительное время уделялось изучению фундаментальных дисциплин, но, к сожалению, в минимальном объеме рассматривались «внешние аспекты», в частности, оценка соответствия, аудит ИБ, обеспечение устойчивости и пр. Как следствие, в настоящее время во многих вузах по Программе нет таких «внешних аспектов», поскольку некому преподавать, и отсутствуют соответствующие формализованные требования в Программе. В результате выпускаются магистры, достаточно неплохо ориентирующиеся в национальной системе НМД ФСБ России и ФСТЭК России, но практически не знакомые

с современным уровнем развития науки в остальных 5/6 частях мира... И на это пустое «святое место» незамедлительно «слетаются» всевозможные консультанты, предлагающие, в лучшем случае, классические методики на базе тех же ISO (ISO/IEC), а в большинстве случаев — доморощенные «уникальные» разработки от известных консалтинговых компаний. В результате мы можем наблюдать частую ситуацию, как наши вчерашние выпускники возвращаются в родной ВУЗ и ловят преподавателей за руку: «Помнится, Вы что-то там говорили про ISO, GDPR[1] (General Data Protection Regulation, Общий регламент по защите данных, https://gdpr.eu/), Compliance (Соответствие требованиям)... у нас приезжают иностранные аудиторы и/или акционеры и/или партнеры... Как нам доказать соответствие? Как нам показать обработку рисков? Как нам подтвердить заданную степень устойчивости?», и таких вопросов не счесть...

Часть 3. Обеспечение национальной безопасности

Третьей актуальной проблемой является «перекос» в системе существующих национальных НМД, прежде всего, ФСТЭК России и ФСБ России, что особенно хорошо видно на примере студентов, приезжающих на Программу магистров из стран СНГ и иных государств. Для многих студентов (особенно из Казахстана и Азербайджана) характерно знание фундаментальных основ теории информации, криптографии и существующих международных стандартов. Более того, многие иностранные студенты после завершения бакалавриата в национальных университетах демонстрируют знание работ Боэма (по теории проектирования программного обеспечения), нобелевских лауреатов Пригожина и Стенгерс (по теории хаоса и энтропии), Месаровича, Мако и Такахара (по теории иерархических многоуровневых систем). Это прекрасный пример того, насколько важно изначально «закладывать» в молодых специалистов по выбранной специальности систему фундаментальных знаний и «на выходе» получать компетентных и образованных работников, способных действительно понимать сложности порученных им задач по обеспечению безопасности ценных для бизнеса активов.

Кратко рассматривая современные национальные НМД в России можно отметить существенное отставание не только в тактике обеспечения ИБ, но и в вопросах стратегического уровня, в частности, обеспечения вопросов национальной безопасности. В двух важнейших опубликованных документах: Стратегии национальной безопасности РФ (утверждена Указом Президента РФ В. В. Путиным 31.12.2015 г. N 683) и Доктрине информационной безопасности РФ (утверждена Указом Президента РФ В. В. Путиным 05.12.2016 г., № 646) подчеркивается важнейшая задача учета угроз безопасности информации в части нарушения устойчивости функционирования объектов КИИ, необходимость совершенствования системы мониторинга и прогнозирования чрезвычайных ситуаций и отражены все современные вызовы, в том числе появление новых рисков ИБ. На эту тему опубликованы десятки и сотни публикаций и экспертных суждений, но пока мы не видим значимых результативных усилий от представителей науки и промышленности ни в области «цифрового суверенитета», ни в области «импортозамещения», ни в области совершенствования высшего образования.

Под значимыми усилиями подразумеваются инициативы по созданию архитектуры вертикальной национальной системы безопасных ИТ, базирующихся полностью на доверенных компонентах по всему стеку ИТ [5]. Термин «вертикальная» применен здесь для отражения важной роли каждого из 7 уровней модели взаимодействия открытых систем ISO/OSI. Для создания такой архитектуры обязательно требуется создание собственной полностью независимой системы производства ИТ компонент в системе цифрового суверенитета РФ, что влечет также изменение подходов в области высшего профессионального образования в РФ. Статистика применения заимствованных операционных систем[2], систем управления базами данных, специального и прикладного ПО[3], телекоммуникационного оборудования[4] и даже элементной базы говорит о том, что доля национальной высокотехнологичной продукции редко превышает 5%. Всем памятна яркая ситуация 2014 г., когда VISA и MasterCard без предупреждения просто отключили шесть российских банков от своих сервисов. Этот инцидент был первым реальным примером эффективных действий противоборствующих сторон, находящихся на разных уровнях технологической зрелости и поставленных в неравные условия (очень похоже на противостояние вооруженных конкистадоров и дикарей, никогда не видевших кораблей...). Особо ценный урок был в том, что в системе Банка России существует собственная система НМД и именно в области ИБ: стандарт «Обеспечение информационной безопасности организаций банковской системы»[5] (СТО БР ИББС), которая оказалась неэффективной при первом же серьезном внешнем испытании. Отчасти этот пример характеризует степень восприятия специалистами и руководством Банка России «ландшафта угроз» и игнорирование известных фактов — тех самых рассмотренных выше «внешних аспектов», что, во-первых, вся техническая инфраструктура международного процессинга платежных карт находится вне их контроля, и во-вторых, «ландшафт угроз» не является чем-то однажды созданным и зафиксированным навечно в создании «эффективных менеджеров».

Другой пример — инцидент по отказу компании Splunk с 2019 г. работать на российском рынке[6]. Известно, что американский разработчик ПО для обработки и анализа машинно-генерируемых данных имеет хорошие позиции в области мониторинга инцидентов, в том числе ИБ и эти решения используются, в частности, в крупных компаниях: МегаФон, Росгосстрах, Mars[7].

[1] https://gdpr.eu/
[2] http://www.cnews.ru/news/top/2019-01-31_nazvany_prichiny_medlennogo_importozameshcheniya_po
[3] https://www.kommersant.ru/doc/3833580
[4] https://tass.ru/ekonomika/3609436
[5] https://www.cbr.ru/Content/Document/File/46921/st-10-14.pdf
[6] https://www.securitylab.ru/news/497998.php
[7] https://www.kommersant.ru/doc/3889546

В процессе проведения практических занятий по Программе со студентами по дисциплине «Риски информационной безопасности» были проведены следующие сопоставления: для реальных объектов (в которых работали студенты) нужно было оценить риски для классической «триады» ИБ: конфиденциальность, целостность и доступность. В качестве «базы» были предложены НМД ФСТЭК России (актуальные на тот момент Приказы № 17, № 21 и № 31), а в качестве «сравнения» была предложена пара стандартов ISO/IEC серии 27001 (содержащий перечень мер обеспечения ИБ) и серии 27005 (содержащий методику оценки рисков ИБ). Желающие могли выбрать указанные выше системы стандартов NIST, CIP или методику Cobit5. Каждая бригада за установленное время выбрала перечень объектов защиты (активов), определила уязвимости, угрозы и рассчитала численные значения рисков. Определялись критерии оценки рисков, меры защиты и остаточные риски. После этого все варианты защищались перед другими бригадами в рамках реализации «виртуального противоборства», при этом все участники практики заранее знали о выбранных объектах защиты и имели возможность подготовить любые свои вопросы.

По итогам этой практики было получено два значимых результата, впоследствии подтверждаемых ежегодно. Первый — на основании только национальных НМД невозможно оценить достоверно все риски современного объекта (что следует, во-первых, из отсутствия в НМД ФСТЭК России даже упоминания о рисках, кроме Приказа № 31 в части, касающейся АСУТП, и во-вторых, из фиксированного жесткого перечня угроз и применяемых мер защиты). Второй — значение априорных рисков (и как следствие — обязательные меры, например, аттестация, защита персональных данных, установка антивирусного ПО и пр.) в разы превышало значение апостериорных рисков, рассчитанных по статистике реализации известных инцидентов ИБ за определенный срок наблюдений. Заметим, что Приказ ФСТЭК № 31 в значительной степени противоречит стандартам семейства ISA/IEC серии 62443 и ISO/IEC серии 27001. В тоже время в действующих НМД ФСТЭК России и ФСБ России практически не отражены меры защиты нематериальных активов (о чем еще в 1997 г. было указано в первой версии стандарта ISO/IEC серии 13335-1, и заметим, что ГОСТ Р ИСО/МЭК 13335-1 версии 2006 г. до сих пор актуален в РФ). Среди нематериальных активов наиболее значимыми были определены лицензии на ПО, патенты и чувствительная информация (маркетинговые программы, чертежи, инновации и пр.), репутация (*image*), стоимость бренда (*goodwill*) и пр. Одна из команд провела дополнительные исследования и выявила, что ряд крупных компаний в России, тем не менее, выполняют оценку нематериальных активов (НМА), например, ПАО «Газпром-нефть» отражает НМА в своем балансе[8].

Известно, что в феврале 1882 г. Д. И. Менделеев продиктовал текст, посвященный его программе реформирования Академии наук[9]. Этот текст впервые опубликован с предисловием академика Б. М. Кедрова в журнале «Новый мир», № 12, 1966 г. Представляется целесообразным для целей данной публикации процитировать одну важную мысль: *«Очевидно, что критерием ... должны служить одни чисто научные заслуги, а так как наука, прежде всего, есть дело не кабинетное и частное, а общественное и публичное, то непременным условием ... должны служить труды публичные, то есть или публикованные, или публичному суду подлежащие, то есть доступные всеобщей оценке и могущие служить на пользу всем и каждому»*.

Заключение

В представленной публикации изложены некоторые актуальные проблемы образования в области информационной безопасности, определяемые автором на основании практики преподавания ряда дисциплин по специальности 10.04.01 «Информационная безопасность» (программа магистратуры). Отмечено, что наибольший риск для успешной подготовки магистров представляют упущения в процессе обучения на первой (базовой) ступени подготовки (бакалавриат) и непринятие во внимание необходимости разработки и применения компенсирующих мер в процессе обучения на второй ступени (магистратура). Высказаны обоснованные опасения, что без принятия неотложных мер, в частности, увеличения внимания к современным международным стандартам и ознакомления с лучшим мировым опытом создания защищенных ИТ, задача обеспечения национальной безопасности может и не иметь приемлемого по срокам и стоимости решения.

Список литературы

1. *Лившиц И.И., Неклюдов А.В.* Кибербезопасность - новое понятие или хорошо известное настоящее? // Автоматизация в промышленности. 2018. № 7. С. 32-35.
2. *Livshitz I.I., Neklyudov A.V., Lontsikh P.A.* Evaluation of IT security – genesis and its state-of-art//Journal of Physics: Conference Series, IET - 2018, Vol. 1015. pp. 042029.
3. *Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Kunakov E.P., Drolova E.Y.* Implementation and auditing of risk management for the oil and gas company//2017 International Conference, Quality Management, Transport and Information Security, Information Technologies; (IT&QM&IS), IET – 2017. pp. 539-543.
4. *Почечуев А.М. и др.* Актуализация стандартов ПАО «Газпром» на системы менеджмента качества СТО Газпром серии 9000 // Газовая промышленность. 2018. 4 (774). С. 142- 146.
5. *Лившиц И.И., Неклюдов А.В.* Обеспечение цифрового суверенитета России // Стандарты и качество. 2017. № 8. С. 58-61.

Лившиц Илья Иосифович *– канд. техн. наук, доцент факультета безопасности информационных технологий НИУ ИТМО (Университет ИТМО).*
Контактный телефон +7(921)9344846.
E-mail: livshitz.il@yandex.ru

[8] http://ir.gazprom-neft.com/fileadmin/user_upload/documents/ad-hoc_releases/new/new_04.03.16/qrep/1q2018/pril1.pdf
[9] http://www.ng.ru/nauka/2019-02-26/11_7518_dim2.html