ИТ-образование: методология, методическое обеспечение

УДК 378:37.031.4

Минзов А.С.[1], Токарева Н.А.[1], Черемисина Е.Н.[2]

[1]Государственный университет «Дубна», г. Дубна, Россия
[2] Отделение «Геоинформатики «ВНИИгеосистем», ФГБУ «Всероссийский научно-исследовательский геологический нефтяной институт», г. Москва, Россия

О СОВЕРШЕНСТВОВАНИИ СИСТЕМЫ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ В СВЕТЕ НОВОЙ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

Аннотация

В статье проводится анализ основных положений новой доктрины информационной безопасности и рассматриваются пути её реализации в развитии науки и образования в сфере обеспечения информационной безопасности общества и организаций.

Ключевые слова

Доктрина; информационная безопасность; киберугрозы; образование.

Minzov A.S.[1], Tokareva N.A.[1], Cheremisina E.N.[2]

[1] Dubna State University, Dubna, Russia
[2] Department of «Geoinformatics «VNIIgeosystem», Federal State Budgetary Institution «All-Russian Research Geological Oil Institute», Moscow, Russia

ON IMPROVEMENT OF THE SYSTEM OF HIGHER PROFESSIONAL EDUCATION IN THE LIGHT OF THE NEW DOCTRINE OF INFORMATION SECURITY OF RUSSIA

Abstract

The article analyzes the main provisions of the new doctrine of information security and the basic ways of its realization in the development of science and education in the sphere information security of society, organization and personality.

Keywords

Doctrine; information security; cyber threats; education.

Введение

Новая доктрина информационной безопасности [1], принятая в декабре 2016 года, представляет собой стратегический план развития системы обеспечения национальной безопасности РФ в информационной сфере деятельности. Однако, в отличие от предыдущей подобной доктрины 2000 года [2], в новой доктрине главные стратегические цели информационной безопасности существенно расширились в сторону *защиты жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в сферах обороны и безопасности, экономики, науки и образования, стратегической стабильности.* Стоить отметить, что в доктрине более четко определено и само содержание понятия «*обеспечение информационной безопасности РФ*», которое несколько изменилось и включило следующий комплекс взаимоувязанных мер: *правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.*

Доктрина стала более конкретной и направленной в сторону совершенствования национальной безопасности. Основными причинами резкого изменения направленности доктрины 2016 года по сравнению с предшествующей стали [1]:

1. Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на

информационную инфраструктуру в военных целях, а также усиление деятельности организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

2. Усиление активности кибератак и изменение направленности их на объекты ключевой инфраструктуры [3].
3. Появление нового высокоинтеллектуального вредоносного кода (StaxNet, Duqu, Flame и др.), способного проникать различными путями в корпоративные и промышленные автоматизированные системы управления технологическими процессами, исследовать их, модифицировать программное обеспечение, скрывать свои действия и самоликвидироваться при определенных условиях [3].
4. Стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.
5. Появление новых технологий информационно-психологического воздействия на население с использованием социальных сетей (Twitter, FaceBook, YouTube и др.) и СМИ. Практические результаты применения этих технологий были реализованы в ряде произошедших социальных революций в арабских странах в 2011 году [3].
6. Увеличение в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики РФ. Наращивание информационного воздействия на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.
7. Зависимость отечественной промышленности от зарубежных информационных технологий, электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи.
8. Недостаточная эффективность научных исследований, направленных на создание перспективных информационных технологий.
9. Недостаточное кадровое обеспечение в области информационной безопасности, а также низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности.
10. Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения.
11. Отсутствие комплексной основы при выполнении мероприятий по обеспечению безопасности информационной инфраструктуры с использованием отечественных технологий и продукции. Т.е. речь идет фактически об отсутствии системности в данном направлении деятельности.

В новой доктрине были сформулированы взаимоувязанные основные направления деятельности в сфере информационной безопасности, которые должны быть осмыслены и детализированы в конкретных задачах. Отсюда и цель настоящего исследования: *определить состав задач, направленных на совершенствование профессиональной подготовки персонала в сфере информационной безопасности, и предложить механизмы их реализации*.

Основные направления обеспечения информационной безопасности в области науки, технологий и образования

В Доктрине информационной безопасности сформулированы следующие пять направлений, непосредственно связанных с совершенствованием кадрового обеспечения сферы информационной безопасности:

- достижение конкурентоспособности российских информационных технологий (ИТ) и развитие научно-технического потенциала в области обеспечения информационной безопасности (ИБ);
- создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;
- проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;
- развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;
- обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

Рассмотрим более подробно требования к системе подготовки кадров, которые предъявляют эти направления обеспечения информационной безопасности.

Понятие «*конкурентоспособность ИТ в области ИБ*» (*первое направление*) обычно подразумевает

создание ИТ, свойства и функции которых сопоставимы или превышают возможности аналогичных технологий зарубежного производства. При этом понятие «*ИТ в области ИБ*» может быть рассмотрено с двух точек зрения:

- создание ИТ, реализующих только функции ИБ. К таким технологиям относятся антивирусное программное обеспечение (ПО), системы предотвращения утечек информации ограниченного доступа (DLP, Data leak prevention,), системы обнаружения и предотвращения вторжений (IDS/IPS, Intrusion detection system / Intrusion prevention system) и другие технологии;
- создание ИТ со встроенными функциями ИБ. К этому классу технологий относятся ИТ, в которых спроектированы и реализованы профили и задания по безопасности с использованием технологий разработки ИТ на основе «общих критериев»[38].

Изучение этих двух классов ИТ в сфере ИБ является обязательным, но недостаточным условием для успешного решения задач первого направления в области совершенствования образования. На наш взгляд, главным условием создания конкурентоспособных технологий является *овладение не только современными методами проектирования ИТ, но* и *способностью к созданию инновационных проектов в сфере информационной безопасности*. К сожалению, обучение методам создания инновационных проектов в сфере информационной безопасности сегодня практически не проводится и в планах учебных дисциплин образовательных учреждений встречается крайне редко. Введение в учебные планы дисциплины «Инновационный менеджмент» не решает всей проблемы подготовки студентов к разработке инновационных решений, так как концепция этой дисциплины практически во всех учебных пособиях направлена на управление поиском и внедрением инноваций, а не на создание инновационных идей в сфере ИТ и информационной безопасности. Отсюда возникает острая необходимость научной проработки учебной дисциплины «*Методология инновационных проектов в сфере ИТ и ИБ*» с описанием наиболее ярких и интересных инновационных решений в этой сфере деятельности и методологии разработки инновационных идей [7].

Вторая часть этого направления связана с *совершенствованием научно-технического потенциала* (НТП) в сфере информационной безопасности. Понятие НТП представляет собой совокупность трудовых, материально-технических, финансовых, информационных и организационных ресурсов для осуществления комплекса научных исследований и разработок, а также внедрение их результатов в производство [8]. Это понятие актуально как на уровне государства, так и на уровне организации. Во всех случаях НТП предполагает реализацию следующего цикла процессов: генерирование научных идей, их реализацию и практическое внедрение. Нормативно-правовой основой реализации этого цикла является Федеральный закон №217 [9], который разрешает образовательным учреждениям быть учредителями хозяйственных обществ, осуществляющих практическое применение и внедрение результатов своей интеллектуальной деятельности на условиях применения упрощенной системы налогообложения и льгот по страховым отчислениям. К сожалению, практическая реализация этой формы создания и совершенствования НТП вузами в настоящее время используется недостаточно по нескольким причинам, главными из которых являются:

1. Высокая загруженность профессорско-преподавательского состава кафедр информационной безопасности организационно-методической работой (разработка учебных планов, основных профессиональных образовательных программ, рабочих учебных программ, фондов оценочных средств), связанной с переходом за последние 2 года на новые стандарты от ФГОС 3 до ФГОС3+ (2015 г.), ФГОС3++(2016 г.), а в ближайшем будущим и ФГОС4.
2. Необходимость реализации кафедрами собственных научных программ, направленных на повышение качества обучения, разработку электронных образовательных ресурсов (ЭОР), расширение профилей и программ обучения, внедрение новых форм обучения, руководство научными работами студентов и подготовка их к участию в научных конференциях и конкурсах.
3. Отсутствие у кафедр опыта создания и управления хозяйствующими субъектами научно-технико-внедренческого типа при образовательных учреждениях.
4. Высокая степень риска успешного функционирования этих проектов из-за отсутствия механизмов их начального финансирования на запуск проекта, включающего подготовку персонала, закупку или аренду оборудования, приобретение материалов, аренду помещений, оплату персонала и решение других организационных и технических вопросов. Эти хозяйствующие субъекты практически сразу же после создания

38*Общие критерии – термин, определяющий серию стандартов ГОСТ ИСО/МЭК 15408 части 1,2,3 [4-6]*

должны вести как научную, так и бизнес-деятельность со всеми присущими этому видами деятельности процессами (научный и производственный менеджмент, маркетинг, реклама, логистика, организация внедрения, бухгалтерия и т. д.).

Практическая реализация задач *второго направления* по созданию и внедрению информационных технологий, изначально устойчивых к различным видам воздействия, для нас не является новой. В образовательном процессе кафедр информационной безопасности многих вузов предусматривается изучение методов проектирования встроенных систем безопасности в ИТ [4-6]. Однако, на наш взгляд, этому направлению сегодня не уделяется достаточного внимания, особенно при проектировании АСУТП реального времени[39]. Основная причина такого состояния заключается в том, что решения по созданию устойчивых к различным воздействиям ИТ обычно являются комплексными и требуют разработки новых подходов и решений в сфере информационной безопасности по созданию *доверенной среды*[40]. Существующие решения на основе отечественной криптографии не позволяют обеспечить технические требования по обработке информации в реальном времени. Это может быть достигнуто только на основе *облегченной криптографии, реализованной в виде отдельных компонент в SCADA–системах.* Это направление сегодня практически не обсуждается и не развивается.

Третье направление, связанное с интенсификацией проведения научных исследований и осуществлением опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности, тесно связано с рассмотренными нами ранее направлениями. На наш взгляд, это требование доктрины требует решения в системе высшего профессионального образования и других задач:

1. Повышение уровня научности и обоснованности предлагаемых студентами решений в выпускных квалификационных работах (ВКР). Темы ВКР в магистратуре должны быть обязательно связаны с созданием новых решений в сфере информационной безопасности или со значительной (инновационной) модернизацией имеющихся.
2. Повышение активности студентов и студенческих коллективов в участии в научных конференциях, семинарах, конкурсах, летних школах и соревнованиях CTF. Задача кафедр информационной безопасности – создание системы мотивации студентов, разработка и публикация новых научных направлений.
3. Повышение открытости конкурсов среди студентов и проведение обязательной публикаций открытых работ, занявших призовые места.
4. Повышение открытости грантов для студентов, научных сотрудников и преподавателей с обязательным свободным доступам к отчетам по выполненным открытым работам.
5. Усиление обратной связи между образовательными учреждениями и организациями, предлагающими промышленные разработки в сфере ИБ, путем публикации ими актуальных направлений научных исследований.

Развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий (*четвертое направление*) может решаться как самостоятельно путем обучения, тренингов и осведомления персонала организации в соответствии с политикой подготовки персонала в сфере ИБ, так и путем реализации программ в образовательных учреждениях. В настоящее время большинство специализированных кафедр вузов реализует основные образовательные программы высшего профессионального образования, в меньшей степени уделяя внимание программам повышения квалификации и профессиональной переподготовки персонала. На наш взгляд, сочетание разных образовательных программ для специалистов различного уровня позволяет в целом повысить качество обучения по основным образовательным программам, так как опирается на конкретную практическую деятельность и опыт привлекаемых специалистов-практиков.

Заключение

В статье был проведен анализ новой доктрины информационной безопасности, утвержденной Указом Президента РФ 5 декабря 2016 года. Доктрина включает комплекс взаимосвязанных мер защиты информации, который приводит к

39*Режим реального времени — это способ обработки информации, при котором обеспечивается взаимодействие системы обработки информации с внешними по отношению к ней процессами в темпе, соизмеримом со скоростью протекания этих процессов (ГОСТ 15971-90. Системы обработки информации. Термины и определения).*

40*Доверенная среда — область функционирования доверенных компонентов информационных систем, в пределах которой обеспечиваются необходимые условия их целостности, непрерывности и поддержания требуемого уровня доверия на всем протяжении их жизненного цикла (авт.).*

необходимости существенных изменений в различных сферах деятельности, в том числе, в системе высшего профессионального образования в сфере информационной безопасности. Предложен ряд новых мер по совершенствованию подготовки специалистов ИБ, созданию конкурентоспособных ИТ в сфере ИБ, совершенствованию НТП, созданию и внедрению информационных технологий, изначально устойчивых к различным видам воздействия, интенсификации НИР и совершенствованию кадрового потенциала. Рассмотренные нововведения начинают использоваться в образовательном процессе Института системного анализа и управления университета «Дубна».

Литература

1. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.).
2. Доктрина информационной безопасности РФ (утверждена Указом Президента РФ № 1895 от 9 сентября 2000 г.).
3. Минзов А.С. E-PR (Electronic and everything PR). Концепции, модели, технологии и механизмы реализации.-М.: ВНИИгеосистем, 2012, 235 с.
4. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
5. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.
6. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
7. Андропова Е.В., Сухомлин В.А. Диверсификация программ профессиональной подготовки в международных образовательных стандартах в области информационных технологий / Е.В. Андропова, В.А. Сухомлин // Вестник Московского университета. Серия 20: Педагогическое образование. 2013. № 1. С. 73-86.
8. Краткий экономический словарь, М., 1987
9. Федеральный закон от 2 августа 2009 г. N 217-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам создания бюджетными научными и образовательными учреждениями хозяйственных обществ в целях практического применения (внедрения) результатов интеллектуальной деятельности".

References

1. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii (utverzhdena Ukazom Prezidenta RF № 646 ot 5 dekabrja 2016 g.).
2. Doktrina informacionnoj bezopasnosti RF (utverzhdena Ukazom Prezidenta RF № 1895 ot 9 sentjabrja 2000 g.).
3. Minzov A.S. E-PR (Electronic and everything PR). Koncepcii, modeli, tehnologii i mehanizmy realizacii.-M.: VNIIgeosistem, 2012, 235 s.
4. GOST R ISO/MJeK 15408-1-2012 Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast' 1. Vvedenie i obshhaja model'.
5. GOST R ISO/MJeK 15408-2-2013 Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast' 2. Funkcional'nye komponenty bezopasnosti.
6. GOST R ISO/MJeK 15408-3-2013 Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast' 3. Komponenty doverija k bezopasnosti.
7. Andropova E.V., Suhomlin V.A. Diversifikacija programm professional'noj podgotovki v mezhdunarodnyh obrazovatel'nyh standartah v oblasti informacionnyh tehnologij / E.V. Andropova, V.A. Suhomlin // Vestnik Moskovskogo universiteta. Serija 20: Pedagogicheskoe obrazovanie. 2013. № 1. S. 73-86.
8. Kratkij jekonomicheskij slovar', M., 1987
9. Federal'nyj zakon ot 2 avgusta 2009 g. N 217-FZ "O vnesenii izmenenij v otdel'nye zakonodatel'nye akty Rossijskoj Federacii po voprosam sozdanija bjudzhetnymi nauchnymi i obrazovatel'nymi uchrezhdenijami hozjajstvennyh obshhestv v celjah prakticheskogo primenenija (vnedrenija) rezul'tatov intellektual'noj dejatel'nosti".

Поступила 20.05.2017

Сведения об авторах:

Минзов Анатолий Степанович, доктор технических наук, профессор кафедры информационных технологий ГБОУ ВО Московской области «Университет «Дубна», 9083083@rambler.ru

Токарева Надежда Александровна, кандидат физико-математических наук, заведующий кафедрой информационных технологий ГБОУ ВО Московской области «Университет «Дубна», tokareva@uni-dubna.ru

Черемисина Евгения Наумовна, доктор технических наук, профессор, заведующий отделением «Геоинформатики «ВНИИгеосистем», ФГБУ «Всероссийский научно-исследовательский геологический нефтяной институт», lena@geosys.ru

Note on the authors:

Minzov Anatoliy, doctor of technical sciences, professor of the Department of Information Technologies, Dubna State University, 9083083@rambler.ru

Tokareva Nadezhda, Candidate of Physical and Mathematical Sciences, head of the Department of Information Technologies, Dubna State University, tokareva@uni-dubna.ru

Cheremisina Evgeniya, doctor of technical sciences, professor, head of the Department of «Geoinformatics «VNIIgeosystem», Federal State Budgetary Institution «All-Russian Research Geological Oil Institute», lena@geosys.ru