УДК 378:37.031.4

НОВЫЕ ЗАДАЧИ ПОДГОТОВКИ КАДРОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ В КОНТЕКСТЕ «ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ» (2016)

Астахова Л.В., Томилов А.А.

ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет), Челябинск, e-mail: tomilov62@yandex.ru

В статье показан непрерывный рост утечек защищаемой информации по вине внутренних нарушителей – настоящих и бывших сотрудников организации; определены новые задачи по подготовке кадров по защите информации в контексте новой «Доктрины информационной безопасности Российской Федерации» (2016 год), связанные с развитием культуры информационной безопасности личности и общества, защиты от информационных воздействий на индивидуальное, групповое и общественное сознание, повышением эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям, развитием кадрового потенциала в области обеспечения информационной безопасности и др.; выявлено противоречие между этими задачами и отсутствием их отражения в новых федеральных государственных образовательных стандартах высшего образования и профессиональных стандартах по информационной безопасности; намечены пути разрешения обоснованного противоречия.

Ключевые слова: информационная безопасность, защита информации, кадры, задачи, доктрина.

NEW PROBLEMS OF TRAINING ON PROTECTION OF INFORMATION IN THE CONTEXT OF “DOCTRINE OF INFORMATION SECURITY OF THE RUSSIAN FEDERATION” (2016)

Astakhova L.V., Tomilov A.A.

South Ural State University (national research university), Chelyabinsk, e-mail: tomilov62@yandex.ru

The article shows the continuous growth of leakage of protected information through the fault of internal infringers - current and former employees of the organization; New tasks for the training of personnel in the protection of information in the context of the new "Doctrine of Information Security of the Russian Federation" (2016), related to the development of a culture of information security of the individual and society, protection against information impacts on individual, group and public consciousness, increasing the effectiveness of preventing offenses committed using information technology, and counteracting such violations, the development of human resources in the field of information security, etc.; revealed a contradiction between these tasks and the lack of their reflection in the new federal state educational standards of higher education and professional standards for information security; The ways of resolving a justified contradiction are outlined.

Keywords: information security, information protection, personnel, tasks, doctrine.

Стремительное развитие информационного общества в России обострило проблему информационной безопасности. По данным Аналитического центра InfoWatch в России, только за I полугодие 2016 года зарегистрировано 840 случаев утечки конфиденциальной информации, что на 16 % больше, чем за аналогичный период 2015 года. При этом большинство утечек информации происходит по вине внутренних нарушителей – настоящих или бывших сотрудников организации [5]. В 2015 году по вине или неосторожности внутреннего нарушителя утечка информации произошла в 984 (65,4 %) случаях [6], а за I полугодие 2016 года по этой причине зарегистрировано уже 506 (67 %) утечек информации. Доля умышленных утечек по отношению к случайным тоже растет.

Принятие новой Доктрины информационной безопасности Российской Федерации

(далее – Доктрина) стало особенно актуально в связи с политическим, в том числе – информационным давлением на Россию в новых социально-политических условиях разрушения однополярного мира. По мнению авторов документа – членов Совета безопасности РФ, Россия должна находиться в постоянной готовности к противоборству в информационной среде [2]. Эксперты справедливо отмечают, что в новом документе гораздо больше упоминаний о защите от информационно-психологического воздействия, что обусловлено увеличением количества зарубежных СМИ, имеющих предвзятые взгляды на российскую политику. Еще одно актуальное направление деятельности в области государственной и общественной безопасности – это профилактика и противодействие преступности в информационной сфере, также имеющие человеческую природу [3].

Как справедливо заметил В.А. Северин, новая Доктрина информационной безопасности Российской Федерации впервые выделяет угрозы интересам коммерческих организаций, в т.ч. сфере ОПК и меры по их предупреждению, которые ранее самостоятельно формировали собственную систему информационной безопасности [11]. Все причины нарушения режима коммерческой тайны (организационно-управленческого, воспитательного и правового характера) также связаны с человеком.

Обострившееся противоречие между заявленной в «Доктрине информационной безопасности Российской Федерации» (2016) потребностью современной экономики в специалистах, способных эффективно управлять кадровой безопасностью организаций, развитием культуры информационной безопасности граждан и – недостаточным использованием возможностей вуза в развитии управленческой компетенции в области кадровой безопасности будущего специалиста по защите информации обусловливает актуальность темы настоящей статьи.

Ее цель – обосновать низкий уровень соответствия новых федеральных государственных стандартов высшего образования и профессиональных стандартов по информационной безопасности новым задачам подготовки кадров по защите информации в контексте «Доктрины информационной безопасности Российской Федерации» (2016) и определить пути повышения этого уровня.

Как указывается в новой «Доктрине информационной безопасности Российской Федерации» 2016 года [4], террористические и экстремистские организации широко используют не только средства деструктивного воздействия на объекты критической информационной инфраструктуры, но механизмы информационного воздействия на индивидуальное, групповое и общественное сознание. При этом низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности становится причиной нарушения информационной безопасности личности. Поэтому «Доктрина

информационной безопасности Российской Федерации» (2016) подчеркивает тенденцию к развитию как средству предупреждения угроз информационной безопасности не только государства, но и любой организации и гражданина. Так, п.23 Доктрины определяет одним из основных направлений обеспечения информационной безопасности «повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям»; п.27 нацеливает на «развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий» и «обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности» [4].

Названные задачи можно сгруппировать по двум направлениям деятельности. Первая группа задач связана с защитой информационных ресурсов, а также с защитой сотрудника любой организации от деструктивных информационных воздействий. Вторая группа задач базируется на развитии культуры информационной безопасности гражданина, а также на развитии его личности. Обе группы задач для руководителя организации – это задачи по обеспечению кадровой безопасности. Это требует от системы высшего образования подготовки специалистов по защите информации, способных управлять кадровой безопасностью организации и свести к минимуму кадровые угрозы: и угрозы защищенности, и угрозы развития. Только единство этих двух направлений решаемых задач будет способствовать достижению кадровой безопасности как подсистемы информационной безопасности.

Как же эти задачи отражены в федеральных государственных образовательных стандартах высшего образования и профессиональных стандартах по информационной безопасности?

Переход высшего профессионального образования на компетентностный подход актуализировал изучение проблем, связанных с определением способов формирования не отдельных знаний и умений, а компетенций, обеспечивающих решение задач управления информационной безопасностью. Однако управленческая компетенция в области кадровой безопасности не упоминается в образовательных стандартах группы «Информационная безопасность» третьего поколения. Отсутствует управление кадровой безопасностью и в перечне трудовых функций и действий в профессиональных стандартах специалист по защите информации (2016) [7-10]. При этом работодатели указывают на низкий уровень владения выпускниками этой компетенцией, на неспособность выполнять эту трудовую функцию.

Новое поколение ФГОС ВО по информационной безопасности, как и ФГОС ВПО, не

предусматривают формирования названной компетенции. Так, в ФГОС 3+ по специальности 10.05.03 «Информационная безопасность автоматизированных систем» эта компетенция угадывается в ПК-4 – «способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы» и в ПК-5 – «способность проводить анализ рисков информационной безопасности автоматизированной системы». Очевидно, что кадровые угрозы и риски не выделены отдельно, и, хотя имеют ярко выраженную специфику, должны изучаться студентами в комплексе с другими угрозами и рисками. Однако, поскольку типовые рабочие программы дисциплин отсутствуют, вузы, к сожалению, традиционно будут считать обучение студентов технологиям кадровой безопасности автоматизированных систем задачей факультативной.

ФГОС 3+ по образовательному направлению 10.03.01 «Информационная безопасность» предусматривает овладение выпускником «способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты» (ПК-4), что, казалось бы, предполагает использование не только технических, но и гуманитарных методов защиты информации в комплексе. Однако, ПК-6 – «способность принимать участие в организации и проведении проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации» – явно не предполагает организационных мер работы с кадрами и оценки их результативности, что противоречит комплексному подходу к защите информации. Очевидно, что отсутствие в федеральных образовательных стандартах и профессиональных стандартах управленческой компетенции по обеспечению кадровой безопасности обостряет проблему не только реализации требований Доктрины, но и самого субъекта этой деятельности.

И все же определить субъекта обеспечения кадровой безопасности помогают международные и российские стандарты по управлению информационной безопасностью. В них четко и недвусмысленно работа с кадрами закреплена за специалистами по информационной безопасности и выделены три стадии взаимодействия человека с нанимающей его организацией: трудоустройства, занятости и увольнения. В ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [1] (п. 8) регламентируются правила и методы работы с персоналом в целях обеспечения конфиденциальности, целостности и доступности информационных активов на предприятии. Для комплексного обеспечения безопасности, связанной с персоналом, принимаются организационные меры на всех трех стадиях взаимодействия человека с нанимающей его организацией: трудоустройства, занятости и увольнения.

Что касается бакалавров управления персонала, то в новом стандарте ФГОС ВО в качестве профессиональных задач выпускника обозначено «участие в обеспечении безопасных условий труда, экономической и информационной безопасности [16]. Это подчеркивает главенство специалиста по защите информации в деятельности управления кадровой безопасностью в системе информационной безопасности в организации.

Изложенное позволяет заключить, что главным субъектом обеспечения кадровой безопасности сегодня в наибольшей степени призван, согласно стандартам по управлению информационной безопасностью и образовательным стандартам, выпускник укрупненной группы специальностей по образовательному направлению «Информационная безопасность».

Однако, несмотря на то, что ФГОС ВО группы «Информационная безопасность» утверждены совсем недавно, после утверждения Президентом «Доктрины информационной безопасности Российской Федерации», они по-прежнему не акцентируют внимание на вопросах кадровой безопасности. Исключение составляет ФГОС ВО по специальности «Безопасность информационных технологий в правоохранительной сфере», в котором профессиональной задачей выпускника определяется «противодействие деструктивным и негативным информационно-психологическим воздействиям» [13]. Эта компетенция, безусловно, важна и в работе с кадрами организации. И все же для выполнения функции управления кадровой безопасностью специалист по защите информации должен обладать соответствующими компетенциями, сформулированными в образовательных стандартах в контексте управления человеческими ресурсами информационной безопасности. Так, В.А. Северин включает в систему предупреждения правонарушений в информационной сфере организаций такие элементы, как определение субъектов профилактики и наделение их полномочиями; установление содержания объектов профилактики; реализация мероприятий и применение мер ответственности к виновным; оценка эффективности профилактики и разработка дополнительных мер предупреждения. Мы разделяем позицию автора, который связывает эффективность обеспечения охраны конфиденциальности информации с необходимостью аналитической работы: выявлением причин нарушений и разработкой мер по их предупреждению [11], что требует профессиональной подготовки работников служб информационной безопасности на основе междисциплинарных знаний.

Изложенное позволяет заключить, что утвержденные в конце 2016 года образовательные стандарты по подготовке специалистов, бакалавров и магистров информационной безопасности [12-15] нуждаются в серьезной корректировке: управленческая компетенция в области кадровой безопасности должна найти в них более широкое отражение. Профессиональные стандарты по информационной безопасности также

должны быть дополнены трудовой функцией управления кадровой безопасностью организации.

Учебные планы по информационной безопасности в свете требований новой Доктрины не могут не содержать специальную дисциплину, связанную с кадровой безопасностью. Если нет специальной дисциплины – соответствующие содержательные блоки необходимо включать в стандартные дисциплины по организационной защите информации, управлению информационной безопасностью, комплексным системам защиты информации и др. Не должны игнорировать этот аспект и Учебные центры, реализующие образовательные программы по повышению квалификации и переподготовке специалистов в области информационной безопасности.

Новые задачи по работе с кадрами специалиста по защите информации актуализируют развитие его педагогической компетенции, что следует учесть в процессе обучения студентов данных образовательных направлений дисциплине «Педагогика» на всех уровнях непрерывного образования в области информационной безопасности.

Анализ результатов педагогических исследований также свидетельствует о недостаточном внимании к развитию управленческой компетенции в области кадровой безопасности будущих и действующих специалистов по защите информации, к учебно-методическому обеспечению этого процесса, дидактический потенциал вуза как субъекта развития этой компетенции обучающихся остается нераскрытым. Это требует от научно-педагогического сообщества интенсивных усилий по теоретической и организационно-методической разработке названной проблемы. Авторами настоящей статьи разработаны программа и методические указания по дисциплине «Кадровая безопасность» для будущих специалистов по защите информации. В них учтены требования новой Доктрины информационной безопасности Российской Федерации. Они предполагают, во-первых, освоение технологий защиты сотрудников организации от негативных информационных воздействий для профилактики угроз защищаемой информации в организации, и, во-вторых, – технологий их личностного развития, в т.ч. культуры информационной безопасности. Только единство этих двух задач позволит на практике интегрировать интересы и цели работодателя и сотрудника, обеспечивая тем самым повышение информационной и экономической безопасности организации.

Таким образом, научная новизна настоящей статьи заключена в выявлении противоречия меду новыми, актуальными задачами, поставленными перед высшим образованием «Доктриной информационной безопасности Российской Федерации» (2016), и низким уровнем отражения этих задач в новых федеральных государственных образовательных стандартах высшего образования и профессиональных стандартах по

информационной безопасности; а также в разработке путей разрешения обоснованного противоречия.

Работа выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Список литературы

1. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности». – М.: Стандартинформ, 2014. – 96 с.
2. Гостищева Т.В. О новой Доктрине информационной безопасности РФ /Т.В. Гостищева, А.А. Мисников, И.В. Красильников // Актуальные проблемы обеспечения информационной безопасности: материалы международной научно-практической и научно-методической конференции. – Уфа, 2016. – С. 26-32.
3. Димитренко Е.В. Сравнительный анализ доктрины информационной безопасности РФ в старой и новой редакции /Е.В. Димитренко, А.Ю. Швецов, А.М. Мастяева // Современные проблемы и перспективные направления инновационного развития науки: сборник статей международной научно-практической конференции: в 8 частях. – М., 2016. – С. 139-140.
4. Доктрина информационной безопасности Российской Федерации: Утверждена Указом Президента РФ 05.12.2016. – [Электронный ресурс]. – URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.
5. Исследование утечек конфиденциальной информации в первом полугодии 2016 года //Аналитический центр компании InfoWath. – [Электронный ресурс]. – URL: https://www.infowatch.ru/report2016_half.
6. Исследование утечек конфиденциальной информации в 2015 году //Аналитический центр компании InfoWath. – [Электронный ресурс]. – URL: https://www.infowatch.ru/report2015_half.
7. Об утверждении профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях»: Приказ Минтруда России от 03.11.2016 N 608н (Зарегистрировано в Минюсте России 25.11.2016 N 44449). – [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_207929.
8. Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей»: Приказ Минтруда России от 01.11.2016 N 598н (Зарегистрировано в Минюсте России 28.11.2016 N 44464). – [Электронный ресурс]. – URL:

http://www.consultant.ru/document/cons_doc_LAW_207932.

9. Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах»: Приказ Минтруда России от 15.09.2016 N 522н (Зарегистрировано в Минюсте России 28.09.2016 N 43857). – [Электронный ресурс]. – URL:http://www.consultant.ru/document/cons_doc_LAW_205593.

10. Об утверждении профессионального стандарта «Специалист по технической защите информации»: Приказ Минтруда России от 01.11.2016 N 599н (Зарегистрировано в Минюсте России 25.11.2016 N 44443). – [Электронный ресурс]. – URL:http://www.consultant.ru/document/cons_doc_LAW_207927.

11. Северин В.А. Теоретико-методологические основы обеспечения безопасности коммерческих структур в информационной сфере / В.А. Северин // Информационное право. – 2016. – № 4. – С. 13-19.

12. Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета): приказ Минобрнауки России от 1 декабря 2016 г. N 1509 (Зарегистрировано в Минюсте России 20 декабря 2016 г. № 44831). – [Электронный ресурс]. – URL: http://fgosvo.ru/uploadfiles/fgosvospec/100503.pdf.

13. Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки (специальности) 10.05.05 Безопасность информационных технологий в правоохранительной сфере (уровень специалитета): приказ Минобрнауки России от 19 декабря 2016 г. N 1612 (Зарегистрировано в Минюсте России 11 января 2017 г. № 45174). – [Электронный ресурс]. – URL: http://fgosvo.ru/uploadfiles/fgosvospec/100505.pdf.

14. Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки (специальности) 10.05.01 Компьютерная безопасность (уровень специалитета): приказ Минобрнауки России от 1 декабря 2016 г. N 1512 (Зарегистрировано в Минюсте России 20декабря 2016 г. № 44825). – [Электронный ресурс]. – URL: http://fgosvo.ru/uploadfiles/fgosvospec/100501.pdf.

15. Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки (специальности) 10.03.01 Информационная безопасность (уровень бакалавриата): приказ Минобрнауки России от 1 декабря 2016 г. N 1515 (Зарегистрировано в Минюсте России 20 декабря 2016 г. № 44821). – [Электронный ресурс]. – URL: http://fgosvo.ru/uploadfiles/fgosvob/100301.pdf.

16. Об утверждении федерального государственного образовательного стандарта

высшего образования по направлению подготовки (специальности) 38.03.03 Управление персоналом (уровень бакалавриата): приказ Минобрнауки России от 14 декабря 2015 г. N 1461 (Зарегистрировано в Минюсте России 19 января 2016 г. № 40640). – [Электронный ресурс]. – URL: http://fgosvo.ru/uploadfiles/fgosvob/380303.pdf.