УДК 004.056

Р.В. МЕЩЕРЯКОВ, А.А. ШЕЛУПАНОВ

КОНЦЕПТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНА И ПОДГОТОВКИ КАДРОВ

Мещеряков Р.В., Шелупанов А.А. **Концептуальные вопросы информационной безопасности региона и подготовки кадров.**

Аннотация. В статье рассматриваются концептуальные вопросы, определяющие состояние информационной безопасности государства и региона. Предлагается подход к формированию функций защиты и функций состояния безопасности на региональном уровне. Описываются различные требования к обеспечению требуемого уровня информационной безопасности. Приводятся сведения по подготовке кадров в области информационной безопасности в Сибирском и Дальневосточном федеральном округах.

Ключевые слова: информационная безопасность, концепция, высшее образование, подготовка кадров.

Meshcheryakov R. V., Shelupanov A.A. **Conceptual issues of information security of the region and training.**

Abstract. The article discusses the conceptual issues that determine the state of information security of the state and region. An approach to building security features and functions of state security at the regional level. Describes the various requirements to ensure the required level of information security. Provides information on training in the field of information security in the Siberian and Far Eastern Federal Districts.

Keywords: information security, conception, high education, personnel training.

1. Введение. Информационная безопасность является новой отраслью науки и требует пристального внимания и научного обоснования [1, 2]. Следует отметить очень важное, на наш взгляд, обстоятельство. Оно заключается в следующем. Несмотря на то, что информационная безопасность является новой и быстро развивающейся областью знаний, ряд аспектов, понятий, определений и представлений стали уже классическими. Одной из целей нашей работы является акцентирование внимания читателя на важнейшем принципе информационной безопасности – комплексности.

Любого рода информационная деятельность невозможна без осуществления вспомогательных (обеспечивающих) видов деятельности, непосредственно не преследующих нормативно определенных целей, но необходимых для их достижения. Одним из таких видов деятельности является защита информации. Этим термином обозначается регулярная деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [1]. Рассмотрим содержание и дадим определения основных компонентов этого понятия.

2. Требования к защите информации. Необходимость защиты информации существует в случае ее конфиденциальности, под которой понимается свойство, позволяющее не давать право на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам [1]. Вместе с тем классически выделяют три базовых понятия обеспечения требуемого уровня информационной безопасности: обеспечение конфиденциальности, целостности и доступности. Очевидно, что все обеспечение всех свойств информации подразумевает комплексность защиты информации.

Из этого следует, что потребность в защите информации - это определенное состояние субъекта информационной деятельности, которое возникает в связи с необходимостью защиты сведений, обеспечивающих решение его задач. При этом проблема выявления, описания и измерения потребностей в обеспечении конфиденциальности информации становится одной из основных в комплексе проблем защиты информации. Только на основе ее решения можно формулировать требования к защищенности информационной деятельности. При этом важно учитывать современные подходы и технологии к обеспечению национальной безопасности в условиях формирования информационного общества [3].

Потребности в защите информации определяют ее цель, которая состоит в обеспечении защищенности информационной деятельности. При этом под защищенностью информации понимается соответствие эффективности защиты информации требованиям нормативных документов [1].

В качестве субъекта защиты информации могут выступать сотрудники, реализующие свою информационную деятельность в условиях обеспечения ее конфиденциальности, а также специализированные подразделения, обеспечивающие:

– оборот документов, содержащих сведения, составляющие государственную и служебную тайну (или информацию другого уровня ограниченного распространения), их хранение и уничтожение, а также контроль над правильностью оборота таких документов;

– криптографическую защиту информации, передаваемой по каналам связи, а также учет и хранение документов, переданных по каналам связи;

– проведение комплекса мероприятий, направленных на исключение возможности утечки сведений, составляющих государственную и служебную тайну (или иную информацию ограниченного распространения), по так называемым «побочным» каналам (сети электропитания, радиотрансляция и т.п.).

Структурирование основных компонентов является необходимым, но недостаточным условием понимания сущности деятельности, так как не учитывает ряда факторов, непосредственно не входящих в понятие, но создающих определенную обстановку (среду), в которой осуществляется деятельность. При этом возникают противоречия в решении проблем информационной безопасности, изложенные в работе [4].

Среду деятельности по защите информации составляют сфера доминирования и неуправляемая сфера. К сфере доминирования относят средства, которыми располагает субъект деятельности, и элементы окружающей действительности, на которые он может воздействовать. Неуправляемую сферу образует группа элементов, на которые субъект деятельности не может воздействовать, но которые необходимо учитывать в виде ограничений [5].

В рамках среды определяется необходимый и достаточный набор активностей (процедур) по достижению целей защиты информации.

Будем называть процедурой защиты информации набор однородных в функциональном отношении действий (операций), регулярно осуществляемых субъектами по обеспечению защищенности своей информационной деятельности. Целями реализации процедур защиты информации являются закрытие информации или ее криптопреобразование инвариантно способу реализации процедуры и используемым средствам. Информация здесь рассматривается нами как предмет защиты (используемый специфический ресурс). При этом необходимо учитывать возможность проведения оперативно-розыскной и криминалистической деятельности [6].

Совокупность логически упорядоченных, взаимосвязанных и организованных процедур защиты информации, ведущая к достижению цели обеспечения защищенности информационной деятельности, составляет процесс защиты информации.

В общем случае процесс защиты информации может включать следующие процедуры: идентификация и аутентификация, паролирование и управление доступом к информации, учет событий, контроль состояния защиты информации, шифрование.

Очевидно, что формирование компетенций специалистов должно основываться на понятийном аппарате в области защиты информации и информационной безопасности [1]. Понятийный базис обеспечивает единство признаваемых требований. Таким образом,

можно формировать компетенции специалистов на базе концептуальных понятий деятельности в области защиты информации.

Это особенно важно при подготовке специалистов в области защиты информации и информационной безопасности. Опыт проведения курсов «Основы информационной безопасности» и «Комплексное обеспечение информационной безопасности автоматизированных систем» на кафедре Комплексной информационной безопасности электронно-вычислительных систем Томского государственного университета систем управления и радиоэлектроники показали необходимость формирования единого понятийного базиса.

Кроме того, анализ квалификации сотрудников отделов защиты информации Пенсионного фонда России (повышение квалификации которых проводилось на базе Центра технологий безопасности ТУСУРа) показал, что подготовка понятийного аппарата, соответствующего всем нормам [1-4] требует не только аккуратного обращения с терминами и определениями, но и четкого выстраивания логически упорядоченных взаимосвязей.

Принятие новых федеральных образовательных стандартов третьего поколения ФГОС ВПО 3 и работа над ФГОС ВО 3+ требует от преподавателя и выпускника планомерной работы над получением компетенций в рамках образовательных стандартов бакалавров, специалистов и магистров [7]. Кроме того, важно внимание необходимо уделить подготовке кадров высшей квалификации в области (аспирантура и адъюнктура) по научной специальности «информационная безопасность» и обеспечение защиты кандидатских и докторских диссертаций по специальности 05.13.19 – информационная безопасность, методы и средства защиты информации.

3. Состояние информационной безопасности государства. В работах [2, 3] справедливо и очень точно дана оценка современного состояния информационной безопасности. Следуя авторам этой работы, приведем их. В последние годы реализованы некоторые практические меры по укреплению информационной безопасности в Российской Федерации.

Осуществлен ряд мероприятий по совершенствованию информационной безопасности в органах государственной власти и управления, в государственных организациях и на предприятиях. Успешному решению ряда вопросов информационной безопасности способствует создание Государственной системы защиты информации в Российской Федерации от иностранных технических разведок и от ее

утечки по техническим каналам, а также систем лицензирования деятельности предприятий в области защиты информации и сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности в Российской Федерации показывает - в настоящее время ее уровень не отвечает жизненно важным потребностям личности, общества и государства. Сегодняшние условия политического и социально-экономического развития государства и общества вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения определенных ограничений на ее распространение со стороны государства. Отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве приводит ко многим негативным последствиям. Слабое обеспечение органов государственной власти и управления достоверной, своевременной и полной информацией затрудняет принятие обоснованных решений. Недостаточная защищенность государственного информационного ресурса, включая государственные информационные системы и критические системы, приводит к утрате важной политической, экономической и научно-технической информации, в том числе о высокоэффективных технологиях военного и двойного назначения.

Неразвитость информационных отношений в сфере предпринимательства тормозит становление цивилизованного рынка, а отсутствие механизма включения национального информационного ресурса в хозяйственный оборот приводит к серьезным экономическим потерям [7].

Потерям важной информации способствуют бессистемность защиты данных и слабая координация в общегосударственном масштабе мероприятий по защите информации, ведомственная разобщенность в обеспечении конфиденциальности информации.

Серьезно ослаблены меры по обеспечению сохранности государственных секретов, коммерческой и служебной тайны в органах государственной власти и управления и на предприятиях оборонного комплекса. Неудовлетворительно организована защита персональных данных, налоговой, таможенной, имущественной информации.

Отставание отечественных информационных технологий вынуждает идти по пути закупок незащищенной импортной техники, в результате чего повышается вероятность несанкционированного доступа к базам и банкам данных, а также возрастает зависимость

России от иностранных производителей компьютерной и телекоммуникационной техники и информационной продукции.

Положение дел с обеспечением информационной безопасности в Российской Федерации таково, что не позволяет ей на равноправной основе включиться в мировую информационную систему и требует безотлагательного решения следующих ключевых проблем [2]:

1. Развития научно-практических основ информационной безопасности, отвечающей современной геополитической ситуации и условиям политического и социально-экономического развития Российской Федерации.

2. Формирования законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, предприятий, нормативного закрепления ответственности должностных лиц и граждан за соблюдение требований информационной безопасности.

3. Разработки механизмов реализации прав граждан на информацию.

4. Формирования системы информационной безопасности, являющейся составной частью общей системы национальной безопасности страны.

5. Разработки современных методов и технических средств, обеспечивающих комплексное решение задач защиты информации.

6. Разработки критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации.

7. Исследований форм и способов цивилизованного воздействия государства на формирование общественного сознания.

8. Комплексного исследования деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

Решение вышеперечисленных ключевых проблем информационной безопасности должно осуществляться на основе соответствующей государственной политики. Проработка принципов и основных положений государственной политики обеспечения информационной безопасности была проведена коллективом ученых и специалистов в рамках Концепции информационной безопасности Российской Федерации.

В результате исследований сформулированы следующие основные принципы государственной политики обеспечения информационной безопасности:

1. Государственная политика должна обеспечить безусловное правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса. Она основывается на обязательном обеспечении прав граждан и организаций на свободное создание, поиск, получение и распространение информации любым законным способом и обеспечение защиты информации. В этих целях государство совершенствует существующее и разрабатывает новое законодательство и формирует нормативно-правовую базу информационных отношений в обществе, осуществляет контроль за безусловным исполнением законов и нормативно-правовых актов.

2. Государство исходит из того, что информационные ресурсы являются объектом собственности, и способствует введению их в хозяйственный оборот. Обеспечивается защита интеллектуальной собственности и неисключительных прав на информационные ресурсы, включая программное обеспечение.

3. Государство считает приоритетным развитие современных информационных и телекоммуникационных технологий и средств, способных обеспечить создание национальных телекоммуникационных сетей и включение России в глобальные информационные сети и системы мониторинга при соблюдении национальной безопасности Российской Федерации.

4. Государственная политика предусматривает согласованность решений, принимаемых органами власти и местного самоуправления для обеспечения информационной безопасности в рамках единого информационного пространства России. Государственная политика не допускает монополизма министерств, ведомств и организаций в области обеспечения информационной безопасности. Обеспечивается предоставление государственных услуг в электронной форме [8].

Основные положения государственной политики обеспечения информационной безопасности:

– государство формирует нормативно-правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

– государство законными средствами обеспечивает защиту общества от ложной, искаженной и недостоверной информации, поступающей через средства массовой информации;

– ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;

– государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности в области защиты информации;

– ответственность за сохранность, засекречивание и рассекречивание информации персонифицируется;

– доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учетом определяемых законом прав собственности на эту информацию;

– государство способствует предоставлению гражданам доступа к мировым информационным ресурсам, глобальным информационным сетям;

– юридические и физические лица, собирающие, накапливающие и обрабатывающее персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

– государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

– государство стремится к отказу от зарубежных информационных технологий для информатизации органов государственной власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

– государство прилагает усилия для противодействия информационной экспансии США и других развитых стран, поддерживает интернационализацию глобальных информационных сетей и систем.

На основе принципов и положений государственной политики обеспечения информационной безопасности должны проводиться все мероприятия по защите информации в политической, экономической, оборонной и других сферах деятельности государства. В этой связи следует иметь в виду, что в каждой из этих сфер имеются свои особенности, что в первую очередь связано с характером решения поставленных задач, наличием свойственных каждой области

информационной безопасности слабых элементов и уязвимых звеньев.

В каждой сфере деятельности государства требуется специальная организация работ, включая научные исследования [7], а также использование форм и способов обеспечения информационной безопасности.

В политической сфере наиболее серьезной опасности подвергаются:

– общественное сознание и политическая ориентация различных групп населения страны (регионов), непрерывно формируемые под воздействием отечественных и зарубежных средств массовой информации (печать, радио, телевидение);

– система принятия политических решений, существенно зависящая от качества и своевременности ее информационного обеспечения;

– право политических организаций, партий, объединений и движений на свободное выражение своих программ, социально-политических и экономических ориентацией через средства массовой информации;

– система регулярного информирования населения органами государственной власти и управления о политической и социально-экономической жизни через средства массовой информации, пресс-центры, центры общественных связей и т.п.;

– система формирования общественного мнения, включающая специальные институты, центры и службы выявления, изучения и анализа общественного мнения.

В сфере экономики наиболее подвержена воздействию угроз информационной безопасности система государственной статистики, а также источники, порождающие информацию о коммерческой деятельности хозяйственных субъектов всех форм собственности, о потребительских свойствах товаров и услуг, системы сбора и обработки финансовой, биржевой, налоговой, таможенной информации, информации о внешнеэкономической деятельности государства и коммерческих структур.

В оборонной сфере к наиболее уязвимым звеньям относятся:

– информационные ресурсы аппарата Министерства обороны, Генерального штаба, Главных штабов видов Вооруженных сил и родов войск, научно-исследовательских учреждений, содержащие сведения и данные об оперативных и стратегических планах подготовки и ведения боевых действий, о составе и дислокации войск, о мобилизационной готовности, тактико-технических характеристиках вооружения и военной техники;

– информационные ресурсы предприятий оборонного комплекса, содержащие сведения о научно-техническом и производственном потенциале, об объемах поставок и запасах стратегических видов сырья и материалов, об основных направлениях развития вооружения;

– военная техника, её боевые возможности и проводимые в интересах обороны фундаментальные и прикладные НИР;

– системы связи и управления войсками и оружием, их информационное обеспечение;

– политико-моральное состояние войск в части, зависящей от информационно-пропагандистского воздействия;

– информационная инфраструктура, в том числе центры обработки и анализа информации Генерального штаба и информационные подразделения штабов видов Вооруженных Сил, штабов объединений и соединений видов Вооруженных Сил и родов войск, пункты управления, узлы и линии радиосвязи, радиорелейной, тропосферной и спутниковой, а также линии проводной связи, развертываемые и арендуемые Министерством обороны и другими силовыми структурами.

Как справедливо отмечено в [2], общеизвестное практическое средство для оценки и снижения уровня риска содержит одиннадцать пунктов первоочередных оборонительных мероприятий:

– все сотрудники подписывают обязательство о неразглашении сведений ограниченного характера в качестве условия приема на работу;

– сотрудникам не разрешается приносить программные средства из дома или других внешних источников; им также не разрешается выносить компьютерные диски и другие магнитные носители с предприятия, передача данных по сети интернет или социальные сети;

– существует и действует политика информационной безопасности, обеспеченная соответствующим персоналом и ресурсами;

– обучение всех работников мерам безопасности проводится на регулярной основе;

– организация проводит квалифицированный анализ факторов риска и имеет план экстренного реагирования и план ликвидации последствий;

– все пользователи компьютерных систем имеют пароли, составленные методом случайной генерации, которые периодически

меняются, допускается использование средств усиленной аутентификации, включая биометрические [9,10, 11];

– все случаи нарушения безопасности тщательно расследуются и докладываются руководству;

– проводится проверка деятельности всех сотрудников до трудоустройства на работу;

– на каждом объекте существует программа контроля управления доступа и действий посетителей;

– существуют специальные методики при приеме на работу граждан других государств [12];

– безопасность каждого объекта проверяется регулярно [13].

4. Образовательные технологии по направлению информационной безопасности. Переход на новые стандарты ВПО ФГОС-3 в 2011 г. ознаменовал качественно новую стратегию подготовки специалистов в области информационной безопасности, которая повлекла модернизацию всех компонентов образовательного процесса. Реализация инновационной государственной образовательной политики обеспечения высокопродуктивными и профессионально эффективными кадрами потребовало совершенствования всех форм подготовки, переподготовки и повышения квалификации в области информационной безопасности.

За прошедший период Сибирское региональное отделение учебно-методического объединения (СибРОУМО) вузов России по образованию в области информационной безопасности продолжало мероприятия по совершенствованию методов адаптации основных образовательных профессиональных программ направления «Информационная безопасность» в Сибирском Федеральном округе (далее СФО) и в Дальневосточном федеральном округе (ДФО). Концепция непрерывного образования интегрирована в область высшего образования, как поэтапный процесс, обеспечивающий постоянное пополнение и расширение знаний.

Ниже на рисунке 1 схематично представлены составляющие непрерывного процесса подготовки кадров СФО и ДФО с перечислением вузов, обеспечивающих обучение в области информационной безопасности и основных компонентных условий реализации программ подготовки.

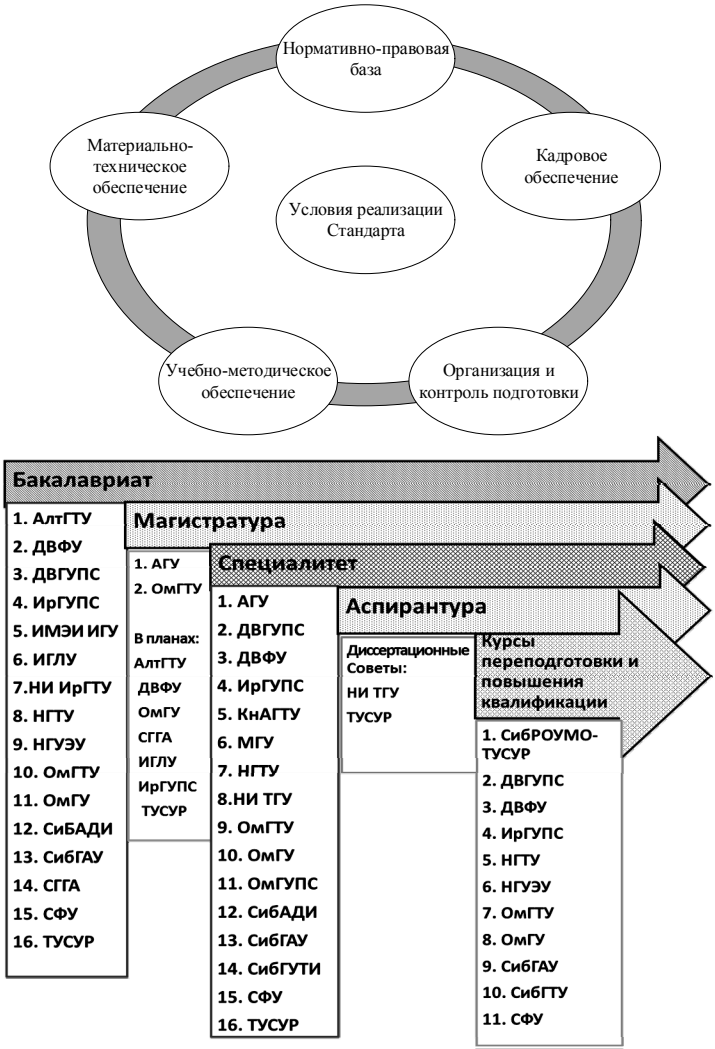

Рис. 1. Схема процесса непрерывного образования СФО и ДФО

Стратегия непрерывного профессионального развития включает, прежде всего, базисное профессиональное образование для получения знаний, умений, а также обучение профессиональным навыкам, удовлетворяющим компетенциям, заявленным в федеральных государственных образовательных стандартах.

4.1. Подготовка студентов ВПО в Сибирском и Дальневосточном регионах. За истекшие два года с 2012 по 2014 произошли изменения в области нормативно-правового регулирования, сопровождаемого нормативным пакетом документов. Приказом Минобрнауки России № 1061 от 12 сентября 2013 г. утверждён новый перечень направлений подготовки и введены новые классификационные коды с определением квалификаций специальностей в области информационной безопасности. Предложены новые методические рекомендации Минтруда России по доработке профессиональных стандартов ВПО в соответствии с заявленными уровнями квалификаций и перечня должностей и профессий.

В соответствии с этими документами переоснащения материально-технического обеспечения вузов продолжается через процесс модернизации современных учебно-лабораторных и испытательно-диагностических баз.

В области кадрового обеспечения на текущий момент средний показатель укомплектованности штатным профессорско-преподавательским составом в вузах Сибирского и Дальневосточного регионов составляет 78,4%, а в 2012 г. этот показатель был равен 84,2%. Проблема обеспечения вузов молодыми кадрами стоит крайне остро, и одной из главных причин называют недостаточный уровень заработной платы современного преподавателя.

Новый формат государственных стандартов естественно повлёк за собой переработку существующих комплексов учебно-методических материалов (далее УМК), которые были разработаны для государственных стандартов второго поколения.

Процент базовых дисциплин, для которых разработаны в данный момент новые материалы для формата ФГОС-3 в среднем по вузам СФО и ДФО достиг 73%. Но вопрос совершенствования учебно-методического обеспечения, ориентированного на компетентностный подход с использованием инновационных технологий, оказался весьма трудным и спорным. Он явно требует дополнительного обсуждения. Так, как, по мнению многих представителей вузов, созданные пособия для формата ГОС-2 в реальности можно считать приемлемыми для формата ФГОС-3, однако требуется их существенная модернизация и обновление.

Ещё одним важным фактором успешной организации учебного процесса в вузах является обеспеченность учебно-методическими комплексами в электронном виде, представленными как в сети Internet, так и в локальной сети вузов. Процент учебно-методических пособий

оформленных как электронный ресурс в среднем составил – 67,1%. На рисунке 2 приведена диаграмма, отображающая соотношения переработанных УМК в формате ФГОС-3 и используемых УМК формата ГОС-2 для вузов СФО и ДФО, а так же соответствующие представления материалов в электронном виде.

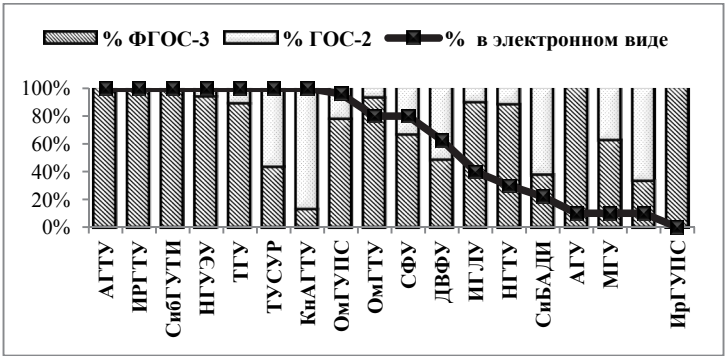

Рис. 2. Диаграмма соотношения используемых УМК двух форматов и наличия электронных вариантов в нормализованном виде

Безусловно, ответственность за достоверность представленных данных несут сами вузы.

Седьмым пунктом решения Пятого пленума СибРОУМО была обозначена задача издания учебников и учебных пособий по дисциплинам основных образовательных программ для группы специальностей в области информационной безопасности. В приложении представлены результаты мониторинга вузов Сибири и Дальнего Востока и описан перечень дисциплин ФГОС-3 поколения, для которых вузы в настоящее время разрабатывают базовые учебники, а так же выделены предметы, для которых пока учебники отсутствуют.

Идея создания банка учебно-методических материалов для дисциплин направления информационной безопасности так же неоднократно озвучивалась на прошедших пленумах СибРОУМО. Перечень пособий, изданных преподавателями вузов наших регионов, в настоящее время содержит 135 наименований. А конечным итогом данной работы на долгосрочный период времени должна стать сформированная база учебно-методических материалов, доступная всем преподавателям нашего сообщества, как в текстовом, так и в электронном видах.

За три последних года членами аттестационной комиссии СибРОУМО проведены экспертизы учебников и учебно-методических пособий и выданы 14 рекомендаций о присвоения грифа СибРОУМО вузов по образованию в области информационной безопасности.

Организация обучения студентов естественным образом предполагает развитие всевозможных видов контроля обучения как внутри вуза, так и государственную проверку через аккредитацию, аттестацию и лицензирования образовательных программ учебных заведений. При содействии членов СибРОУМО в качестве экспертов Росаккредагенства МОН в 2012 г. успешно прошли аккредитацию 6 вузов, а в 2013 г. – 8 вузов Сибири и Дальнего Востока.

Далее приведём статистические показатели набора студентов на все специальности и профили бакалавриата для направления «Информационная безопасность» в сибирском и дальневосточном регионах начиная с 2011 г. по 2014 г.

4.2. Бакалавриат. За прошедшие три года на профили бакалавриата ФГОС-3 поколения в регионе Сибири и Дальнего востока было принято1078 студентов, из которых на платной основе полного возмещения затрат (далее ПВЗ) обучается 195 человек, то есть 18% студентов (рисунок 3).

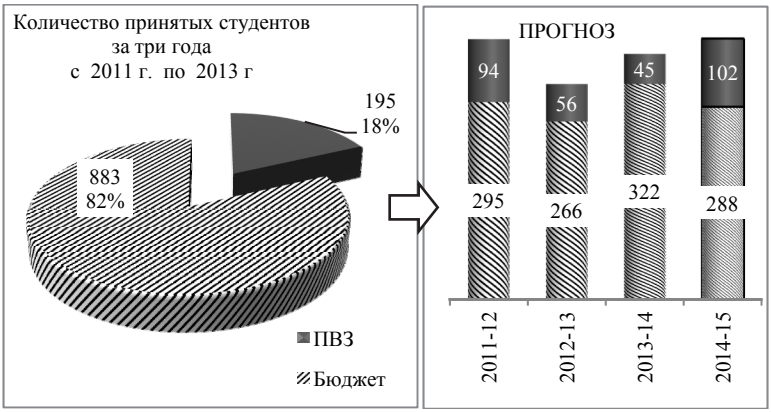

Рис. 3. Диаграммы, отражающие абсолютные и долевые отношения набора на профили бакалавриата в вузах СФО и ДФО за три года (2011–2013 гг.) и прогноз на 2014/15 учебный год

В планах на 2014/15 учебный год, количество студентов должно пополниться приблизительно на 390 человек.

4.3. Специалитет. Общее количество принятых студентов на специальности направления за период с 2011 по 2013 годы составило 1253 студента, из них 31% на платной основе. Приведённые ниже четыре диаграммы (рисунки 4–6) отражают характеристики распределения набора студентов по специальностям, а так же соотношение платного и бюджетного обучения за три прошедших учебных года с прогнозом на будущий 2014/15 учебный год.

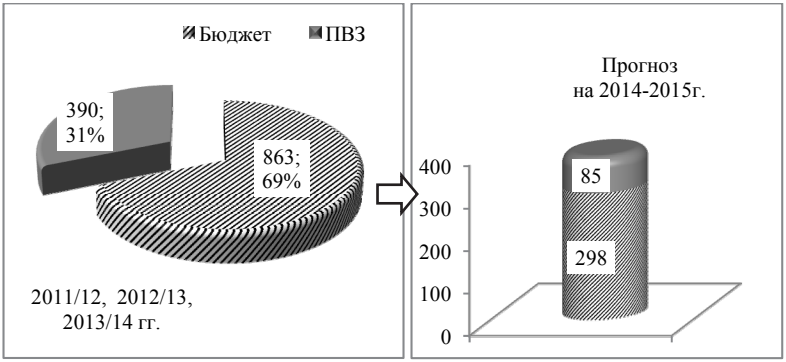

Рис. 4. Диаграммы, отражающие абсолютные и долевые отношения набора на специальности в вузах СФО и ДФО за три года (2011–2013 гг.) и прогноз на 2014/15 учебный год

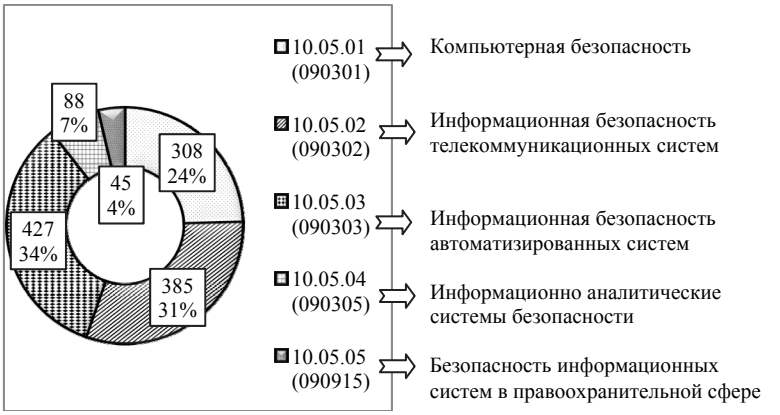

Рис. 5. Диаграмма распределения набора по специальностям направления информационной безопасности за период 2011–2013 гг.

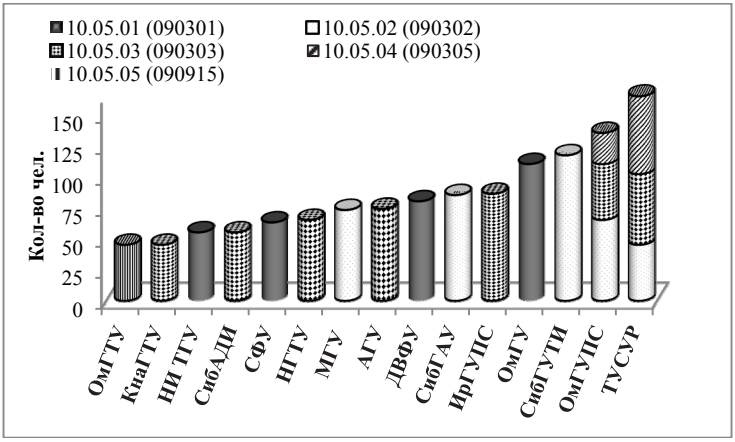

Рис. 6. Качественная картина набора студентов на специальности за три учебных года (2011–2013) по вузам СФО и ДФО

Гистограмма на рисунке 6 описывает общую качественную картину набора на специальности за прошедший период с 2011 по 2013 годы по вузам Сибири и Дальнего востока.

4.4. Магистратура. Количество студентов, поступавших в магистратуру за предыдущие три года, достигло 50 человек. Стоит отметить, что пока наборы в магистратуру в сибирский и дальневосточный регионы осуществляют только два вуза: АГУ и ОмГТУ и эти два вуза запланировали принять ещё 14 человек на следующий учебный год.

Однако ряд вузов нашего региона уже в ближайшее время также намерены получить лицензии для обучения студентов в магистратуре: АлтГТУ, ДВФУ, ОмГУ, СГГА, ИГЛУ, ИрГУПС и ТУСУР. К сожалению, в Росакредагенстве менялись правила лицензирования магистратуры, что привело к неоднократной отправке материалов вузами.

Организация обучения студентов предполагает непрерывное совершенствование всех параметров системы для подготовки, востребованных рынком труда профессионально квалифицированных специалистов в области информационной безопасности.

К характерным показателям этого процесса относится показатель востребованности выпускников на рынке труда. Выпускники направления информационная безопасность практически востребованы на 99,4%. Из 1552 выпущенных за три года специалистов, не заявлены были только 10 и в основном по причине

призыва в ряды Вооружённых сил РФ. В этом году рынок труда пополнят ещё 366 выпускников.

Распределение выпускников по секторам экономики, а также динамика его показателей по годам с 2011 по 2014 гг. представлено на рисунке 7.

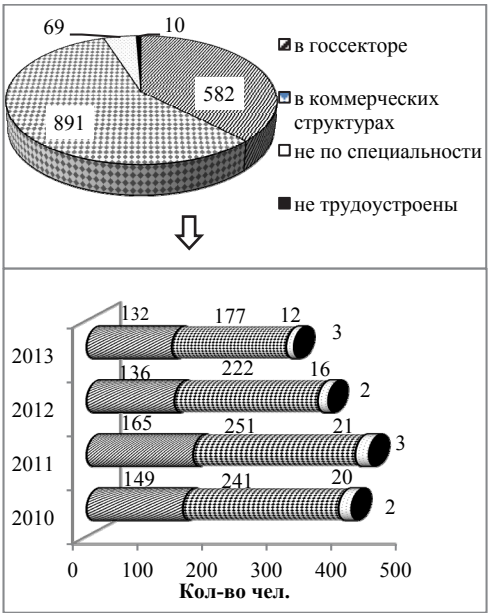

Рис. 7. Динамика распределения выпускников по секторам экономики

Обсуждая вопросы подготовки студентов невозможно не отметить такие позитивные достижения, как участие и победы на всевозможных внутренних, областных, региональных, а так же Всероссийских конкурсах.

Традиционно каждый год в апреле силами членов СибРОУМО и Института системной интеграции и безопасности (далее ИСИБ) организуется Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности «SIBINFO». Ниже (таблица 1) представлены города и вузы, представители которых явились победителями среди 16 городов и 18 вузов России за 2013–2014 годы.

Таблица 1. Победители конкурса-конференции студентов и аспирантов по информационной безопасности «SIBINFO»

Город	Вуз	Год
Барнаул	Алтайский государственный университет	2013
Владивосток	Морской государственный университет им. адм. Г.И. Невельского	2014
Красноярск	Сибирский государственный аэрокосмический университет им. акад. М.Ф. Решетнева	2014
Москва	Национальный исследовательский университет «МИЭТ»	2013
Новосибирск	Новосибирский государственный университет экономики и управления.	2013, 2014
Омск	Омский государственный технический университет	2014
Орёл	Академия ФСО России	2014
Самара	Поволжский государственный университет телекоммуникаций и информатики	2014
Томск	Томский государственный университет систем управления и радиоэлектроники.	2013, 2014
Уфа	Уфимский государственный авиационный технический университет	2013, 2014

Лауреатами престижной премии ежегодно проводимого Всероссийского конкурса «Инфофорум – Новое поколение» неизменно становятся вузы СФО и ДВФО. Ниже (таблица 2) приведены вузы – победители.

Таблица 2. Лауреаты премии Всероссийского конкурса «Инфофорум – Новое поколение»

Город	Вуз	Год
Барнаул	Алтайский государственный университет	2014
Владивосток	Морской государственный университет им. адм. Г.И. Невельского	2013
Владивосток	Дальневосточный федеральный университет	2014
Комсомольск на Амуре	Комсомольский-на-Амуре государственный технический университет»	2013
Красноярск	Сибирский государственный аэрокосмический университет им. акад. М.Ф. Решетнева	2014
Новосибирск	Сибирский государственный университет телекоммуникаций и информатики	2013
Новосибирск	Новосибирский государственный технический университет	2014
Томск	Томский государственный университет систем управления и радиоэлектроники	2013, 2014
Тюмень	Тюменский государственный университет	2013

Кроме того, за эти два года дважды был отмечен Сибирский государственный аэрокосмический университет им. акад. М.Ф. Решетнева, представители которого победили в двух номинациях: «Преподаватель года» (2013 г.) и «Молодой специалист года» (2014 г.).

Лауреатом премии в номинации «Образовательный центр года» в 2014 году за вклад в подготовку специалистов в области информационной безопасности стал Институт системной интеграции и безопасности (ИСИБ) ТУСУР**.**

4.5. Аспирантура. Следующую ступеньку непрерывного процесса повышения квалификации в области информационной безопасности занимает аспирантура. За период с 2012 года кандидатские диссертации по направлению информационной безопасности защитили 20 человек и на текущий момент в аспирантуре обучаются ещё 80 аспирантов.

4.6. Повышение квалификации и переподготовка кадров. Замыкает цепочку концепции непрерывного образования курсы повышение квалификации и переподготовка кадров.

«Выступая на Гайдаровском форуме, премьер-министр РФ Дмитрий Медведев поставил задачу добиться увеличения доли работников среднего и старшего возрастов, прошедших переподготовку с существующих 10% до 37% к 2015 г. Председатель Правительства РФ подчеркнул, что во всём мире в настоящее время инвестиции в знания растут быстрее, чем вложения в основные фонды. «Динамика прогресса такова, что принцип «одна жизнь – один диплом» очень быстро устаревает. Практически невозможно себе представить, что, получив образование в 22 года, можно всю жизнь использовать навыки, обретённые на студенческой скамье».

Перечень образовательных учреждений, реализующих дополнительные профессиональные образовательные программы в области информационной безопасности, согласованные с Федеральной службой по техническому и экспортному контролю насчитывает 11 вузов Сибири и Дальнего Востока: ДвГУПС, ДФУ, ИрГУПС, НГТУ, НГУЭУ «НИНХ», ОГТУ, ОГУ, СибГАУ, СибГТУ, СФУ, ТУСУР.

Что касается СибРОУМО, то совместно с сотрудниками ИСИБ ТУСУР только за 2013 г. на курсах повышения квалификации «Защита конфиденциальной информации в организации (персональные данные – 72 ч)» прошли подготовку 56 человек, причём география слушателей распространялась на регионы Сибири, Дальнего Востока и центральные области России. На начало 2014 г. повышение

квалификации уже осуществило 6 человек и отдельно для структуры Пенсионного фонда (ПФР) – 20 человек.

В начале 2014 г. так же успели получить сертификаты 8 человек на курсах профессиональной переподготовки «Информационная безопасность» – 504 часа.

Необходимость непрерывного образования диктуется, прежде всего, непрекращающимся развитием самого общества, постоянным обновлением учебных планов и программ, совершенствованием технических средств обучения, изданием новых учебников и пособий, появлением новых педагогических технологий, способствующих повышению профессиональной компетентности всех участников этого процесса.

СибРОУМО вузов России по образованию в области информационной безопасности будет продолжать намеченный курс на координацию деятельности высших и средних учебных заведений в научном, учебном и учебно-методологическом обеспечении регионов СФО и ДФО для поддержания качественной и эффективной системы непрерывной подготовки и переподготовки кадров.

5. Заключение. По результатам проведенного исследования, описанного в данной статье, можно сделать следующие выводы:

– предложенная концепция развития информационной безопасности Российской Федерации является частью концепции национальной безопасности;

– определена необходимость обеспечения защиты информации в органах государственных власти и способы ее реализации;

– рассмотрены и сформулированы требования по обеспечению подготовки кадров.

Как следствие достигнута поставленная цель. Полученные результаты могут быть использованы в органах государственной власти, местного самоуправления и профильных организациях.

Литература

1. *Мещеряков Р.В., Шелупанов А.А., Белов Е.В., Лось В.П.* Основы информационной безопасности // М.: Горячая линия – Телеком. 2004. 540 с.
2. *Волокитин А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А.* Информационная безопасность государственных организаций и коммерческих фирм. Справочное пособие (под общей редакцией Реймана Л.Д.) // М.: НТЦ "ФИОРД-ИНФО". 2002. 272 с.
3. *Юсупов Р.М.* О влиянии информационно-коммуникационных технологий на обеспечение национальной безопасности в условиях формирования информационного общества // Труды СПИИРАН. 2009. № 8. С. 21–33.
4. *Юсупов Р.М., Шишкин В.М.* О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН. 2008. № 6. С. 11–23.

5. *Авсентьев О.С., Александров В.С., Мещеряков Р.В., Рябин Г.И., Скрыль К.С.* Принципы моделирования механизмов воздействия вредоносных программы на защищенные информационные системы в интересах оценки угроз их безопасности // Доклады ТУСУР. 2008. № 2(18). С. 135–136.
6. *Скрыль С.В., Мещеряков Р.В., Белов Е.Б.* Структурирование описания противоправных действий в сфере компьютерной информации как методологическая основа их криминалистического исследования // Доклады ТУСУР. 2008. № 2(18). С. 132–135.
7. *Юсупов Р.М., Шульц В.Л.* Национальная безопасность и наука // Труды СПИИРАН. 2009 № 10. С. 11–32.
8. *Галин Р.Р., Мещеряков Р.В.* Методика оценки качества государственных услуг в сфере молодёжной политики // Качество. Инновации. Образование. 2013. № 10. С. 61–65.
9. *Сабанов А.Г., Мещеряков Р.В., Шелупанов А.А.* Требования к системам аутентификации по уровням строгости // Ползуновский вестник. 2012. № 2-1. С. 61–67.
10. *Савчук М.В., Мещеряков Р.В., Ходашинский И.А., Горбунов И.В.* Технология усиленной аутентификации пользователей информационных процессов // Доклады ТУСУР. 2012г. № 2 (34). Ч. 3. С. 236–248.
11. *Исхаков А.Ю., Мещеряков Р.В., Ходашинский И.А.* Двухфакторная аутентификация на основе программного токена // Вопросы защиты информации. 2013. № 3(102). С. 23–27.
12. Специальная техника и информационная безопасность / Под ред. В.И. Кирина // М.: Академия управления МВД. 2000. 83 с.
13. *Юсупов Р.М., Ронжин А.Л.* От умных приборов к интеллектуальному пространству // Вестник Российской академии наук. 2010. Т. 80. № 1. С. 45–51.

References

1. Meshcheryakov R. V., Shelupanov A.A., Belov E.B., Los V.P. *Osnovy informacionnoj bezopasnosti* [Base of Information security]. Moscow: Goryachaya linia – Telecom. 2004. 540 p. (In Russ.).
2. Volokitin A.V., Manoshkin A.P., Soldatenkov A.V., Petrov Yu.A. *Informacionnaja bezopasnost' gosudarstvennyh organizacij i kommercheskih firm. Spravochnoe posobie (pod obshhej redakciej Rejmana L.D.)* [Information security of government agencies and commercial firms. Handbook (edited by L.D. Reiman)]. M.: NTC "FIORD-INFO", 2002. 272 p. (In Russ.).
3. Yausupov R.M. [On the impact of information and communication technologies to ensure national security in the context of the information society]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2009. no. 8. pp 21–33. (In Russ.).
4. Yausupov R.M., Shishkin V.M. [Some contradictions in addressing information security]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2008. no. 6. pp. 11–23. (In Russ.).
5. Avsentev O.S., Aleksandrov V.S., Meshcheryakov R.V., Sorbs G.I., Skril K.S. [Principles of modeling of mechanisms of malicious programs on the protected information systems for assessing threats to their security]. *Doklady TUSUR – Reports of TUSUR*. 2008. no. 2(18). pp. 135–136. (In Russ.).
6. Skril S.V., Meshcheryakov R.V., Belov E.B. [Structuring of describing illegal actions in the computer information as a methodological basis of forensic research]. *Doklady TUSUR – Reports of TUSUR*. 2008. no. 2(18). pp. 132–135. (In Russ.).
7. Yausupov R.M., Shultch V.L. [National security and science]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2009. no. 10. pp. 11–32. (In Russ.).
8. Galin R.R., Meshcheryakov R.V. [Methods of assessing the quality of public services in the field of youth policy]. *Kachestvo. Innovacii. Obrazovanie – Quality. Innovation. Education*. 2013. no. 10. pp. 61–65. (In Russ.).

9. Sabanov A.G., Meshcheryakov R.V., Shelupanov A.A. [Requirements for systems of authentication by levels of severity]. *Polzunovskij vestnik – Polzunovsky Bulletin*. 2012. no. 2-1. pp. 61–67. (In Russ.).
10. Savchuk M.V., Meshcheryakov R.V., Khodashinsky I.A., Gorbunov I.V. [Technology enhanced user authentication information processes]. *TUSUR – Reports of TUSUR*. 2012. no. 2(34). part 3. pp. 236–248. (In Russ.).
11. Ishakov A.Yu., Meshcheryakov R.V., Khodashinsky I.A. [Two-factor authentication is based on the software token]. *Voprosy zashhity informacii – Information security*. 2013. no. 3 (102). pp. 23–27. (In Russ.).
12. *Special'naja tehnika i informacionnaja bezopasnost'* [Special equipment and information security]. edited by V.I. Kirin. M.: Akademija upravlenija MVD. 2000. 783 p. (In Russ.).
13. Yusupov R.M., Ronzhin A.L. [From smart devices to intelligent space]. *Vestnik Rossijskoj akademii nauk – Bulletin of the Russian Academy of Sciences*. 2010. vol. 80. no. 1. pp 45–51. (In Russ.).

Мещеряков Роман Валерьевич — д-р техн. наук, профессор, кафедра комплексной информационной безопасности электронно-вычислительных систем Томского государственного университета систем управления и радиоэлектроники (ТУСУР). Область научных интересов: системный анализ, анализ и синтез речи, информационная безопасность, вопросы обработки информации в интеллектуальных системах, особое внимание уделяется вопросам создания информационно-безопасных систем. Число научных публикаций — 247. mrv@security.tomsk.ru; 634050, г. Томск, пр. Ленина, 40, ауд. 210; р.т. +7 (3822) 900-111, факс +7 (3822) 900-111.

Meshcheryakov Roman Valerievich — Ph.D., Dr. Sci., professor, Dept. of Complex Security of Electronic-computing Systems of Tomsk State University of Control Systems and Radioelectronics (TUSUR). Research interests: speech analysis, speech recognition, medical technology, information security. The number of publications — 247, mrv@security.tomsk.ru; KIBEVS Dept., TUSUR, 40, Lenin-avenue Tomsk, 634050, Russia; office phone +7(3822)413-426, fax +7(3822)900-111.

Шелупанов Александр Александрович — д-р техн. наук, профессор, проректор по научной работе Томского государственного университета систем управления и радиоэлектроники (ТУСУР), директор института системной интеграции и безопасности ТУСУР. Область научных интересов: информационная безопасность, математическое моделирование. Число научных публикаций — 314. saa@tusur.ru; 634050, г. Томск, пр. Ленина, 40, ауд. 216; р.т. +7 (3822) 900-111, факс +7 (3822) 900-111.

Shelupanov Alexander Alexandrovich — Ph.D., Dr. Sci., professor, vice-rector on Science of Tomsk State University of Control Systems and Radioelectronics (TUSUR), Chief of System integration and Security. Research interests: information security, mathematical modelling. The number of publications — 314, saa@tusur.ru; ISIB. TUSUR, 40, Lenin-avenue Tomsk, 634050, Russia; office phone +7(3822)413-426, fax +7(3822)900-111.

Благодарности. Авторы благодарят сотрудников Института системной интеграции и безопасности ТУСУР и Сибирского регионального отделения учебно-методического объединения вузов России по образованию в области информационной безопасности за сотрудничество.

Acknowledgments. The authors thank the staff of the Institute of System Integration and Security TUSUR and Siberian regional department of educational and methodical association of universities in Russia Education in information security for your cooperation.

РЕФЕРАТ

Мещеряков Р.В., Шелупанов А.А. **Концептуальные вопросы информационной безопасности региона и подготовки кадров.**

Статья посвящена исследованию концептуальных вопросов обеспечения информационной безопасности. Предлагаются подходы к формированию функций защиты и обеспечению требуемого уровня информационной безопасности на федеральном и региональном уровнях. В статье сформулирована проблема повышения качества обеспечения деятельности различных структурных подразделений по защите информации при обеспечении функционирования системы обеспечения национальной безопасности.

В статье приводятся общие сведения по основным положениям государственной политики обеспечения информационной безопасности в социальной, общеполитической и экономической сферах. Приводится перечень мероприятий, необходимых для первоочередного выполнения на объектах информатизации и обеспечивающих требуемый уровень защиты информации. Рассматривается система подготовки кадров на региональном уровне. Приводятся основные сведения по учебному, методическому и научному потенциалу Сибирского и Дальневосточного Федеральных округов Российской Федерации.

В результате, в данной работе описана структура системы обеспечения информационной безопасности на региональном уровне, являющейся частью системы обеспечения национальной безопасностью. Описанные требования и мероприятия представляют собой комплексное решение проблем информационной безопасности.

SUMMARY

Meshcheryakov R.V., Shelupanov A.A. **Conceptual issues of information security of the region and training.**

The article discusses the conceptual issues that determine the state of information security of the state and region. An approach to building security features and functions of state security at the regional level. Describes the various requirements to ensure the required level of information security. Provides information on training in the field of information security in the Siberian and Far Eastern Federal Districts.

The article investigates the conceptual issues of information security. The approaches to the formation and protection functions to ensure the required level of information security at federal and regional levels. In the article the problem of improving the quality assurance activities of various departments for the protection of information while ensuring the functioning of the national security system. The article provides an overview of the main provisions of the state information security policy and other information to ensure information security policy in social, general political and economic spheres. A list of activities required to run on the primary objects of information and ensure the required level of security. Following is the training system at the regional level. Provides basic information on educational, methodical and scientific potential of the Siberian and Far Eastern Federal Districts of the Russian Federation.

As a result, this paper describes the structure of the information security at the regional level, which is part of the national security system. Described requirements and measures provide a comprehensive solution to the problems of information security.