Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ И ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОСОБЕННОСТИ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.Н. КАСАНИН, В.А. ФИЛИПОВИЧ

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»

Требования, предъявляемые работодателями к специалисту в области информационной безопасности, достаточно обширны, нужны кадры нового поколения, способные быстро адаптироваться к постоянно изменяющимся угрозам информационной безопасности, обладающие высоким уровнем профессиональной компетентности. В условиях постоянно меняющейся ситуации информационных угроз, стали востребованы новые знания и умения в сфере информационной безопасности.

Указ Президента Республики Беларусь от 09.11.2010 № 57 «Об утверждении Концепции национальной безопасности Республики Беларусь» выделяет следующие угрозы:

деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;

недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;

снижение научно-технологического и образовательного потенциала до уровня, не способного обеспечить инновационное развитие;

снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента

нарушение функционирования критически важных объектов информатизации;

утрата либо разглашение сведений, составляющих охраняемую законодательством тайну и способных причинить ущерб национальной безопасности

Основные индикаторы (показатели) состояния национальной безопасности:

уровень обеспеченности ресурсами здравоохранения, образования;

уровень развития информационных технологий и телекоммуникаций.

Подготовку специалистов первой ступени высшего образования по направлению образования 98 «Информационная безопасность» по специальности 98 01 «Защита информации» осуществляют:

Белорусский государственный университет;

Белорусский государственный университет информатики и радиоэлектроники;

Белорусский государственный технологический университет;

Витебский государственный университет имени П. М. Машерова;

Полоцкий государственный университет;

Гродненский государственный университет имени Янки Купалы.

Дополнительное образование (переподготовка) проводится по специальности 1-98 01 71 «Математическое обеспечение компьютерной безопасности» – Белорусский государственный технологический университет.

98 80 «Научная и педагогическая деятельность».

98 81 «Инновационная деятельность (с углубленной подготовкой специалистов)» – не ведется.

Несмотря на определенные успехи в образовательной политике, проблема нехватки высококвалифицированных специалистов остается весьма острой.

Поэтому и в дальнейшем необходимо уделять пристальное внимание вопросам образования в сфере безопасности информационных технологий. Надо отметить, что индустрия информационной безопасности формируется в значительной мере частными предприятиями, и качество их работ и услуг непосредственно влияет на состояние защищенности нашей информационной сферы.

Принимая во внимание данный фактор, в нашем законодательстве введено требование к организациям-лицензиатам Оперативно-аналитического центра о необходимости наличия у них соответствующего количества специалистов со специальным образованием в сфере информационной безопасности.

Процессы формирования специалиста, его компетентности, достаточно трудоемки и растянуты во времени.

Классическая схема подготовки специалистов давала неплохие результаты только в зрелых отраслях с установившимися технологическими процессами.

Для инновационных отраслей, к которым относится отрасль информационных технологий, в том числе, и одно из ее наиболее динамично развивающихся направлений защита информации, такая схема формирования компетентности специалистов становится неприемлемой.

В инновационных отраслях знания устаревают очень быстро и часто конкретные знания по специальности, полученные в учебном заведении, оказываются ненужными, поскольку технологии ушли вперед.

В настоящее время наблюдается диспропорция в подготовке кадров для защиты государственных секретов.

В ВУЗах Республики Беларусь осуществляется подготовка специалистов по защите информации в телекоммуникациях, по расследованию компьютерных преступлений, с изложением основ теории защиты информации и т.д.

Понятно, что досконально изучить вопросы, связанные с технической защитой информации, не представляется возможным.

Один из подходов организации эффективного повышения квалификации является привлечение высококвалифицированных специалистов по защите информации.

Однако, в настоящее время, они практически не знакомы с особенностями учебных программ.

Подготовка по второй ступени высшего образования:

В соответствии с постановлением Совета Министров Республики Беларусь от 24.06.2011 г. № 807 «Об утверждении перечня специальностей, по которым не допускается получение образования в вечерней, заочной формах получения образования, и признании утратившими силу некоторых постановлений Совета Министров Республики Беларусь» обучение в магистратуре по 98 направлению образования «Информационная безопасность» невозможно в заочной форме получения образования (таблица 1).

Это является сдерживающим фактором для продолжения обучения выпускников первой ступени высшего образования, которые распределяются для работы в организациях Республики Беларусь.

Кроме того, поступление в магистратуру лиц, уже имеющих рабочее место и желающих получить степень магистра, также является невозможным.

Проблемы подготовки кадров в области информационной безопасности:

низкий уровень довузовской подготовки будущих специалистов по информационной безопасности, школьный курс информатики касается только вопросов антивирусной защиты компьютеров и некоторых вопросов правовых норм в отношении защиты информации;

отсутствует продуманная система отбора абитуриентов, которая должна учитывать не только математическую подготовку, но и моральные, и психологические качества в сфере защиты информации;

отсутствуют профессиональные стандарты для всех видов деятельности специалистов информационной безопасности;

недостаточное МТО занятий по профессиональному циклу;

квалификационный уровень ППС, не всегда соответствует необходимому уровню;

научно-исследовательская деятельность по информационной безопасности в вузах в настоящее время проводится недостаточно активно.

Таблица 1 – Перечень специальностей, по которым не допускается получение образования в вечерней, заочной формах получения образования по 98 направлению

Код	Наименование профиля и направления образования, специальности, направления специальностей	Форма получения образования, по которой не допускается подготовка специалистов
98	Информационная безопасность	
98 01	Защита информации	
98 01 01	Компьютерная безопасность (по направлениям)	Заочная, вечерняя
98 80	Научная и педагогическая деятельность	
98 80 01	Методы и системы защиты информации, информационная безопасность	заочная
98 80 02	Аппаратное и программно-техническое обеспечение информационной безопасности	заочная

Решение проблем кадрового обеспечения информационной безопасности потребует:

разработки общеметодологических основ кадрового обеспечения информационной безопасности, включающих разработку и исследование механизмов государственного регулирования подготовки кадров в области информационной безопасности,

анализ и обоснование предметной области подготовки кадров в области информационной безопасности как междисциплинарной отрасли научного знания,

исследование путей использования современных образовательных технологий в целях повышения эффективности распространения знаний в области обеспечения информационной безопасности,

формирование научного и учебно-методического обеспечения непрерывной подготовки кадров в области информационной безопасности;

создания системы организационного и нормативно-правового обеспечения подготовки кадров в области информационной безопасности;

создания системы технологического обеспечения подготовки кадров в области информационной безопасности, в том числе разработки методик, специальной и учебной литературы, формирования эффективных механизмов использования современных информационных технологий в образовательном процессе.

Принципы подготовки специалистов в области информационной безопасности:

активное взаимодействие с работодателями сферы ИБ, как при разработке содержательной части образовательных программ, так и выполнении совместных проектов, предоставлении своей производственной базы для реализации практических задач;

ориентация образовательного процесса на динамичные изменения профессиональной среды, синхронизацию с потребностями региона;

усиление внимания на изучении нормативно-законодательных документов, национальных и международных стандартов в сфере обеспечения информационной безопасности;

приобретение практических навыков использования средств защиты информации в условиях современных угроз информационной безопасности;

создание инновационной образовательной среды, способствующей формированию у студентов мотивирующей системы участия в инновационной деятельности;

развитие сотрудничества с научными центрами, привлечение специалистов из таких центров для проведения совместных исследований.

МЕТОДИКА ОПТИМИЗАЦИИ ПРОГРАММЫ АУДИТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.И. ЛИВШИЦ, А.В. НЕКЛЮДОВ

Университет ИТМО, г. Санкт-Петербур

В последнее время применение интегрированных систем менеджмента (ИСМ) привлекает внимание высшего руководства (лиц, принимающих решения – ЛПР). Наблюдаются практически единичные случаи, когда современные организации самой разной отраслевой принадлежности (нефтеперерабатывающие, приборостроительные, авиационные и оборонные) внедряют только одну систему менеджмента (СМ), напротив, сейчас, как правило, реализуются именно проекты ИСМ. Однако на данный момент остается важной проблемой обеспечение выполнения программы аудита в ИСМ – реализация в полном объеме комплекса проверок по различным стандартам ISO при существенном сокращении доступных ресурсов. В большей степени эта проблема характерна для обеспечения программы аудита ИСМ для проверок информационной безопасности (ИБ), поскольку негативные последствия инцидентов ИБ могут привести к существенному ущербу для организации, вплоть до прекращения деятельности. В то же время, постоянное совершенствование принципов управления и, в частности, переход к мышлению, основанному на рисках, обеспечивают повышение интереса к рациональному применению современных риск-ориентированных стандартов [1, 2]. Соответственно, представляет определенный интерес изучение существующих проблем при выполнении аудита ИСМ, а также поиск способов оптимизации программы аудита ИСМ, основанных на принципах непрерывной адаптации при поступлении данных в течение одного микроцикла PDCA (Plan-Do-Check-Act), т.е. одного элементарного цикла аудита. На основании практики выполнения аудитов ИСМ предлагается новая методика оптимизации программы аудита, которая позволит обеспечить более рациональное принятие решений для ЛПР в современной сложной экономической обстановке.

Как отмечалось ранее, для обеспечения стабильного развития современных организаций в условиях наличия рисков различного происхождения, представляется це-