ПРОБЛЕМЫ КАДРОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ ГОСТИНИЦАХ

Абдуллаева З.И.-старший преподаватель СамИЭС

Аннотация – В данном тезисе были рассмотрены проблемы, возникающие при обеспечении информационной безопасности в современных гостиницах. Также было рассмотрено решение проблем по подготовке кадров по информационной безопасности.

Ключевые слова: подготовка кадров, электронная коммерция ,современные гостиницы, информационная безопасность, компания, информационные услуги, обучение.

Annotation – In the given thesis the problems arising at maintenance of information safety in modern hotels have been considered. Also has been considered the decision of problems on a professional training on information safety .

Key Words: A professional training, electronic commerce, modern hotels, information safety, the company, information services, training.

Аннотация –Ушбу мақолада замонавий меҳмонхоналарда ахборот хафсизлигини таъминлаш жараёнида вужудга келадиган муаммолар кўриб чиқилган. Ҳамда хафсизлигини таъминлаш бўйича кадрлар тайёрлаш муаммоларни ечишни кўриб чиқилган.

Калит сўзлар: кадр тайёрлаш, электрон тижорат, замонавий

С начала 21-го века электронная коммерция ускоренными темпами проникла в различные сферы социально-экономической деятельности, в том числе это затронуло и гостиничный бизнес. Это постепенно стало образом жизни для всех современных гостиниц. На сегодняшний день приоритетным вопросом ведения электронной коммерции является обеспечение безопасности электронного документа и электронного документооборота. В связи с этим разработаны различные методы обеспечения безопасности обмена данными в электронной коммерции.

Актуальным становится вопрос подготовки кадров для обеспечения информационной безопасности в современных гостиницах.

В быстро меняющемся современном мире проблема информационной безопасности является одной из ключевых составляющих деятельности любого предприятия. Чем сложнее информационная система, тем труднее решить эти задачи.

В современных условиях информационная безопасность становится важнейшим базовым элементом всей системы национальной безопасности государства. Обусловлено это, прежде всего, быстро растущими технологическими возможностями современных информационных систем, которые по своему влиянию на политику, хозяйственно-экономическую жизнь, духовно-идеологическую сферу и умонастроения людей стали в настоящее время решающими и всеохватывающими.

Достаточно часто предприятия, закупив большое количество различных средств защиты, сталкиваются с целым рядом проблем. Дело в том, что они вынуждены решать комплексную и достаточно сложную задачу: защищаться от постоянно возрастающего числа угроз, одновременно с этим разворачивать закупленные средства обеспечения безопасности и управлять ими.

Самая главная проблема - нехватка квалифицированных специалистов в данной области и отсутствие у имеющихся ИТ-специалистов необходимых знаний и практического опыта по организации безопасности в условиях разнородной информационной среды, так как уже имеющиеся в штате сотрудники чаще всего перегружены и вынуждены одновременно решать и организационные, и технические задачи. Содержать штат сотрудников, которые в круглосуточном режиме будут заниматься мониторингом и отражением атак, может позволить себе далеко не каждая компания. Поэтому необходим непрерывный и последовательный мониторинг угроз, связанных с возможным развязыванием информационной войны, с постоянной и трезвой оценкой возможностей противодействия, нейтрализации и предотвращения этих угроз.

Сегодня, информационная сфера является одним из системообразующих факторов жизни государства, что определяет исключительную важность вопросов, связанных с формированием его информационной инфраструктуры, предполагающей интенсивное развитие систем телекоммуникаций и связи, различных информационных систем, технологий предоставления информационных услуг или, другими словами, индустрии информатизации.

Вместе с тем глобальная информатизация общества чрезвычайно обострила проблему обеспечения информационной безопасности государства, что определило необходимость разработки соответствующей государственной политики в этой области. Цели, задачи, принципы и основные направления обеспечения информационной безопасности, определяющие основы такой политики, изложены в нормативных документах информационной безопасности.

С целью сосредоточения усилий информационной безопасности, связанных с обеспечением национальной безопасности, разработаны перечни основных направлений и приоритетных проблем в области информационной безопасности.

Одним из приоритетных направлений является решение проблем кадрового обеспечения информационной безопасности.

Для решения проблем кадрового обеспечения информационной безопасности необходимо:

разработать общеметодологических основы 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;

совершенствовать систему организационного и нормативно-правового обеспечения подготовки кадров в области информационной безопасности;

создать систему 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.

На сегодняшний день высшие учебные заведения осуществляют подготовку кадров по информационной безопасности. ТУИТ определен головной организацией по научным проблемам обеспечения информационной безопасности, имеющим гуманитарный характер.

На наш взгляд ТУИТ обладает необходимым потенциалом, чтобы стать ведущей организацией в области проведения научных исследований и подготовки специалистов с высшим образованием по всему спектру проблем информационной безопасности.

Учитывая потребности в высококвалифицированных специалистах по информационной безопасности, необходимо продолжить работу по созданию в ТУИТ

системы образования в данной области. Эта система по сути своей является междисциплинарной, многоуровневой, поэтому при ее создании необходимо обеспечить выполнение следующих принципов:

Все виды и формы обучения должны вестись под единым методическим руководством.

Необходимо искать заказчиков и создавать условия для развития различных форм обучения, включая:

обучение по специальностям;

обучение по новым специализациям внутри имеющихся специальностей;

обучение по новым военно-учетным специальностям;

обучение в магистратуре по информационной безопасности;

различные формы дополнительного образования (курсы повышения квалификации, курсы переподготовки, дополнительная квалификация, второе высшее образование);

включение в учебный процесс различных факультетов блоков знаний по тем или иным аспектам информационной безопасности (с помощью специальных курсов, специальных семинаров, курсовых работ, дополнений к государственным стандартам образования и т.д.).

Общий принцип подготовки кадров в области информационной безопасности – это подготовка специалистов на базе фундаментального (университетского) образования, поскольку они в первую очередь должны быть специалистами в той или иной области, чтобы затем на базе профессиональных знаний получить дополнительное образование в сфере информационной безопасности.

Поэтому особое внимание должно быть уделено развитию магистратуры как формы и этапа обучения в вузах. Специалисты, которые требуются сегодня, должны иметь фундаментальное базовое образование, к которому дополнительно надо дать «надстройку» в виде специализации по информационной безопасности. Например, экономистам необходимо дополнительное образование по специальности «электронная экономика», которое в полном объеме сегодня нельзя получить в рамках существующих экономических специальностей, юристам необходима специализация в сфере правового обеспечения безопасности информационных и телекоммуникационных систем, в частности, в сфере компьютерной преступности, которая набирает темпы по всему миру по мере становления информационного общества. Такие специализации можно полноценно организовать, как представляется, на базе дополнительного образования (например, магистерского уровня).

Востребованность специалистов в области обеспечения информационной безопасности уже сегодня высока, а по мере вхождения Узбекистана в информационное общество, без сомнения, будет увеличиваться. Чтобы отвечать требованиям времени, необходимо продолжить развитие этой формы образования.

Итак, для решения проблемы кадрового обеспечения информационной безопасности в современных гостиницах мы предлагаем:

- разработку государственных образовательных стандартов по новым специальностям высшего профессионального образования;
- создать нормативно-правовую базу особого порядка лицензирования образовательной деятельности в области информационной безопасности;
- совершенствовать нормативную базу, направленной на сохранение интеллектуального потенциала государственных вузов, осуществляющих подготовку специалистов в области современных информационных технологий и информационной безопасности;
- разработать методику специальной и учебной литературы по специальностям в области информационной безопасности, включая разработку учебных пособий для подготовки специалистов в области криптографии.
- разработать методику специальной и учебной литературы по изучению общих вопросов информационной безопасности в специальностях, не отнесенных к группе «Информационная безопасность».

- разработать методику специальной и учебной литературы для курсов переподготовки и повышения квалификации кадров в области информационной безопасности.

Список литературы:

1. Барбара Гутман, Роберт Бэгвилл. Политика безопасности при работе в Интернете - техническое руководство.
2. В. Ф. Шаньгин. Информационная безопасность компьютерных систем и сетей. Москва ИД «ФОРУМ» - ИНФРА-М 2011
3. Бесплатно скачать Гафнер В.В. “Информационная безопасность” 2010 г.
4. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2012 г.