ДОКЛАД НА ТЕМУ:

«СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ПОДГОТОВКИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

д.э.н., профессор Сейдахметова Ф.С.

Алматинский гуманитарно- экономический университет

РЕСПУБЛИКА КАЗАХСТАН

АКТУАЛЬНОСТЬ ТЕМЫ

Масштабное внедрение «цифровизации», повсеместная информатизация, глобализация, рост конкуренции значительно совершенствовали современное общество, оказав влияние на экономику, политику и другие сферы жизнедеятельности.

Одновременно с этими процессами произошли коренные изменения в системе образования, поскольку ее перемещение в электронную среду актуализировало научные исследования информационной безопасности

В ПОСЛЕДНИЕ ГОДЫ В РК :

- формируются новые образовательные процессы и получают распространение непрерывное обучение в виде экспресс-курсов, мини семинаров, онлайн конференций, и т.п., Это свидетельствует об интеграции системы различных видов образования.
- возрастает потребность в специалистах, обладающих навыками управления рисками и быстрой адаптации в своей профессиональной деятельности к нестабильным ситуациям.

ПОНЯТИЕ VUCA

Происходящее в мире перемены объясняют такие термины как VUCA характеризующий эффективность деятельности в неустойчивой, сложной и агрессивной среде. Слово VUCA - акроним, (volatility, uncertainty, complexity, ambiguity — нестабильность, неопределён-ность, сложность и неоднозначность) объединяет четыре понятия, которые в полной мере раскрывают суть неподконтрольных человеку явлений современной эпохи. «Термин придумали в 1990-х годах американские военные, а сегодня он используется в бизнес-среде для обозначения условий, в которых работают компании»

СЛОЖИВШИЕСЯ В МИРЕ СИТУАЦИИ НЕОПРЕДЕЛЕННОСТИ:

1) показывают отсутствие заранее отработанных схем действий для человека, который не всегда понимает как вести себя в тех или иных условиях. Поэтому ему приходится оперативно менять мышление и искать новые подходы, так как «количество факторов, которые нужно сегодня принимать во внимание превышает емкость сознания».

2) распространяются продукты нанотехнолгий биотехнологий и других современных направлений науки и техники .

Эти обстоятельства требуют необходимости совершенствования современной образовательной деятельности. Развитие сети Internet обязывает к оперативной переработке больших объемов информации, многомерному анализу данных и формированию управленческих решений в условиях неопределенности и риска.

ПОЛУЧАЮТ РАСПРОСТРАНЕНИЕ НОВЫЕ СИСТЕМЫ ОБРАЗОВАНИЯ, ТАКИЕ КАК

«Smart-образование» (от слова «Smart», означающее «умный, продвинутый») основанное на идеях цифро-визации и информатизации.

Формируются Smart-университетоы , где среда обучения преоразуется в гибкую, актуализиро-ванную, интерактивную и персонифицированную»

Это наиболее рациональный способ организации сотрудничества преподавателей и студентов, главная цель которой сводится к формированию модели специалиста нового поколения, на базе единых стандартов .

МИНИСТР НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РК САЯСАТ НУРБЕК ЗАЯВИЛ:

Вузы перейдут к модели smart-университетов», которые предусматривают формирование цифрового профиля студента, т.е.

1. student life track,
2. развитие цифровых сервисов EdTech,
3. оптимизация процессов в соответствии с передовыми трендами цифровизации .

Иначе говоря, перед системой образования Казахстана возникают новые задачи, связанные с подготовкой человека к деятельности в виртуальном мире. Это обуславливает необходимость разработки новых методов защиты безопасности информации в целях противостоять попыткам манипулирования сознанием обучаемого.

ПОНЯТИЕ БЕЗОПАСНОСТЬ

Характеризуя безопасность в целом, можно подчеркнуть, что это необходимость защищенности от внешних и внутренних угроз, т.е. предотвращение причин и обстоятельств, порождающих риски. Существуют несколько классификаций этого понятия. К примеру, в Википедии «информационная безопасность (англ. *Information Security*, а также — англ. *InfoSec*) — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации» охватывающие конкретные типы информации, инструменты, используемые для защиты информации, и области, где информация нуждается в защите.

. АКТУАЛЬНОСТЬ ИЗУЧЕНИЯ ПРОБЛЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В СФЕРЕ БЕЗОПАСНОСТИ

Перевод значительного объема информационных ресурсов в электронный вид создают условия для возникновения все новых уязвимостей и угроз в обществе. Одной из важных является не только защита информации, но и *защита от информации.*

Задача защиты от информации, в свою очередь, подразделяется на две составляющие:

защита от информации технических средств и систем, и

защита различных людей, обучающихся и обучаемых.

Поэтому в состав защищаемого ресурса необходимо включать персонал, который занимается как обучением, так и преподаванием. Именно такие квалифицированные специалисты будут востребованы в ближайшие годы на казахстанском рынке труда.

В МИРОВОЙ СИСТЕМЕ ОБРАЗОВАНИЯ

Имеется различное количество программ, связанных с общими вопросами подготовки специалистов по информационной безопасности, в том числе в бизнес-структурах.

Большинство международных программ и стандартов подготовки специалистов в области информационной безопасности по многим направлениям, связанным с расследованием компьютерных инцидентов и безопасностью информационных технологий и свидетельствуют о ежегодной возрастающей потребности общества в специалистах данного профиля.

Анализ и обобщение интернет ресурсов, посвященных проблеме подготовки специалистов показал, что каждая страна имеет свои приоритеты образовательных программ в области информационной безопасности

В США ПРИ РАССМОТРЕНИИ ПРЕДМЕТНОЙ ОБЛАСТИ ПОДГОТОВКИ ОБУЧАЮЩИХСЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫДЕЛЯЮТ :

У БАКАЛАВРОВ - четыре укрупненных блока:

1. Информационная безопасность
2. Компьютерная безопасность
3. Расследование компьютерных инцидентов
4. Безопасность компьютерных сетей

У МАГИСТРОВ - помимо вышеперечисленных, выделяются еще два укрупненных блока:

1. Менеджмент информационной безопасности
2. Экономика информационной безопасности

ФРАНЦУЗСКАЯ ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

четко ориентируется на изучение вопросов, связанных с криптографией, сетевой безопасностью и аудитом информационных систем.

Среди особенностей французской школы подготовки специалистов по защите информации студентам дается серьезное математическое образование, необходимое для освоения математических аспектов криптологии и сетевой безопасности.

Это связано с тем, что во Франции активно формируются структуры по контролю граждан в киберпространстве с тенденцией на перехват сообщений во французских (и не только) линиях электронных коммуникаций.

В ДРУГИХ ЕВРОПЕЙСКИХ СТРАНАХ

В Германии особое внимание уделяется дисциплинам, связанным со сбором доказательств и расследованием инцидентов компьютерной безопасности, применением программно-аппаратной защиты информации, в том числе электронных ключей.

В Великобритании обращают внимание вопросам компьютерной экспертизы, а также различным аспектам обеспечения информационной безопасности в открытых бизнес-системах и электронной коммерции

Другими словами, многие программы в своем большинстве направлены на то, чтобы противостоять или защитить людей и организации от онлайн-угроз. Согласно отчету компании Accenture, в 80% крупных организаций всего мира расходы на кибербезопасность составляют 15% от общего бюджета, заложенного на информационные технологии.

ОСНОВНЫЕ ПОДХОДЫ К РЕШЕНИЮ ПРОБЛЕМЫ В РК:

1) изучение всех доступных средств коммуникаций системы образования, которые расширили бы возможности безопасности виртуального общения, имеющего свои правила и нормы.
2) развитие новых технологиий, которые в достаточной степени должны быть обеспечены нужным пакетом программ,
3) разработка единых стандартов программного обеспечения и компетенций при подготовке обучающихся , связанных с безопасностью информации
4) повышение требований к квалификации специалистов по обслуживанию технических устройств в этой сфере.

ПРОФЕССИЯ СПЕЦИАЛИСТА ПО КИБЕРБЕЗОПАСНОСТИ. ИМЕЕТ НЕСКОЛЬКО ОСНОВНЫХ НАПРАВЛЕНИЙ:

-*Специалист по реверс-инжинирингу.* Занимается детальным изучением кода с целью определения слабых мест системы и составления рекомендаций для усиления ее защиты.
- Форензик. Расследует уже совершенные киберпреступления. Обладает навыками, необходимыми для поиска следов проникновения, сбору улик, восстановлению хронологии событий и разоблачению хакерских группировок.
- Антифрод-аналитик. Наиболее востребован в компаниях финансового сектора. Контролирует безопасность проведения онлайн-транзакций. На основе дифференцированного анализа покупок и трат по картам отслеживает проведение подозрительных операций.
-*Пентестер.* С одобрения нанимателя пытается при помощи хакерских методов взломать систему с целью выявления уязвимостей информационной безопасности. Прежде чем настоящий преступник нанесет удар, пентестер устранит имеющиеся пробелы и защитит программное обеспечение
-*Баг-хантер.* Занимается выявлением и быстрым устранением сбоев в программном и аппаратном обеспечении. Как правило, его услуги требуются, когда первоначальный разработчик преднамеренно расставил «ловушки» в созданном продукте и исчез
-. *Этичный хакер.* Данная специальность схожа с предыдущей. Но кибервзломщик «в белой шляпе», как правило, действует самостоятельно и имеет больше свободы. Пентестеры же работают в команде и действуют в строгом соответствии с разработанным планом.
Востребованность всех перечисленных специальностей находится на очень высоком уровне.

ПРАВИЛЬНОЕ ФУНКЦИОНИРОВАНИЕ БЕЗОПАСНОСТИ РАЗЛИЧНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ВЫДВИГАЕТ:

- новые цели и перед «создателями» и «потребителями» этой информации;
- радикальные решения проблем подготовки кадров в системе безопасности информации;
- законодательное регулирование этой деятельности;
- необходимость обобщения международных научных достижений

Важно осознать, что будущее системы безопасности во многом будет способствовать прогрессивному развитию многих сфер жизнедеятельности общества

НА НАЧАЛЬНОМ ЭТАПЕ НЕОБХОДИМО:

1) провести комплексную оценку эффективности подготовки высококвалифицированных кадров в сфере информационной безопасности в мире;
2) проанализировать и сравнить достижения Казахстана с другими странами;
3) сформировать модель специалиста нового поколения которая должна быть построена с учетом международных достижений в образовательной деятельности;
4) адаптировать к казахстанской системе образования с учетом опыта университетов, осуществляющих подготовку специалистов в системе информационной безопасности.

НА СЛЕДУЮЩЕМ ЭТАПЕ РЕКОМЕНДУЕТСЯ:

- создание инновационной образовательной среды. предусматривающей активное взаимодействие различных систем образования;
- систематическое отслеживание динамичных изменений и ориентация образовательного процесса в вузовской среде на безопасность информации;
- осуществлять синхронизацию видов деятельности, связанных с защитой данных и снижение возникающих в процессе угроз и уязвимостей информации.

В ПРОЦЕССЕ ЭТОГО ЭТАПА НУЖНО:

- *Определить показатели, измеряющие эффективность работы системы информационной безопасности в РК.*
- Создать стандартизированную базу данных, охватывающую типовые программы обучения специалистов в области защиты информации, позволяющей проводить сравнения с другими странами.

К ЧИСЛУ ПОКАЗАТЕЛЕЙ МОЖНО ОТНЕСТИ:

1.Общее количество специалистов системы информационной безопасности в Казахстане и за рубежом;

2.Количество вузов, занятых подготовкой специалистов на международном уровне;

3. Потребность и расходы на подготовку квалифицированных кадров

4. Спрос и потребности в специалистах для страны в целом и каждого региона.

Перечень показателей можно расширять в зависимости от обоснования тех или иных критериев, которые характеризуют эту систему

К ВАЖНЫМ МЕТОДАМ В ПРОЦЕССЕ ИССЛЕДОВАНИЯ МОЖНО ОТНЕСТИ:

. 1. Методы сбора первичной информации, способы обработки данных. В качестве первичной информации могут быть выбраны материалы анонимного анкетирования различных категорий обучающихся

2. Методы передачи информации направленные на сотрудничество вузов, позволяющих обеспечить доступ к качественным, но менее дорогостоящим знаниям. Подобная практика реализована в межуниверситетской телеобразовательной программе КЕПРИКОН в 1990 г.,

3. Методы применения телекоммуникационных технологий по мультимедийным курсам на примере Открытого университета (OpenUniversity) в Лондоне (ВеликобританияНа основе этого опыта провести научные эксперименты и предложить методику эффективного и открытого взаимодействия преподавателей и обучающихся.

РЕЗУЛЬТАТОМ ИССЛЕДОВАНИЯ ДОЛЖНО СТАТЬ:

Раскрытие взаимосвязей между системой подготовки кадров в сфере информационной безопасности и ее эффективностью основанной на сравнительной оценке казахстанской модели специалиста со странами СНГ, Европы и Азии.

Рассмотрение *компетентностного и инновационного* подходов в разных странах, *Компетентностный подход* направлен на усиление практикориентированности образования, т.е. наличие разностороннего опыта и умений практически реализовать знания. Развитие *инновационной подхода* предусматривает фундаментализацию образования, т.е. реальное участие вуза в процессах модернизации экономики.

Поиск перспективных путей повышения эффективности образовательного процесса, направленного на дифференцирование вузов в международном пространстве,

.

БЛАГОДАРЮ ЗА ВНИМАНИЕ!