ТЕХНОЛОГИЯ СИТУАЦИОННОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ УЧЕБНОГО ПРОЦЕССА ВУЗА

Б.Ахметов

Казахский национальный университет имени аль-Фараби

Резюме: *рассматриваются вопросы ситуационного управления информационной безопасностью учебного процесса для повышения его качества.*

Ключевые слова: *Подготовка кадров, качество учебного процесса, информационная безопасность, ситуационное управление, ущерб знаний, технология ситуационного управления.*

Одними из основных компонент информационной образовательной среды вуза, влияющими на качество профессиональной подготовки специалистов, являются его материально-техническая база и используемое программное обеспечение. Своевременное проведение регламентных работ и списание морально устаревших компьютеров, регулярное обновление антивирусной базы, жесткое следование правилам парольной политики и т.д., или другими словами, соблюдение режима информационной безопасности приводит к устойчивой и надежной работе компьютеров и его программного обеспечения и, как следствие, к повышению качества учебного процесса. Игнорирование этого момента, наоборот, может привести к выходу из строя компьютеров, сбоям в работе программного обеспечения, фальсификации результатов обучения, необъективному оцениванию знаний студентов и т.д. [1].

Необходим высокотехнологичный инструмент управленческой деятельности, который позволяет наиболее полно и оперативно представлять информацию о сложившейся ситуации органам управления, прогнозировать возможные сценарии ее развития, оперативно подготавливать возможные альтернативные варианты управленческих решений и оценивать их последствия. Этим требованием в полной мере удовлетворяют ситуационные центры, которые интегрируют в одной организационно-функциональной структуре административно-управленческие, технические, телекоммуникационные, информационные и программные ресурсы для обеспечения оперативного, всестороннего, интеллектуального анализа обстановки и выработки качественных и адекватных решений по управлению сложными ситуациями [2].

Несмотря на актуальность создания ситуационных центров, мало исследованными остаются организационные и технологические аспекты их применения в вузах. Существующие ситуационные центры в основном предназначены для подготовки специалистов и обучения управленческих кадров ситуационному анализу с использованием интеллектуальных информационно-коммуникационных технологий.

В статье рассматриваются вопросы ситуационного управления информационной безопасностью учебного процесса с целью обеспечения его высокого качества.

Ситуационный центр управления информационной безопасностью, как организационная система, имеет глобальную цель своего существования, которую можно определить как обеспечение оперативного, интеллектуального анализа обстановки и выработки адекватных решений по управлению информационной безопасностью в различных сферах деятельности вуза. Для дальнейшей декомпозиции определимся с основными направлениями деятельности ситуационного центра. В качестве критерия при этом можно использовать естественное деление видов деятельности, характерных любому вузу, на:

1. учебный процесс;
2. контроль и измерение результатов обучения;
3. научно-исследовательскую работу;
4. внеучебную деятельность;
5. организационно-управленческую деятельность.

В соответствии с ними можно сформулировать следующие цели второго уровня. Например, для цели первого уровня оно может быть сформулировано следующим образом – обеспечение

оперативного, интеллектуального анализа обстановки и выработки адекватных решений по управлению информационной безопасностью учебного процесса**.**

Третий уровень дерева целей должен отражать требования основных систем, взаимодействующих с ситуационным центром. Очевидно, что структура этого уровня зависит от конкретного вуза, его системы менеджмента качества, в соответствии с которой в «Положении о ситуационном центре» отражаются все его взаимодействия по входящей и исходящей информации.

Например, в Казахском национальном университете имени аль-Фараби, для цели 2.1 основными взаимодействующими подсистемами являются:

- ученый совет;
- департамент учебно-методической работы;
- департамент информационных технологий;
- факультеты;
- кафедры;
- отдел разработки программного обеспечения;
- отдел программного сопровождения;
- отдел технического обслуживания.

Каждая из взаимодействующих подсистем предъявляет ряд требований к конечным продуктам системы. Эти требования можно отразить, декомпозируя соответствующие цели второго уровня. Полученное после полной декомпозиции всех уровней дерево целей представляет собой модель функционирования ситуационного центра – многоуровневого описания ее целей, иерархической системы управления и процесса функционирования [3].

Рассмотрим теперь вопросы влияния соблюдения режима информационной безопасности на качество учебного процесса.

Существующая в вузах технология обеспечения непрерывности процесса обучения в лабораториях вуза работает неэффективно. При выходе из строя компьютеров в классах технический персонал (операторы, лаборанты) подают соответствующую письменную заявку с указанием возможной причины в отдел технического обслуживания. Технический персонал мог бы сам попытаться устранить возникшую неисправность, однако это не входит в его функциональные обязанности. Более того, этих неисправностей, возможно, могло и не быть, при своевременном проведении техническим персоналом профилактических регламентных работ в компьютерных классах. Основной причиной такого отношения технического персонала к состоянию компьютерной техники является независимость их оплаты от числа работающих компьютеров и незаинтересованность в увеличении своей работы ввиду отсутствия поощрения за данный вид деятельности.

Необходимо использовать для сбора информации о состоянии компьютерных лабораторий профессорско-преподавательский состав, так как он напрямую заинтересован в надежно работающей компьютерной технике для обеспечения качественного учебного процесса. Такой подход используется в описываемой ниже технологии ситуационного управления информационной безопасностью учебного процесса (рис.1).

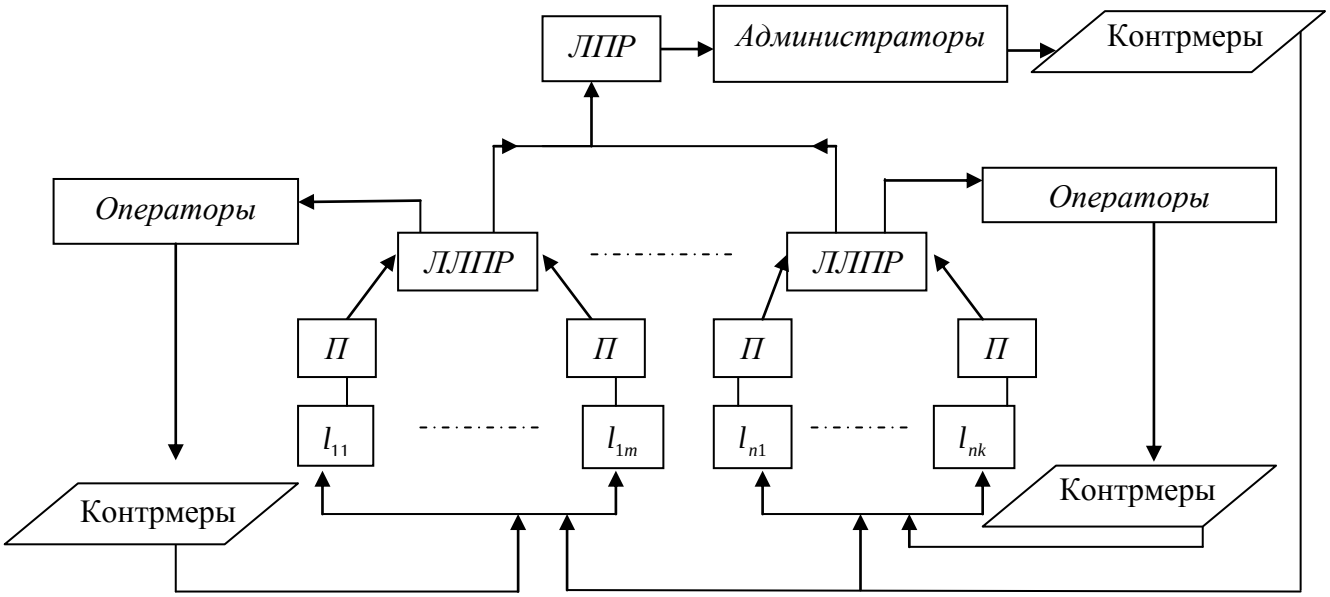

Рисунок 1 - Технология ситуационного управления информационной безопасностью

Здесь l и $П$ представляют собой подуровни компьютерных лабораторий и преподавателей, которые проводят занятия в этих лабораториях; *Операторы* – специалисты департамента информационных технологий, ответственные за состояние компьютерных лабораторий на факультете; *Администраторы* – специалисты департамента информационных технологий, ответственные за состояние компьютерных лабораторий в вузе.

С точки зрения организации оснащения вуза компьютерной техникой вуз представляет собой иерархическую структуру: факультеты, кафедры, лаборатории. Основываясь на такой структуре вуза целесообразно на каждом факультете иметь собственный локальный ситуационный центр с локальным лицом, принимающим решение (ЛЛПР), который осуществляет мониторинг состояния компьютерных лабораторий на факультете и принимает локальные решения. В его обязанности также входит передача данных в ситуационный центр вуза, который занимается накапливанием статистики о состоянии всего компьютерного парка вуза на основании информации от локальных ситуационных центров. Основываясь на этих данных ЛПР принимает решения по применению локальных или глобальных контрмер для устранения текущих неисправностей и предотвращения их появления в дальнейшем.

В общем случае технология ситуационного управления информационной безопасностью включает оперативный мониторинг состояния ресурсов (компьютеры, программное обеспечение, базы данных) в компьютерных классах за каждый академический час, расчет ущерба знаний студентов, анализ обстановки, принятие адекватных решений) и состоит из следующих этапов:

1. Преподаватели после каждого занятия в лаборатории вводят данные о состоянии компьютеров в программу «Security Client»;

2. Серверная программа «Security Server» собирает данные с клиентских программ и выводит на веб-страницу ЛПР ситуацию о состоянии компьютерных лабораторий и величину ущерба знаний студентов в них, на основании методики, описанной в [4].

3. ЛПР на основе анализа данных «Security Server» принимает решения о принятии контрмер в компьютерных лабораториях и определяет приоритеты их выполнения.

Библиография:

1. Ахметов Б. Качество дистанционного образования и проблемы информационной безопасности. – Материалы республиканского семинара по проблемам дистанционных технологий. – Шымкент:ЮКГУ им.М.Ауэзова, 2009. – С.60-62.
2. Филиппович А.Ю. Ситуационные центры: определения, структура и классификация. // PCWeek/RE N26(392), М., 15-21 июля 2003 г. с.21-22.
3. Ахметов Б.С., Ехлаков Ю.П., Силич М.П., Яворский В.В. Методология моделирования информационной образовательной среды вуза. – Алматы: Изд-во «LEM», 2008. - 336 с.
4. Ахметов Б. Информационная безопасность и его влияние на уровень знаний студентов// Вестник КазАТК имени М.Тынышпаева, 2009. – № 2. – С.153-158.