ТЕХНОЛОГИЯ СИТУАЦИОННОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ УЧЕБНОГО ПРОЦЕССА КАЗНУ ИМЕНИ АЛЬ-ФАРАБИ

Б.Б. Ахметов, У.А. Тукеев
КазНУ имени аль-Фараби
e-mail: 007berik@mail.ru

Влияние информационной безопасности на качество учебного процесса. 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].

Измерения влияния информационной безопасности на качество учебного процесса. Руководство вуза, как правило, не знакомо с потерями, который несет вуз в связи с неработающими компьютерами. Важно предоставить руководству аргумент на понятным им языке, коим менеджменте являются деньги, который бы характеризовал текущие потери по вузу от числа неработающих компьютеров. Модель ниже, позволяет количественно измерить ущерб и может служить обоснованием инвестиции в информационную безопасность вуза.

Введем понятие «коэффициента знаний» k_i для i-го лабораторного класса, который будет характеризовать текущую обеспеченность студентов на конкретном занятии работающими компьютерами. Предположим, что студент на каждом занятии усваивает одну единицу знаний, если у него есть отдельное рабочее место, иначе его «знание» будет уменьшаться в соответствии с «коэффициентом знаний» i-го лабораторного класса k_i. Формула для вычисления «коэффициента знаний» k_i для i-го лабораторного класса:

$$k_i = \begin{cases} l_i - g_i \geq 0, & k = 1 \\ l_i - g_i < 0, & k = \dfrac{l_i}{g_i} \end{cases} \qquad (1)$$

где g_i – число студентов в i-ой группе, l_i – количество работающих компьютеров в i-ой лаборатории.

Выведем формулу для расчета потерь по лабораторному классу l кафедры b факультета a в единицу времени:

$$S_{abl} = C_0 \cdot \sum_{t=1}^{KG} (1 - k_l) \cdot g_t \cdot q_{tl} \qquad (2)$$

где C_o – оплата студента за единицу времени обучения, KG – количество групп, обучившихся в единицу времени в лабораторном классе l, k_l – «коэффициент знаний» для l - го лабораторного класса, g_t – число студентов в группе t, q_{tl} – количество пройденных занятий в лаборатории l группой t за единицу времени.

Вычислим ущерб знаний для всех студентов по лабораторному классу при 5 работающих компьютеров в течение дня. В среднем на механико-математическом факультете в каждом лабораторном классе проводится по 10 занятий в день. Предположим, что в течение дня в данном лабораторном классе провели занятия три группы, состоящие из $g_1 = 10$, $g_2 = 11$ и $g_3 = 14$ студентов по $q_{11} = 3$, $q_{21} = 3$ и $q_{31} = 4$ занятия соответственно при 5 работающих компьютерах. Из формулы (1) выходит что «коэффициенты знаний» лабораторного класса для каждой из трех групп составляет $k_1 = 0.5$, $k_2 = 0.45$ и $k_3 = 0.35$ соответственно. Из этого следует, что каждый студент из группы g_1 вместо положенных 3 единиц знаний за три занятия получит 1,5 единиц знаний, студент из группы g_2 вместо положенных 3 единиц знаний за три занятия получит 1,35 единиц знаний, а студент из группы g_3 вместо положенных 4 единиц знаний за четыре занятия получит 1,4 единиц знаний в лабораторном классе.

Используя формулу (2) вычислим количественное значение этого недополученного знания (ущерба). Если учесть, что студент в среднем платит ежегодно за обучение 400 000 тенге в год или 250 тенге за каждый час обучения, при обучении 52 недель в году, 5 дней в неделю и 6 часов в день. Для вышеприведенного примера ущерб знаний всех студентов по лабораторному классу в течение дня составил 17 387 тенге.

Обобщая формулу (2) для всех лабораторий вуза, получим формулу для расчета ущерба знаний студентов по вузу в единицу времени:

$$S = C_o \sum_{a=1}^{KF} \sum_{b=1}^{KK} \sum_{l=1}^{KL} \sum_{t=1}^{KG} (1 - k_{ablt}) \cdot g_{ablt} \cdot q_{abtl} \qquad (3)$$

где C_o – оплата студента за обучение в единицу времени, KF - количество факультетов, KK - количество кафедр, KL – количество компьютерных лабораторий, KG – количество групп обучивщих в еденицу времени в лабораторном классе l, k_l – «коэффициент знаний» для l - го лабораторного класса, g_t – число студентов в группе t, q_{tl} – количество проведенных занятии в единицу времени группы t в лаборатории l.

Необходимость оперативного управления информационной безопасностью учебного процесса. В нашей модели выше, оперативность управления информационной безопасностью обеспечивается с помощью параметра q_{tl}. Руководство должно самостоятельно выбирать оперативного управления. Параметр q_{tl} может принимать значение такие как академический час, день, неделя, месяц, и т.д. Чем оперативнее мы будем реагировать на инциденты по устранению неисправностей, тем меньше составит ущерб вуза.

Использование технологии ситуационного управления для реализации оперативного управления информационной безопасностью. 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].

Описание предлагаемой системы ситуационного управления информационной безопасностью учебного процесса.

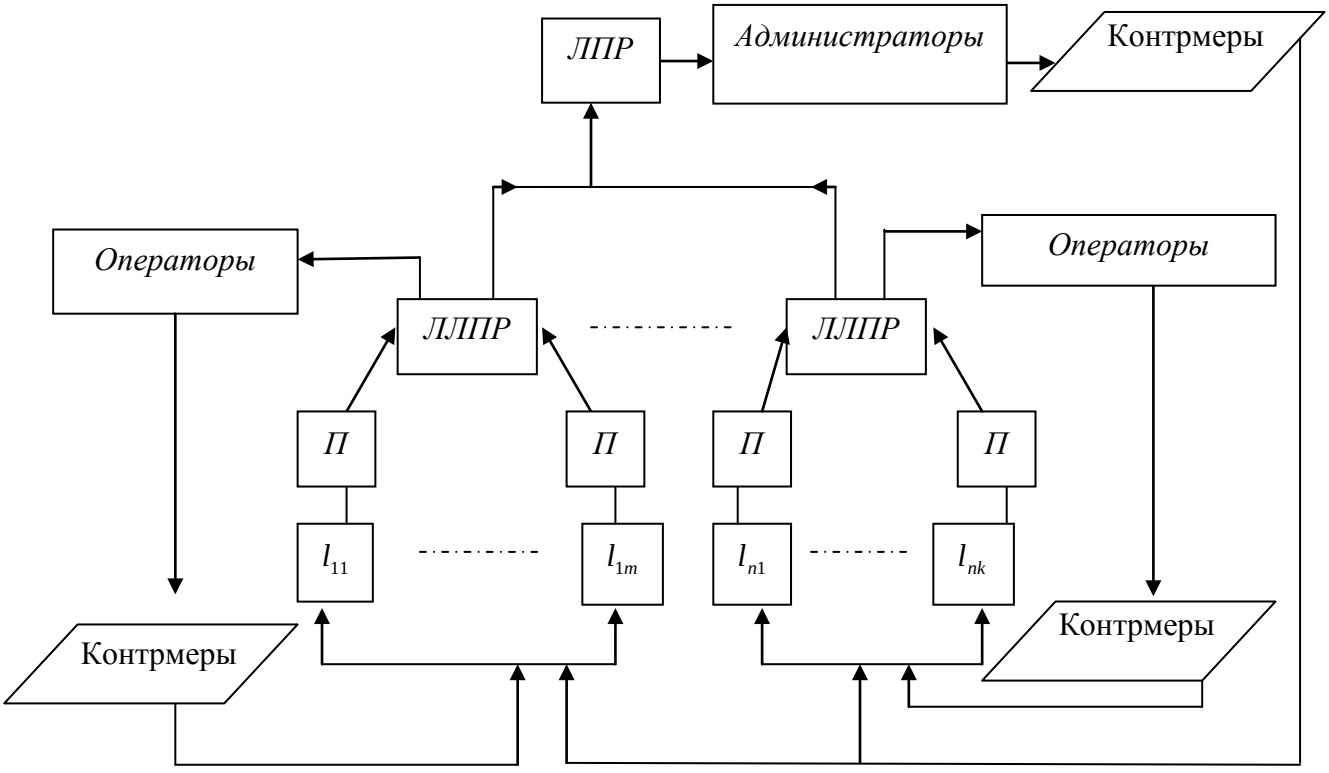

Рисунок 1 - Технология ситуационного управления информационной безопасностью

Существующая в вузах технология обеспечения качества учебного процесса в лабораториях вуза работает недостаточно эффективно. 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).

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

Резюме

В данной статье рассмотрены следующие вопросы:

– Влияние информационной безопасности на качество учебного процесса;

- Измерения влияния информационной безопасности на качество учебного процесса;
- Необходимость оперативного управления информационной безопасностью учебного процесса;
- Использование технологии ситуационного управления для реализации оперативного управления информационной безопасностью;
- Описание предлагаемой системы ситуационного управления информационной безопасностью учебного процесса.

ЛИТЕРАТУРА

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. Информационная безопасность и его влияние на уровень знаний студентов. // Вестник КазАТК имени М. Тынышпаева, 2009., № 2. – С.153-158.