Министерство образования и науки Российской Федерации

Алтайский государственный технический
университет им. И.И.Ползунова

НАУКА И МОЛОДЕЖЬ

3-я Всероссийская научно-техническая конференция
студентов, аспирантов и молодых ученых

СЕКЦИЯ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

подсекция

**БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И
ЗАЩИТА ИНФОРМАЦИИ**

Барнаул – 2006

ББК 784.584(2 Рос 537)638.1

3-я Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых "Наука и молодежь". Секция «Информационные технологии». Подсекция «Безопасность информационных технологий и защита информации» / Алт. гос. техн. ун-т им. И.И.Ползунова. – Барнаул: изд-во АлтГТУ, 2006.– 33с.

В сборнике представлены работы научно-технической конференции студентов, аспирантов и молодых ученых, проходившей в апреле 2006 г.

СОДЕРЖАНИЕ

Яковлев Д.С., Белов В.М. Проблема оптимизации функций удостоверяющего центра электронной цифровой подписи 4
Лынов Е.С., Белов В.М. Методика автоматизированного структурного моделирования безопасности структурно-сложных систем 6
Невзоров А.В., Белов В.М. Проблемы оптимизации работ по защите информации 9
Ступкина А.А., Садовая И.А., Загинайлов Ю.Н. Классификация угроз безопасности информации на основе структурно-логической модели 10
Суворов Д.А., Баташов М.В. Сравнительный анализ моделей данных для создания информационных хранилищ 13
Пивкин Е.Н., Баташов М.В. Логическая структура подсистемы защиты конфиденциального текущего делопроизводства кафедры 15
Ермилов Е.Е., Баташов М.В. Требования к логической структуре информационного хранилища подсистемы архивного хранения документов в составе комплексной системы защиты информации вуза 18
Головина И.С., Козлова С.Б., Загинайлов Ю.Н. Оценка параметров защищаемой информации в интересах формирования требований к комплексным системам защиты информации 20
Киселёв Н.О., Загинайлов Ю.Н., Пути развития аудита информационной безопасности 23
Ефименко К.Н. Белов В.М. Синтез безопасной операционной системы на уровне архитектуры и функциональных требований 25
Русина Л.Ю., Загинайлов Ю.Н. Защита персональных данных студентов в автоматизированных системах вуза 28
Комарова Г.Н., Баташов М.В. Анализ информационных систем управления вузами 30

ПРОБЛЕМА ОПТИМИЗАЦИИ ФУНКЦИЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Яковлев Д.С. – аспирант АлтГТУ
Белов В.М. – проф. каф. ЗИРСС

После выхода федерального закона «об Электронной цифровой подписи» прошло три года. За этот небольшой срок в нашей стране возникло около 150 удостоверяющих центров электронной цифровой подписи (УЦ ЭЦП). Но несмотря на то что в законе прописаны функции которые должен выполнять УЦ ЭЦП выполнятся эти функции могут несколькими методами. Поэтому от выбора методов реализации функций зависит эффективность работы УЦ ЭЦП.

Первый шаг в работе УЦ это взаимодействие с уполномоченным федеральным органом исполнительной власти. В соответствии с Постановлением Правительства РФ от 30.06.2004 № 319 на Федеральное агентство по информационным технологиям (Росинформтехнологии) возложено выполнение обязанностей уполномоченного федерального органа (УФО) исполнительной власти в области электронной цифровой подписи (ЭЦП).

1) УЦ до начала использования электронной цифровой подписи уполномоченного лица УЦ для заверения от имени УЦ сертификатов ключей подписей обязан представить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица УЦ в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью УЦ.

2) Уполномоченный федеральный орган исполнительной власти ведет единый государственный реестр сертификатов ключей подписей, которыми удостоверяющие центры, работающие с участниками информационных систем общего пользования, заверяют выдаваемые ими сертификаты ключей подписей, обеспечивает возможность свободного доступа к этому реестру и выдает сертификаты ключей подписей соответствующих уполномоченных лиц УЦ.

3) ЭЦП уполномоченных лиц УЦ могут использоваться только после включения их в единый государственный реестр сертификатов ключей подписей. Использование этих ЭЦП для целей, не связанных с заверением сертификатов ключей подписей и сведений об их действии, не допускается.

4)Уполномоченный федеральный орган исполнительной власти:

- осуществляет по обращениям физических лиц, организаций, федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления подтверждение подлинности электронных цифровых подписей уполномоченных лиц УЦ в выданных ими сертификатах ключей подписей;
- осуществляет в соответствии с положением об уполномоченном федеральном органе исполнительной власти иные полномочия по обеспечению действия настоящего Федерального закона.

Таким образом, до начала работы УЦ необходимо получить заверение от федерального органа исполнительной власти. А уполномоченный удостоверяющий центр должен включить ЭЦП уполномоченных лиц удостоверяющих центров в свой реестр и только тогда УЦ сертификаты ключей УЦ будут иметь юридическую силу.

Следующий шаг при формировании УЦ это взаимодействие с владельцем сертификата ключа подписи.

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи:

-вносит сертификат ключа подписи в реестр сертификатов ключей подписей;

-обеспечивает выдачу сертификата ключа подписи обратившимся к нему участникам корпоративной системы;

-приостанавливает действие сертификата ключа подписи по обращению его владельца;

-уведомляет владельца сертификата ключа подписи о фактах, которые стали известны Удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;

-выполняет разбор конфликтных ситуаций, связанных с применением электронной цифровой подписи участников системы корпоративного документооборота с выдачей экспертного заключения.

Таким образом УЦ не просто выдает сертификаты ключей подписи но и является органом регулирующим электронный документооборот в своем регионе.

На этом этапе идет определение внутренних функций УЦ таких как:

1)Регистрация пользователя услуг УЦ (сотрудники УЦ вносят в реестр данные по пользователю услуг УЦ и принимают решение о выдачи сертификата ключа подписи)

2)Изготовление и получение сертификата ключа подписи (УЦ выдает сертификат пользователю УЦ по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи)

3)Приостановление и возобновление действия сертификатов ключей подписей, а также их аннулирование.

4)Подтверждение подлинности ЭЦП в электронных документах.

На этом этапе формируется политика работы с пользователями и выданными им сертификатами. От того, как построить эти взаимоотношения и зависит оптимальность работы УЦ.

И последний шаг это взаимодействия между УЦ.

В настоящее время в России формируются два типа таких отношений:

1)При помощи корневого УЦ. В этом случае заданы одинаковые стандарты и спецификации для подчиненных удостоверяющих центров. При этом корневой удостоверяющий центр целесообразно использовать в качестве головного для удостоверяющих центров федеральных и региональных органов государственной власти. Недостатком данного метода является подчиненность заданным стандартам.

2)При помощи добровольного объединения УЦ. В данном случае осуществляется техническая, экономическая помощь и поддержка региональным УЦ, вступившим в объединение.

Лучшим вариантом было бы вступить в обе эти системы.

Исходя из функций УЦ, можно выделить следующие этапы работы УЦ:

1) Регистрация.
2) Выдача сертификата.
3) Обслуживание сертификата.
4) Аутентификация пользователя.

При регистрации УЦ необходимо собрать достоверную информацию о пользователе и принять решение о выдачи сертификата ключа. При принятии положительного решения, сотрудник УЦ выполняет регистрационные действия по занесению регистрационной информации в реестр УЦ.

Выдача сертификата ключа подписи производится в бумажном и(или) электронном виде на основании заявления на изготовление сертификата ключа подписи при личном прибытии пользователя УЦ в офис УЦ.

Обслуживание сертификата состоит из приостановления возобновления действия сертификата ключа подписи, а также аннулирования их.

Эти операции производятся либо по заявлению пользователя УЦ, либо по инициативе УЦ в связи с нарушениями пользователем своих обязательств.

И последнее это осуществление по обращению пользователя УЦ подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей.

Что касается стандартов ЭЦП, то здесь наблюдается практически полное соответствие: стандарты ЭЦП России и США базируются на родственных модификациях схемы ЭЦП Эль-Гамаля и отличаются рядом несущественных деталей. Совсем недавно эти стандарты были обновлены — переведены на «эллиптические кривые». Подобная поспешность может свидетельствовать в пользу того, что государственные структуры продвинулись в изучении проблемы дискретного логарифмирования в конечных полях несколько дальше, чем сообщество, ведущее открытые исследования в криптографии. Кроме того, практическая синхронность принятия и обновления стандартов ЭЦП в России и США может говорить в пользу того, что оба государства находятся на примерно одном и том же уровне в научных исследованиях в области криптографии.

Так что в данном случае я предложил использовать отечественный стандарт ГОСТ Р 34.10-2001, построенный на эллиптических кривых.

Таким образом, получается, что УЦ являет собой сервер безопасности.

На серверной стороне происходит формирование и регулирование сертификатов ключей подписей. Кроме того, по заявлению пользователя осуществляет проверку подлинности сертификата.

Клиентская же часть состоит из механизма создания подписи электронному документу и проверки подлинности ЭЦП у входящих электронных документов.

Проблема оптимизации функций свелась к проблеме построения оптимальной архитектуры взаимодействия сервера с клиентом. И сводится к вопросу программной оптимизации архитектуры УЦ ЭЦП.

Литература

1. Федеральный закон «Об электронной цифровой подписи».
2. А.Ю. Винокуров Стандарты аутентификации и ЭЦП России и США // Отраслевой каталог «Технологии и средства связи-2003».
3. Byte Magazine Online - Цифровая подпись - как это делается (http://www.bytemag.ru/Article.asp?ID=2398)

МЕТОДИКА АВТОМАТИЗОВАННОГО СТРУКТУРНОГО МОДЕЛИРОВАНИЯ БЕЗОПАСНОСТИ СТРУКТУРНО-СЛОЖНЫХ СИСТЕМ

Лынов Е.С. – аспирант каф. ЗИРСС
Белов В.М. – проф. каф. ЗИРСС

Проблема количественной оценки надежности и безопасности структурно-сложных технических систем (ССТС) в последние годы существенно обострилась как в отечественной науке и промышленности, так и за рубежом [1]. Это обусловлено несколькими причинами, среди которых можно выделить две основные:

1. Постоянно возрастающие потребности практики в увеличении уровня надежности и безопасности ССТС, особенно предназначенных для работ на опасных производственных объектах;

2. Постоянно возрастающие структурная сложность и размерность современных ССТС и математических моделей их надежности и безопасности.

Первая из указанных причин диктует необходимость расширения областей применения научных методов анализа этих свойств на предприятиях. Вторая причина определяет содержание главной проблемы, из-за которой, как правило, оказывается невозможным практическое применение даже известных и теоретически проработанных научных методов анализа надежности и безопасности систем. Эта проблема проявляется в следующем:

1. С помощью традиционных (неавтоматизированных, ручных) технологий во многих случаях практически невозможно построение необходимых математических моделей надежности и безопасности современных технических систем большой размерности и высокой структурной сложности;

2. Многие предприятия при разработке технических решений до сих пор недостаточно используют новые информационные технологии автоматизированного моделирования и расчета надежности и безопасности различных СТС.

Количественная оценка надежности и безопасности СТС различных видов, классов и назначения предусмотрена нормативно-техническими требованиями к их промышленной разработке, производству и эксплуатации [2,3]. Это необходимо для объективной и научно обоснованной оценки существующего уровня надежности и безопасности СТС и выработки, обоснования и оптимизации различных управленческих решений, направленных на их повышение.

Цель работы – развитие методов и средств технологии автоматизированного структурно-логического моделирования, обеспечивающее возможность ее использования на предприятиях промышленности для оценки надежности и безопасности сложных технических систем.

Для решения этой главной задачи поставлены и решены следующие частные научные и практические задачи:

1. обоснование выбора технологии автоматизированного структурно-логического моделирования в качестве базовой для оценки показателей надежности и безопасности сложных технических систем;

2. разработка комплекса методов и методик реализации положений односвязной структурной декомпозиции моделей надежности и безопасности систем большой размерности и высокой структурной сложности;

3. определение состава модулей и общей структуры базового образца программного комплекса автоматизированного моделирования и расчета показателей надежности и безопасности структурно-сложных технических систем;

4. разработка методики автоматизированного моделирования и расчета ожидаемого ущерба от отказа аппаратно-программных компонент на предприятии; разработка основных методических положений и рекомендаций по применению теории, технологии и программных комплексов автоматизированного структурно-логического моделирования для оценки надежности и безопасности сложных систем на предприятиях промышленности.

При проведении исследований использовались следующие научные теории и методы: системный подход, теория сложных систем, теория автоматизированного структурно-логического моделирования, общий логико-вероятностный метод, методы теории вероятности, алгебры логики, теории надежности и безопасности систем.

Впервые разработан полный и взаимосвязанный комплекс новых методов и методик многоуровневой реализации односвязной структурной декомпозиции, охватывающий все четыре основные этапа технологии автоматизированного структурно-логического моделирования систем (АСМ). Этот комплекс методов и методик включает в себя:

1. Три новые малоразмерные формы представления и методики получения декомпозированных логико-вероятностных моделей СТС:

- методику построения составных схем функциональной целостности (ССФЦ), которая позволяет применять в технологии АСМ как традиционный прямой, так новый обратный способ декомпозиции.

- методику построения на основе ССФЦ малоразмерных составных логических функций работоспособности (СФРС), которая, в отличие от существующей двухуровневой, позволяет автоматизировать процесс многоуровневой логической декомпозиции высокоразмерных систем;

- методику построения на основе СФРС малоразмерного составного многочлена вероятностной функции (СВФ), которая, в отличие от существующей двухуровневой, позволяет автоматизировать процесс многоуровневой вероятностной декомпозиции высокоразмерных систем.

2. Два метода обратного преобразования составных форм логических и вероятностных функций в явные (полные) формы их представления, которые небыли разработаны в основных положениях односвязной структурной декомпозиции технологии АСМ.

3. Метод последовательной многоуровневой подстановки и пять методик его применения, которые, в отличие от известных методов, позволяют на основе многочлена СВФ вычислять не только статические, но все основные виды вероятностно-временных показателей надежности и безопасности невосстанавливаемых и восстанавливаемых ССТС.

4. Специальную методику, которая впервые позволяет в технологии АСМ на основе ФРС и СФРС любого вида строить математические модели и вычислять показатели ожидаемого ущерба от аварии на опасном производственном объекте. В этой методике разработаны два способа представления сценариев развития аварии на опасном производственном объекте – с помощью СФЦ с инверсными связями и с помощью СФЦ с группами несовместных событий.

Все предложенные методы и методики имеют алгоритмический уровень разработки, что позволило осуществить их непосредственную реализацию в программном комплексе автоматизированного структурно- логического моделирования и расчета надежности и безопасности ССТС большой размерности.

Программном комплекс включает пять групп программных модулей к каждой из которых в диссертации выработаны требования к разработке и программной реализации. Главные из них следующие:

- основное назначение интерфейса пользователя состоит в создании удобной интерактивной среды, позволяющей пользователю эффективно выполнять все виды работ по графическому вводу ССФЦ, заданию критериев функционирования системы, параметров элементов, и общей организации автоматизированного моделирования и расчета показателей надежности и/или безопасности исследуемых ССТС;

- программные модули блока 2 предназначены для автоматизации процессов подготовки, ввода, хранения и преобразования исходных данных, необходимых для автоматизированного моделирования и расчетов надежности и безопасности ССТС. К ним относятся процессы машинного представления ССФЦ исследуемой ССТС, логических критериев, параметров элементов, реализации заданных режимов моделирования и расчетов, объемов информации выводимой на экран дисплея и сохраняемых в файлах результатов;

- модули блока 3 предназначены для организации работы специальных баз данных, с помощью которых хранится, преобразуется и используется информация, необходимая для всех видов работ по оценке надежности и безопасности ССТС на различных стадиях их разработки и эксплуатации. Предполагается организация двух видов баз данных – параметров элементов и проектов ССТС;

- модули блока 4 представляют библиотеку ЛОГ&ВФ программ автоматического построения математических моделей, используемых для детерминированного и вероятностного анализа надежности и безопасности исследуемых ССТС;

- модули блока 5 предназначены для выполнения расчетов показателей надежности и безопасности функционирования исследуемых ССТС на основе автоматически сформированных составных или полных многочленов вероятностных функций.

Практическая ценность работы заключается в том, что полученные научные результаты диссертационного исследования могут непосредственно использоваться при создании программных комплексов автоматизированного структурно-логического моделирования и разработке различных методик их применения на предприятиях для оценки надежности и безопасности систем большой размерности и высокой структурной сложности.

Литература

1. Нозик А.А., Мусаев А.А. Математическая постановка компьютерного моделирования задач оптимизации функциональной надежности автоматизированных систем управления. // Материалы III Международной научно-практической конференции: "Компьютерные технологии в науке, производстве, социальных и экономических процессах". Новочеркасск: ООО НПО "ТЕМП", 2001. -Ч. 1., С.4-10.
1. Можаев А.С., Алексеев А.О. Автоматизированное структурно-логическое моделирование и вероятностный анализ сложных систем. В сб. 1: 'Теория и информационная технология моделирования безопасности сложных систем'. Вып.2. Под редакцией И.А.Рябинина. Препринт 104. СПб.: ИПМАШ РАМ, 1994, с.17-42
2. Рябинин И.А. Надежность и безопасность сложных систем. // СПб.: Политехника, 2000. –248 с

ПРОБЛЕМЫ ОПТИМИЗАЦИИ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Невзоров А.В. – аспирант АлтГТУ
Белов В.М. – проф. каф. ЗИРСС

Во все времена вопросы защиты информации были чрезвычайно актуальны. В современном информатизированном обществе, при многократно возросших потоках информации, фирмы, предприятия, организации серьезно озабочены сохранением своих ноу-хау, коммерческой тайны, специальной информации, утечка которых может привести к многомиллионным убыткам. Проблему обостряют возросшие технические возможности желающих негласно получить эту информацию (криминальные структуры, конкуренты и др.). В связи с этим соответственно возрастает объем работ по аттестации вычислительной техники и выделенных помещений. Так как возрастает количество обращений по защите конфиденциальной информации.

В связи с этим, специалисту организации проводящей работы по защите информации: специсследования или контроль эффективности защиты информации от утечки за счет побочных электромагнитных излучений (ПЭМИ), для оптимизации проводимых работ необходимо четко представлять каналы информационного взаимодействия отдельных модулей ПЭВМ между собой и с периферией. Представление о путях информационного обмена в компьютере позволяет выявить места предполагаемого возникновения канала утечки за счет ПЭМИ. Так как ПЭВМ является сложной электронной аппаратурой, соответственно она является источником электромагнитных излучений, среди которых могут встречаться несущие информативные сигналы. Это является одной из проблем при возрастающих объемах заказов. Четкое представление о местах возникновения наиболее мощных сигналов ПЭМИ минимизирует количество измерений. Так как при обнаружении мощных сигналов от определенных устройств (как правило, наибольший уровень сигналов ПЭМИ получается от мониторов, даже жидкокристаллические мониторы могут давать довольно высокий уровень ПЭМИ) достаточно рассчитать необходимый радиус контролируемой зоны для этих устройств. Это позволяет уменьшить количество измерений при больших объемах исследований. Например, при проведении работ по аттестации локальных вычислительных сетей на соответствие требованиям по безопасности информации.

Второй проблемой является большой объем разрабатываемой документации (пять документов на каждый объект защиты в простейшем случае, но не редко аттестующей организацией, по просьбе заказчика, разрабатывается полный комплект – порядка двадцати документов). В этом случае задача автоматизации расчетных задач и создания документов

становится актуальной. Как правило, разработка документов занимает примерно две трети времени затрачиваемого на аттестацию отдельного объекта. На сегодняшний день в продаже не существует программного обеспечения для решения всех расчетных задач при аттестации на соответствие требованиям по безопасности информации, имеющиеся программные продукты включены в состав дорогостоящих программно-аппаратных комплексов и не удовлетворяют всем нормативно-методическим документам.

Решение выявленных проблем значительно сократит время и усилия, затрачиваемые на разработку документов и проведение расчетов по результатам измерений, что в свою очередь уменьшит время, затрачиваемое на аттестацию отдельного объекта. Оптимальным решением этих проблем является разработка программного комплекса позволяющего на основании данных об объекте защиты и результатов измерений в автоматическом режиме провести необходимые расчеты и сформировать необходимые документы. В рамках данного решения автором были разработаны программные модули, решающие следующие задачи: разработан модуль построения описательной модели объекта защиты с целью формирования в дальнейшем блоков данных об объекте для формирования файлов документов в формате Word. Разработан модуль для генерации документов и модуль сопряжения с программой Word, позволяющий формировать документы и результаты расчетов непосредственно в программе Ms Word для дальнейшего сохранения. Текстовый редактор Ms Word был выбран, как получивший наибольшее распространение. Так же реализованы модули автоматизации расчетов результатов оценки защищенности по акустическому каналу и по каналу утечки за счет ПЭМИ. В дальнейшем все автономные модули будут объединены в программный комплекс.

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ СТРУКТУРНО-ЛОГИЧЕСКОЙ МОДЕЛИ

Ступкина А.А. – аспирант АлтГТУ
Садовая И.А. – студентка гр. КЗОИ-11
Загинайлов Ю.Н.- доцент каф. ЗИРСС

На протяжении всего периода существования проблемы защиты информации, учёными и специалистами в этой области, предпринимаются попытки классифицировать угрозы безопасности информации, с целью стандартизации средств и методов, применяемых для защиты. К настоящему времени фиксируется значительное количество угроз различного происхождения и подходов к их классификации [1-6].

В качестве параметров системной классификации, выполненной в [1,3,6], применяются:

- источник угрозы, фактор (уязвимость), угроза (действие), последствия (атака), ущерб[1];
- каналы несанкционированного получения информации [3];
- виды угроз, природа происхождения, предпосылки появления угроз, источники угроз [6].

Существующие в России методики оценки угроз безопасности информации, для проектирования систем защиты информации на объектах информатизации, базируются на положениях специального стандарта [7], классифицирующего факторы, воздействующие на информацию. Классификация факторов выполнена по двум признакам: внешние и внутренние, субъективные и объективные. Однако ни указанные методики, ни стандарты, в полной мере не предоставляют возможности моделирования угроз и их идентификации для объекта информатизации на практике, а служат лишь теоретическим базисом. Поэтому классификация угроз безопасности информации является актуальной задачей, решение которой позволит дать специалистам методику для практического решения задач

моделирования и идентификации угроз.

Оптимальным решением вопроса классификации угроз видится формирование структурно-логической модели угрозы, элементы которой отражают все аспекты её существования и реализации и их классификация.

Исходя из анализа задач решаемых при моделировании и оценке угроз, каждая угроза информации на объекте информатизации включает: -источник угрозы, способ и средство реализации, уязвимости информации и средств (систем) её обработки, результат воздействия. В соответствии с этим структурно-логическая модель угрозы может быть представлена кортежем взаимозависимых компонентов:

- источники угрозы безопасности информации;
- способ и средство реализации угроз;
- канал реализации угрозы;
- классификация уязвимостей информации и средств (систем) её обработки;
- результат воздействия.

На основе структурно-логической модели выполнена классификация всех её компонентов. При этом принципиально новой является классификация каналов реализации угрозы и способов, основанных на факторах приведенных в стандарте [7].

Классификация способов реализации угроз представляется следующим образом.

Классы способов реализации угроз:

- [A] Способы реализации угроз со стороны внешних субъективных источников;
- [B] Способы реализации угроз со стороны внутренних субъективных источников.

Класс [A] содержит группы и подгруппы.

Группа [A.I]. Доступ к защищаемой информации с применением технических средств разведки:

- [A.I.a] доступ с использованием средств радиоэлектронной разведки;
- [A.I.b] доступ с использованием средств оптико-электронной разведки;
- [A.I.c] доступ с использованием средств фотографической разведки;
- [A.I.d] доступ с использованием средств визуально-оптической разведки;
- [A.I.e] доступ с использованием средств акустической разведки;
- [A.I.f] доступ с использованием средств гидроакустической разведки;
- [A.I.j] доступ с использованием средств компьютерной разведки.

Группа [A.II]. Доступ к защищаемой информации с использованием эффекта «высокочастотного навязывания»:

- [A.II.a] доступ к защищаемой информации с применением генератора высокочастотных колебаний;
- [A.II.b] доступ к защищаемой информации с применением генератора высокочастотного электромагнитного поля.

Группа [A.III]. Несанкционированный доступ к защищаемой информации:

- [A.III.a] подключение к техническим средствам и системам объекта информатизации;
- [A.III.b] использование закладочных устройств;
- [A.III.c] использование программного обеспечения технических средств объекта информатизации;
- [A.III.d] несанкционированный физический доступ;
- [A.III.e] Хищение носителя с защищаемой информацией.

Группа [A.IV]. Блокирование доступа к защищаемой информации:

- [A.IV.a] Блокирование доступа к ЗИ путём перегрузки технических средств обработки информации ложными заявками на её обработку.

Группа [A.V]. Действия криминальных групп и отдельных преступных групп:

- [A.V.a] диверсия в отношении объекта информатизации.

Класс [B] содержит группы и подгруппы.

Группа [B.I]. Разглашение защищаемой информации лицами, имеющими к ней право доступа:

- [B.I.a] разглашение информации лицам, не имеющим права доступа к защищаемой информации;
- [B.I.b] передача информации по открытым линиям связи;
- [B.I.c] обработка информации на незащищенных технических средствах обработки информации;
- [B.I.d] опубликование информации в открытой печати и других средствах массовой информации;
- [B.I.e] копирование информации на незарегистрированный носитель информации;
- [B.I.f] передача носителя информации лицу, не имеющему права доступа к ней.

Группа [B.II]. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

- [B.II.a] несанкционированное изменение информации;
- [B.II.b] несанкционированное копирование информации.

Группа [B.III]. Несанкционированный доступ к защищаемой информации:

- [B.III.a] подключение к техническим средствам и системам объекта информатизации;
- [B.III.b] использование закладочных устройств;
- [B.III.c] использование программного обеспечения технических средств объекта информатизации;
- [B.III.d] хищение носителя защищаемой информации;
- [B.III.e] нарушение функционирования технических средств обработки информации.

Классификация каналов реализации угроз представляется следующим образом.

Классы каналов реализации угроз безопасности информации включают:

- [I] организационные каналы утечки информации;
- [II] технические каналы утечки информации;
- [III] инфо-коммуникационные каналы утечки информации;
- [IV] системно-программные каналы утечки информации;
- [V] комбинированные каналы утечки информации.

Технические каналы утечки информации включают группы и подгруппы.

Группа [II.A]. Радиоэлектронные каналы утечки информации:

- [II.A.1] электромагнитный;
- [II.A.2] электрический.

Группа [II.B]. Оптические каналы утечки информации:

- [II.B.1] визуально – оптический;
- [II.B.2] оптико-электронный;
- [II.B.3] фотографический.

Группа [II.C]. Акустические каналы утечки информации:

- [II.C.1] виброакустический;
- [II.C.2] акустоэлектрический;
- [II.C.3] гидроакустический.

Группа [II.D]. Материально-вещественные каналы утечки информации включает:

- [II.D.1] канал утечки производственных отходов секретного производства;
- [II.D.2] канал отходов бумажного и электронного делопроизводства.

Классификация источников угроз, уязвимостей, результата воздействия рассматривается в ранее упомянутых источниках [1,6].

Рассматриваемая классификация угроз безопасности информации предоставляет возможности их идентификации, формализации и автоматизации процессов анализа и оценки. Принципиально новыми являются классификации способов и каналов реализации угроз.

Предложенная структурно - логическая модель угрозы безопасности информации существенно расширяет возможности по моделированию угроз объектам информатизации и может рассматриваться как основа для разработки соответствующего метода классификации.

Литература

1. Вихорев С. В., Кобцев Р. Ю. Как узнать – откуда напасть или откуда исходит угроза безопасности информации // Защита информации. Конфидент, № 2, 2002. С. 44–49.
2. Ярочкин В.И. Информационная безопасность. М.: Международные отношения, 2000. - 320с.
3. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: 000 "Инком-бук", 1997.
4. В.М. Зима, А.А. Молдовян, Н.А. Молдовян. Безопасность глобальных сетевых технологий.-СПб.:БХВ-Санкт-Пе-тербург,2000.-320с.:ил.
5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем.- М.: Горячая линия - Телеком, 2000.-452 с.
6. Малюк А.А. Информационная бе-зопасность: концептуальные и методологические основы защиты информации. Учеб.пос для вузов.-М: Горячая линия-Телеком,2004.-280 с.
7. ГОСТ Р 51275-99. Объект информатизации. Факторы, воздействующие на информацию. ИПК: Издательство стандартов, 1999. –7с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДЕЛЕЙ ДАННЫХ ДЛЯ СОЗДАНИЯ ИНФОРМАЦИОННЫХ ХРАНИЛИЩ

Суворов Д.А. – студент гр.КЗОИ –11
Баташов М.В. – ст. преп. каф. ЗИРСС

Проводимые специалистами исследования показывают, что на данный момент не менее 30% всей корпоративной информации хранится в электронном виде (документы структурированные – в БД и неструктурированные). Вся остальная информация хранится на бумаге. А отсюда главные проблемы бумажного документооборота – поиск и хранение (по оценкам статистиков в настоящее время только в США ежедневно создается более 1 млрд. страниц документов, а в архивах хранится уже более 1.3 трлн. различных документов)[1]. Следует отметить, что в последнее время расстановка сил изменяется в пользу электронного документооборота.

По некоторым оценкам объем корпоративной электронной текстовой информации удваивается каждые 3 года[1].

В связи с вышеизложенным возросла актуальность создания информационных хранилищ условно-постоянной информации (далее ИХ УПИ), использующих новые подходы к хранению информации.

Был проведен анализ моделей данных таких хранилищ. Следует отметить, что в производительность современных ЭВМ в совокупности с достаточно высокой пропускной способностью вычислительных сетей практически нивелирует время работы систем электронного документооборота, если они построены на основе одинаковых моделей данных. При выборе конкретного решения основную роль должен играть анализ принципов построения внутренней структуры базы данных, чтобы получить максимально точную, полную, а главное – наиболее производительную проекцию моделируемой действительности.

В соответствии с [2] под моделью данных понимают средства логического представления физических данных.

К наиболее известным моделям данных можно отнести иерархическую, сетевую и реляционную модели. Их подробное описание изложено в [3]. Преимущества и недостатки указанных моделей данных представлены в таблице 1.

Более удобным, гибким, а главное менее ресурсоемким средством работы с большими массивами информации является информационно-поисковая система на основе классификационных таблиц (другое название – таблицы принятия решений, далее ТПР), которые позволяют обрабатывать множество независимых переменных, т.е. функцию вида $y = f(x_1,x_2,\ldots,x_n)$. Основы работы с классификационными таблицами описаны в [4].

Отличительной особенностью ТПР является возможность эффективной организации распределенных вычислений. Каждое условие может проверяться независимо от остальных, и на финальном этапе происходит пересечение найденных столбцов. Это позволяет значительно уменьшить время поиска, что особенно ощутимо в условиях кластерной обработки информации. В свою очередь, ни иерархическая, ни сетевая, ни реляционные модели в полной мере не могут быть ориентированны на распределенные вычисления.

Как видно из вышеизложенного, в теории имеются определенные преимущества использования в ИХ УПИ модели данных, основанной на классификационных таблицах.

На кафедре «Защита информационных ресурсов и систем связи» АлтГТУ осуществляется создание прототипа защищенного ИХ УПИ, основанного на классификационных таблицах. Для создания такого хранилища был выбран язык программирования Java, как обеспечивающий:

- безопасность;
- архитектурную независимость;
- ориентацию на объект исследования;
- простоту;
- живучесть;
- высокую производительность;
- многопоточность;
- масштабируемость.

Таблица 1 – Преимущества и недостатки основных моделей данных

Вид модели	Достоинства	Недостатки
Иерархическая	а) простота понимания модели.	а) Доступ к порожденному узлу только через родительский узел, отсюда ограниченный набор структур запроса. б) Удаление исходных узлов ведет к удалению порожденных. в) Избыточность, т.к. любой порожденный узел имеет единственный родительский узел и при необходимости включения одного и того же узла в разные поддеревья необходимо хранить несколько копий объекта.
Сетевая	а) Более широкие возможности по формированию запросов (по сравнению с иерархической моделью).	а) Значительное усложнение как логической, так и физической структуры базы данных (по сравнению с иерархической моделью).
Реляционная	а) Гибкость. б) Простота работы. в) Независимость от физической реализации. г) Хорошее теоретическое обоснование.	а) Возможность логических ошибок на этапе формирования структуры таблиц и установления отношений между ними б) Значительная ресурсоемкость реляционной СУБД

По результатам испытаний прототипа можно будет делать вывод о возможности применения механизма таблиц соответствия для организации защищенного электронного документооборота.

Литература

1. http://www.citforum.ru/consulting/docflow/market/article1.8.2002.html#AEN10 – Мировой рынок систем электронного документооборота, Введение.
2. Озкарахан Э. Машины баз данных и управление базами данных: Пер. с англ. – М.: Мир, 1989. – 696 с., ил.
3. http://www.citforum.ru/database/osbd/glava_11.shtml – С.Д. Кузнецов. Основы современных баз данных, информационно-аналитические материалы Центра Информационных Технологий.
4. Автоматизированные системы технологической подготовки производства в машиностроении. Под ред. чл.-кор. АН БССР Г.К. Горанского. М., «Машиностроение», 1976.

ЛОГИЧЕСКАЯ СТРУКТУРА ПОДСИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОГО ТЕКУЩЕГО ДЕЛОПРОИЗВОДСТВА КАФЕДРЫ

Пивкин Е.Н. – студент гр. КЗОИ-11
Баташов М.В. – ст. преп. каф. ЗИРСС

В современных условиях для повышения эффективности управления необходимо совершенствование работы с документами, так как всякое управленческое решение всегда базируется на информации, отображенном в документе.

Целью исследования являлось анализ системы документационного обеспечения, внесение новых механизмов хранения и управления информации в процессе осуществления документооборота кафедры, как научно-учебного подразделения ВУЗа. Данная цель реализуется в рамках проекта «Логическая структура подсистемы защиты текущего конфиденциального делопроизводства кафедры».

Актуальность данной работы обусловлена следующими факторами:

- не менее 30 % корпоративной информации хранится в электронном виде, остальная в бумажном;
- по оценкам специалистов ежедневно в США создается более 1 млрд. страниц документов, а в архивах хранится более 1,3 трлн. различных документов;
- объем корпоративной текстовой информации удваивается каждые 3 года;
- рост объемов информации и документации в России на 8-15% в год в органах государственного и муниципального управления [1].

Применительно к системе научно-справочного аппарата, бумажный документооборот неэффективен по следующим причинам:

- большое время поиска документов;
- увеличивается потребность в площадях хранения;
- необходимость контроля правильности заполнения документов, дел и т.д. на этапах движения документов;
- трудность осуществления учета конфиденциальных документов, носителей конфиденциальной информации;

- проблема контроля за исполнением документов, своевременностью ответов на различные запросы и ошибок исполнителей, их выявления;
- отсутствует возможность получения объективной, непредвзятой аналитической и статистической информации для выявления наиболее важных вопросов планирования развития кафедры;
- возрастает необходимость получения актуальной, достоверной, исчерпывающей и своевременной информации по любому вопросу, в любой момент времени.

Электронные системы документационного обеспечения решают следующие задачи:

- обеспечивают более эффективного управления за счет автоматического контроля выполнения и прозрачности деятельности на всех уровнях;
- поддерживают эффективность накопления, управления и доступа к информации и знаниям;
- обеспечивают кадровую гибкость за счет формализации деятельности каждого сотрудника;
- протоколирование деятельности в целом;
- экономия ресурсов за счет сокращения издержек на управление потоками документов;
- исключение необходимости или существенное упрощение и удешевление хранения бумажных документов за счет наличия оперативного электронного архива.

Исходя из принципа единства электронного документооборота следует отметить, что наряду с явными достоинствами и недостатками возникают новые каналы утечки информации и несанкционированного доступа нарушителей.

Анализ существующего программного обеспечения российского производства (Effect Office, Optima-WorkFlow, PayDox, ЕВФРАТ-документооборот, Алмаз и Архивное дело), реализующего подобную технологию [2-7], выявил следующие недостатки:

- не соответствуют требованиям государственной системы документационного обеспечения управления (ГСДОУ)[8];
- не соответствуют «Основным правилам работы государственных архивов РФ»[9], за исключением программы «Архивное дело», обеспечивающую только учетную политику в архивах, не реализуя введение документов в научно-справочный аппарат;
- не классифицированы по классам защищенности автоматизированных систем;
- имеют сравнительно высокую стоимость.

В последнее время системы обеспечения безопасности документооборота считаются приоритетными. При этом этапы «начальной» и «финишной» обработки документов, содержащих конфиденциальные сведения, являются довольно уязвимым звеном общего процесса документооборота. Каналы ввода и вывода информации в этом контексте являются наиболее уязвимыми, так как именно через эти потоки конфиденциальная информация (полученная извне и порожденная внутри кафедры) соединяется с авторами и потребителями.

Слабая защищенность таких каналов способствует вторжениям, особенно внутренних нарушителей. Действительно, в течение рабочего дня значительное количество конфиденциальных документов копируется, размножается, печатается, докладывается руководству, переделывается, сканируется, пересылается по каналам электронной почты. А проблему защиты информационных ресурсов именно от внутренних нарушителей широко используемые специализированные средства разграничения доступа пользователей к

информационным ресурсам не решают. Связано это со следующими тремя основными факторами:

- внутренний нарушитель является авторизованным пользователем, следовательно, ему легче осуществлять несанкционированные действия;
- внутренний нарушитель находится в среде обладателей и носителей конфиденциальной информации, активно общается с ними, в том числе по каналам Intranet, где информация объективно менее контролируется;
- внутренний нарушитель легально получает доступ и работает с конфиденциальной информацией, следовательно, существует возможность записи ее на внешние носители, печати, сканирования и последующей обработки при отсутствии должного контроля.

В связи, с чем к подсистеме защиты конфиденциального текущего документооборота были предъявлены следующие основополагающие требования:

- централизованное хранение документов в защищенном (зашифрованном) виде;
- при передаче информации по каналам связи, обязательное шифрование информации;
- возможность замены модулей шифрования/дешифрования на другие;
- наличие модулей, позволяющих использовать электронно-цифровую подпись (ЭЦП);
- все пользователи системы должны осуществлять доступ к информации только в соответствии с наделенными правами;
- наличие системы аудита;
- наличие системы резервного копирования данных;
- соответствие обращения документов в системе государственной системе документационного обеспечения управления;
- соответствие системы «Основным правилам работы государственных архивов РФ».

Проведенное исследование подтвердило актуальность создания подсистемы защиты подсистемы защиты текущего конфиденциального документооборота. Был проведен сравнительный анализ традиционного и электронного документооборота. Определены основные требования к такой подсистеме.

Литература

1. http://www.citforum.ru/consulting/docflow/market/article1.8.2002.html#AEN10 – Мировой рынок систем электронного документооборота;
2. http://www.effectoffice.com/products/Sistema.shtm – Электронный документооборот и делопроизводство. Эффект Офис. Описание системы;
3. http://www.optima-workflow.com/RUS/AboutSystem/advantage.asp – Основные преимущества системы «OPTiMA-WorkFlow»;
4. http://www.paydox.ru – Электронный Документооборот PAYDOX;
5. http://www.evfrat.ru/about/index.htm – О системе ЕВФРАТ-Документооборот;
6. http://www.rcom.ru/almaz/almaz2.htm – Система электронного документооборота «АЛМАЗ»;
7. http://eos.ru/eos/21949 – Электронные офисные системы: "АРХИВНОЕ ДЕЛО", система архивного делопроизводства.
8. приказ ГЛАВАРХИВа СССР №33 от 25 мая 1988г. «Государственная система документационного обеспечения управления»;
9. Основные правила работы государственных архивов Российской Федерации/

Росархив. ВНИИДАД. – М.: Российская политическая энциклопедия (РОССПЕН), 2002. – 304с.

ТРЕБОВАНИЯ К ЛОГИЧЕСКОЙ СТРУКТУРЕ ИНФОРМАЦИОННОГО ХРАНИЛИЩА ПОДСИСТЕМЫ АРХИВНОГО ХРАНЕНИЯ ДОКУМЕНТОВ В СОСТАВЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ВУЗА

Ермилов Е.Е. – студент гр.КЗОИ-11
Баташов М.В. – ст. преп. каф. ЗИРСС

Деятельность любой организации, в том числе и вуза, так или иначе связана с документами, отражающими накопленный опыт: применяемые и разработанные технологии, нормативно-правовые документы, необходимые для регламентирования взаимоотношений внутри организации, а также другие документы сопровождающие деятельность организации.

Таких документов со временем накапливается достаточно большое количество. В соответствии с нормативными требованиями они хранятся длительный период времени в условиях, обеспечивающих их защиту от повреждений, вредных воздействий окружающей среды, исключающих утрату документов, несанкционированный доступ к ним и утечку конфиденциальной информации.

В традиционном понимании, документ представляет бумажный носитель, на котором зафиксирована некоторая информация, соответствующим образом зарегистрированная. Такая форма представления документов прошла испытание временем и поэтому можно говорить о её надёжности, но она имеет ряд недостатков.

При организации архивного хранения открытых бумажных документов наблюдаются следующие недостатки:

- требуется достаточно много пространства при хранении документов (отдельное помещение);
- требуется специальное оборудование и приборы для поддержания необходимых значений параметров светового, температурно-влажностного и санитарно-гигиенического режимов;
- хранилища документов имеют повышенную пожароопасность;
- на носителях накапливается много пыли;
- носители со временем стареют;
- повышенные требования к квалификации сотрудника по сравнению с автоматизированным документооборотом, либо увеличение затрат на обучение;
- создание резервных копий документов и их хранение невозможно в виду больших материальных затрат.

Применительно к системе научно-справочного аппарата, бумажный документооборот неэффективен по следующим причинам:

- поиск документов занимает много времени;
- увеличивается потребность в площадях хранения, т.к. объём вторичной документации велик;
- необходимость контроля правильности заполнения документов, дел и т.д. на многих этапах движения документов.

При организации архивного хранения бумажных конфиденциальных документов добавляются следующие проблемы:

- персонал, участвующий в формировании системы научно-справочного аппарата может получать доступ к конфиденциальным документам;
- введение большого количества учётных документов и выделение для этой работы дополнительного персонала;

- увеличивается время поиска и выдачи необходимых документов, если они могут быть выданы;
- существенно увеличивается количество обрабатываемых документов, т.к. необходимо учитывать также черновики, проекты документов и т.д., что ведёт к существенному увеличению трудозатрат.

Достигнутый на сегодняшний день уровень развития информационных технологий позволяет ввести новое понятие документа – электронный документ. Использование принципа единства электронного и традиционного документооборота с учетом применения электронного документа позволяет решить описанные выше проблемы.

Электронный документ имеет два основных преимущества:

- занимает значительно меньше места, чем традиционный;
- передаётся на большие расстояния за небольшое время, при этом обеспечивается его целостность, конфиденциальность и однозначная идентификация его владельца или отправителя (эти вопросы становятся на первое место при организации конфиденциального делопроизводства);

Использование электронных документов позволяет:

- существенно снизить нагрузку на площади помещений;
- ускорить поиск документов;
- значительно облегчить уборку помещений, т.к. снижается накопление пыли;
- создавать резервные копии, т.к. стоимость носителя электронного носителя относительно мала и сам он занимает мало места.

Но электронные документы имеют и ряд недостатков (новые каналы утечки и несанкционированного доступа).

Для реализации данного направления была выбрана тема «Требования к логической структуре информационного хранилища подсистемы архивного хранения документов в составе комплексной системы защиты информации вуза».

Был проведен анализ уже существующего программного обеспечения, реализующего подобную технологию. Таким образом, было выбрано несколько систем российского производства с целью определения их сильных и слабых сторон (Effect Office, OPTiMa-WorkFlow, PayDox, ЕВФРАТ-документооборот, Алмаз и Архивное дело).[1-6]

К недостаткам рассмотренных систем относится тот факт, что данные программы не соответствуют требованиям государственной системы документационного обеспечения управления[7] и ни одна из рассмотренных систем не соответствует «Основным правилам работы государственных архивов РФ»[8], за исключением программы «Архивное дело», но данная программа обеспечивает только учетную политику в архивах, не реализуя введение документов в научно-справочный аппарат. Также к недостаткам рассмотренных программных продуктов можно отнести то, что они не классифицированы по классам защищенности автоматизированных систем и имеют сравнительно высокую стоимость для университета.

Проведенное исследование подтвердило актуальность создания информационного хранилища подсистемы архивного хранения документов. Был проведен сравнительный анализ традиционного и электронного документооборота и были определены основные требования к логической структуре информационного хранилища подсистемы архивного хранения документов.

Литература

1. http://www.effectoffice.com/products/Sistema.shtm – Электронный документооборот и делопроизводство. Эффект Офис. Описание системы;
2. http://www.optima-workflow.com/RUS/AboutSystem/advantage.asp – Основные преимущества системы «OPTiMA-WorkFlow»;

3. http://www.paydox.ru – Электронный Документооборот PAYDOX;
4. http://www.evfrat.ru/about/index.htm – О системе ЕВФРАТ-Документооборот;
5. http://www.rcom.ru/almaz/almaz2.htm – Система электронного документооборота "АЛМАЗ";
6. http://eos.ru/eos/21949 – Электронные офисные системы: "АРХИВНОЕ ДЕЛО", система архивного делопроизводства.
7. приказ ГЛАВАРХИВа СССР №33 от 25 мая 1988г. «Государственная система документационного обеспечения управления»;
8. Основные правила работы государственных архивов Российской Федерации/ Росархив. ВНИИДАД. – М.: Российская политическая энциклопедия (РОССПЕН), 2002. – 304с.

ОЦЕНКА ПАРАМЕТРОВ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНТЕРЕСАХ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К КОМПЛЕКСНЫМ СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ

Головина И.С. – студентка гр. КЗОИ-11
Козлова С.Б. – студентка гр. КЗОИ-51
Загинайлов Ю.Н. –доцент. каф. ЗИРСС

Среди современных проблем проектирования комплексных систем защиты информации на объектах информатизации предприятия актуальной является проблема, связанная с выделением и оценкой объектов защиты с целью определения требований к системе защиты, которые невозможно определить без оценки параметров защищаемой информации. Параметры защищаемой информации определяют среду безопасности объекта информатизации, а их оценка позволяет перейти к анализу угроз безопасности информации и формированию требований к комплексной системе защиты информации. Параметром, на основе которого в настоящее время формируются требования к защите, является важность информации. Однако этот параметр был определён в начале 90-х годов XX века в нормативных документах Гостехкомиссии России [1], где под важностью понималась условно определяемая степень секретности (конфиденциальности) информации. Поэтому основной целью защиты определялась защита информации от несанкционированного доступа в интересах обеспечения конфиденциальности. Кроме этого, перечень требований ориентирован только на автоматизированные системы, не включает других аспектов, связанных с комплексной защитой.

Новые реальности, связанные с развитием в России института авторского права, и, в частности, введением в 2004-2006 годах правовых норм предусматривающих защиту объектов авторского права с использованием технических устройств [2], коммерческой тайны [3], а также необходимость использования для формирования требований к безопасности информационных технологий международных стандартов [4], рассматривающих в качестве целей защиты не только обеспечение конфиденциальности, но и таких показателей как целостность и доступность, вызывают необходимость исследования взаимосвязи и влияния традиционных параметров информации определяющих её ценность (например: адекватность, толерантность) с такими параметрами безопасности как конфиденциальность, целостность, доступность. Эти факторы определяют новизну исследования.

С учётом актуальности и новизны, задачей исследования является установление взаимосвязи параметров (характеристик) информации с параметрами её безопасности,

определение показателей взаимного влияния, и соотнесения показателей параметров с уровнями типовых требований к системам комплексной защиты информации на объектах информатизации.

Результаты анализа взаимосвязи показателей информации с показателями безопасности и соответствующими им целями защиты приведена в таблице 1.

Таблица 1. Взаимосвязь показателей информации с целями её защиты

Показатель информации	Цели защиты информации		
	Конфиденциальность	Целостность	Доступность
Важность	+	+	+
Полнота	-	+	-
Адекватность	-	+	-
Релевантность	-	+	-
Толерантность	-	+	-
Объём	-	+	+
Способ кодирования	-	-	+

Степень влияния может быть оценена по трём уровням с использованием лингвистических переменных [5]: определяющая, существенная, второстепенная. Основным критерием такого деления должна служить цель, для достижения которой осуществляется защита информации.

Как показало исследование, определяющими показателями для формирования требований к системе защиты информации следует считать:

- при обеспечении конфиденциальности: важность,
- при обеспечении целостности: важность, полнота, адекватность, релевантность, толерантность, объём;
- при обеспечении доступности: важность, адекватность, релевантность, объём.

Требуемый уровень защиты при необходимости может быть скорректирован с учётом значения существенных показателей. Значения второстепенных показателей при этом могут игнорироваться.

Требования к системам защиты информации, определённые в Руководящих документах Гостехкомиссии России [1] для автоматизированных систем, которые являются основным типом объекта информатизации, систематизированы и сгруппированы по 5 уровням и соответствующих им 5 классам автоматизированных систем (классы 1А, 1Б,1В,1Г,1Д). В проектах новых Руководящих документов ФСТЭК, технических регламентах по безопасности информационных технологий, которые планируется принять в России в качестве федеральных законов, количество уровней сохранилось. Поскольку в интересах экономической эффективности проектирование комплексных систем защиты информации целесообразно осуществлять по типовым вариантам, тогда методология оценки показателей информации на объекте информатизации в интересах выбора типового класса, должна предусматривать определённую шкалу для ранжирования показателей на 5 уровней.

На основе существующей методологии определения важности информации [5], при определении требований к защите информации в целях сохранения её конфиденциальности, предложен подход при котором защищаемая информация (информационные ресурсы) шкалируются по 5-ти уровням важности, а условная шкала соответствует грифам конфиденциальности. Соответствие показателей важности грифам конфиденциальности и классам типовых автоматизированных систем приведено в таблице 2.

Таблица 2. Взаимосвязь показателей важности информации с классами требований по защите АС

Показатели важности			Степень конфиденциальности		Типовой класс АС
Ценность	Обозначение	Наименование	Для организаций с государственной формой собственности	Для организаций с негосударственной формой собственности	
С5	А	Чрезвычайная важность	Особой важности	Особо конфиденциально	1А
С4	Б	Большая важность	Совершенно секретно	Совершенно конфиденциально	1Б
С3	В	Повышенная важность	Секретно	Конфиденциально	1В
С2	Г	Средняя важность	Для служебного пользования	Конфиденциально для офиса	1Г
С1	Д	Малая важность	Объект интеллектуальной собственности без образования тайны		1Д

Аналогичный подход применён к требованиям обеспечения целостности информации. Однако отсутствие типовых требований и классов, где главной целью защиты является обеспечение целостности, вызывает необходимость разработки соответствующих профилей защиты с набором функций безопасности различных уровней, в зависимости от ценности защищаемой информации. Обсуждение вопросов взаимосвязи параметров информации, их показателей и взаимосвязи с целями защиты обсуждались в рамках выполнения и защиты курсовой работы по специальному курсу информатики. Определение важности и ценности информации, грифы конфиденциальности и формирование на их основе требований к системам защиты обсуждались при выполнении и защите курсовой работы по курсу «Комплексные системы защиты информации на предприятии».

Практическое значение работы заключается в формировании подхода к оценке информационных ресурсов и систем позволяющих на основе ценности или важности информации проектировать и внедрять используя типовые технологии экономически обоснованную систему защиты.

Литература

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992. 39с.
2. Федеральный Закон РФ от 29.07.2004г. №98-ФЗ «О коммерческой тайне».
3. Закон РФ от 9 июля 1993 г. N 5351-I "Об авторском праве и смежных правах" (с изменениями от 19 июля 1995 г., 20 июля 2004 г.).
4. ГОСТ Р ИСО\МЭК 15408 -2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. ИПК: Издательство стандартов, 2002. – 35с.

5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб.пос для вузов.-М: Горячая линия-Телеком, 2004.-280с.

ПУТИ РАЗВИТИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Киселев Н.О. – студент гр.КЗОИ-41
Загинайлов Ю.Н. –- доцент каф. ЗИРСС

Информационная безопасность не может быть целью деятельности организации, а потому не имеет самостоятельного значения, но она является одним из мощнейших инструментов, который при правильном использовании может оказывать существенную поддержку бизнесу или деятельности организации. Кроме того, очень остро стоят вопросы обеспечения защиты ключевых объектов информационной и телекоммуникационной инфраструктуры Российской Федерации.

Одним из направлений, позволяющих оценить уровень обеспечения информационной безопасности, является аудит информационной безопасности. Поэтому формирование взглядов на аудит информационной безопасности в России является актуальной задачей, для решения которой необходимо во-первых оценить уровень обеспечения информационной безопасности, и, в частности, аудита в РФ. Затем должны быть проанализированы системы аудита в других областях деятельности, на основе которых может быть сформирована система взглядов на аудит информационной безопасности в России, после чего уже могут быть определены пути развития аудита информационной безопасности, как одна из важных составляющих обеспечения информационной безопасности.

В настоящее время в Российской Федерации имеется определенный опыт проведения оценки (аттестации) по требованиям защиты информации, в частности, аттестации объектов информатизации и автоматизированных систем. При этом технология контроля (оценки) защищенности информации, принятая в Российской Федерации, основанная на базе Руководящих документов Гостехкомиссии России 1992-1993 г.г., существенно отличается от технологий, применяемых в настоящее время в международной практике [1,2,3]. Этот факт, а также необходимость интеграции с международными системами безопасности и проблема международного признания результатов контроля (оценки) состояния информационной безопасности в российских организациях вызывает серьезные трудности применения существующих в настоящее время в Российской Федерации подходов к оценке информационной безопасности организаций и системы информационных технологий. Необходимо выработать и принять единую согласованную систему взглядов, которая определила бы направления развития и регулирования деятельности по аудиту информационной безопасности в Российской Федерации, включая единство методологии его проведения.

Сегодня в Российской Федерации действует ряд документов, регулирующих аудиторскую деятельность [1,4], которая, однако, направлена на оценку достоверности финансовой отчетности или же на проведение сертификационного аудита (ИСО 9000, ИСО 14000) и не содержат принципов и критериев аудита информационной безопасности. Однако они могут быть взяты за основу для формирования подходов по аудиту информационной безопасности.

Тогда на основе метода аналогий, система взглядов на аудит информационной безопасности должна включать следующие положения.

Аудит информационной безопасности организации должен быть определен как систематический, независимый и документированный процесс для получения свидетельств

аудита информационной безопасности и объективного их оценивания с целью установления степени выполнения критериев аудита.

По содержанию, аудит информационной безопасности может быть разделен на два вида: аудит информационной безопасности организации и аудит информационной безопасности систем информационных технологий организации, причем последний может проводится как самостоятельно, так и быть частью аудита организации.

По форме аудит информационной безопасности может быть внутренним и внешним, т.е. проводиться самой организацией для внутренних целей, либо независимыми коммерческими организациями в соответствии с нормативно – правовыми актами Российской Федерации.

К основным принципам аудита применительно к области информационной безопасности можно отнести независимость и полноту аудита, компетентность и этичность лиц и организаций, проводящих аудит.

Немаловажным при проведении аудита информационной безопасности организации является понимание аудитором деятельности проверяемой организации для того, чтобы он мог правильно оценивать события и процессы в информационной среде и трактовать их применительно к информационной безопасности организации.

Для проведения аудита информационной безопасности должна быть заранее определена система критериев, отраженная в нормативных документах (регламентах и/или стандартах) и действующая в отношении аудируемой организации.

Общение аудиторской организации с представителями проверяемой организации должно осуществляться как в устной форме во время посещения проверяемой организации сотрудниками аудиторской организации, так и в письменной форме путем направления аудиторской организацией запросов и других материалов на имя руководства (представителей) проверяемой организации.

Все вышеприведенные взгляды на аудит информационной безопасности в России должны быть закреплены на государственном уровне. Поэтому первоочередными мероприятиями по обеспечению аудиторской деятельности в области информационной безопасности в Российской Федерации, должны стать [5]:

- принятие концепции аудита информационной безопасности;
- разработка и введение в действие дополнений к Закону РФ «Об аудиторской деятельности» применительно к рассматриваемой отрасли;
- разработка нормативно - методической документации процедурного плана по аудиту информационной безопасности Федеральной службой по техническому и экспортному контролю [6];
- разработка и введение в действие на территории Российской Федерации стандартов аудита информационной безопасности, определяющих критерии аудита и положения по их оценке.

Литература

1. Федеральный закон от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании».
2. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.
3. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
4. Федеральный закон «Об аудиторской деятельности» №119-ФЗ от 7 августа 2001 г.

5. Проект концепции аудита информационной безопасности систем информационных технологий и организаций - ГНИИИ ПТЗИ Гостехкомиссии России. http://www.fstec.ru/_razd/_info.htm.
6. Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента РФ от 16 августа 2004 г. N 1085.

СИНТЕЗ БЕЗОПАСНОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ НА УРОВНЕ АРХИТЕКТУРЫ И ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ

Ефименко К.Н. – студент гр. КЗОИ-51
Белов В.М. – проф. каф. ЗИРСС

Развитие Internet, популяризация обработки данных оказали существенное влияние на разработку защищенных систем. Развитие сетевых технологий в 90-ые годы привело к появлению большого числа сетевых компонентов. Системы, прошедшие сертификацию без учета требований к сетевому программному обеспечению, в настоящее время часто используются в сетевом окружении и даже подключаются к Internet. Однако, это приводит к появлению изъянов и уязвимостей, не обнаруженных при сертификации защищенных вычислительных систем. Классическим примером, иллюстрирующим данную проблему, являются многочисленные атаки на популярную операционную систему Windows NT через сетевые компоненты этой системы [1].

В 90-ые годы при проектировании защищенных систем происходит переход от модульной архитектуры к микроядерной. Использование микроядерной архитектуры не только облегчает перенос ОС на различные аппаратные платформы, но и позволяет проводить доказательство безопасности системы с применением формальных механизмов [2]. Однако функциональные требования к безопасной операционной системе остаются за пределами исследований. Поэтому синтез безопасной информационной системы на уровне архитектуры и функциональных требований представляет актуальный вопрос теории и практики безопасности информационных технологий и требует решения.

Для решения этой задачи были определены частные задачи исследования:

- анализ создания и развития безопасных операционных систем;
- анализ недостатков и достоинств операционных систем;
- архитектура безопасной операционной системы;
- определений функциональных требований для безопасной операционной системы.

Опыт построения защищенных систем обработки информации позволяет выделить две возможные технологии, на основе которых могут быть спроектированы защищенные системы, претендующие на сертификацию в соответствии с требованиями стандартов безопасности информационных технологий:

1. Проектирование защищенной системы «с нуля». В этом случае безопасность является одной из главных целей разработчиков системы. Данный подход характеризуется тем, что система разрабатывается как единое целое, начиная (хотя это не обязательно) от аппаратной части и операционной системы и до приложений пользователя.

Однако, вследствие своей трудоемкости данный подход преимущественно применяется производителями, обладающими значительными материальными ресурсами, или поставляющими собственное аппаратное обеспечение.

2. Доработка существующей системы. Данный подход состоит в улучшении характеристик некоторой системы-прототипа и доработка ее защиты до требуемого уровня. Минимальное требование к базовой системе – обеспечение поддержку защиты функций на аппаратном уровне, например разделение системных и прикладных программ. В этом случае

разработчики существенно ограничены необходимостью совместимости своих продуктов с прототипом, а также функциональными возможностями исходной системы.

Несмотря на то что этот подход характеризуется значительно меньшими затратами, попытки внести защиту в незащищенную систему испытывают серьезные трудности, что подтверждается многочисленными провалами попыток доработки операционных систем, неудовлетворяющих требованиям защиты, таких как MS Windows 3.11 и 95 и Novell Netware3.x.

Для того чтобы быть сертифицированными в соответствии с требованиями современных стандартов безопасности информационных технологий [4] системы должны отвечать как соответствующим требованиям защиты, так и общим функциональным требованиям, которые также существенно влияют на принципы построения защищенных систем. Ведь защищенные системы, как и все остальные современные средства обработки информации, должны быть в зависимости от назначения: многопользовательскими, многозадачными, надежными и масштабируемыми, работать в гетерогенных сетях. В последнее время к системам обработки информации было предъявлено требование распределенной архитектуры. В связи с развитием Internet возрастает значение требований для глобальных распределенных систем.

В связи с тем, что в ходе сертификации защищенные операционные системы подвергаются формальному анализу, подобные системы должны разрабатываться с использованием технологий иерархического и модульного проектирования.

На сегодняшний день самый передовой метод построения защиты операционной системы – технологии микроядра. В отличии от традиционной архитектуры, согласно которой операционная система представляет собой монолитное ядро, реализующее основные функции по управлению аппаратными ресурсами и организующее среду для выполнения пользовательских процессов, микроядерная архитектура распределяет функции операционной системы между микроядром и входящими в состав ОС системными сервисами, реализованными в виде процессов, равноправных с пользовательскими приложениями.

Микроядро реализует базовые функции операционной системы, на которые опираются эти системные сервисы и приложения. В результате, такие важные компоненты ОС как файловая система, сетевая поддержка и т.д. превращаются в по-настоящему независимые модули, которые функционируют как отдельные процессы и взаимодействуют с ядром и друг с другом на общих основаниях. Это означает, что имевшее раньше место четкое разделение программного обеспечения на системные и прикладные программы размывается, т.к. фактически, между процессами, реализующими функции ОС, и прикладными процессами, выполняющими программы пользователя, нет никаких различий. Все компоненты системы используют средства микроядра для обмена сообщениями, но взаимодействуют непосредственно. Микроядро лишь проверяет законность сообщений, пересылает их между компонентами и обеспечивает доступ к аппаратуре.

Другое нововведение в технологии построения ОС, связанное с исключительно с внедрением технологии микроядра, это организация взаимодействий между процессами и ядром с помощью универсального механизма передачи информации – обмена сообщениями, пришедшему на смену технике системных вызовов. При этом десятки или даже сотни вызовов, различающихся числом и типом параметров, можно заменить несколькими типами сообщений, которые содержат компактные порции информации, могут передаваться от одного обработчика к другому.

На современном этапе развития ОС эта технология является самой перспективной, т.к. позволяет преодолеть самые существенные недостатки существующих систем – отсутствие мобильности, громоздкость, ресурсоемкость. Реализация многих традиционных функций ОС за пределами ядра способствует построению на базе этого ядра операционных систем с неожиданным ранее уровнем модульности и расширяемости.

Основные положения архитектуры микроядерных ОС:

1. Минимизация набора функций, поддерживаемых микроядром, и реализация традиционных функций ОС (файловая система, сетевая поддержка) вне микроядра.
2. Организация синхронного и асинхронного взаимодействия между процессами исключительно через механизм обмена сообщениями.
3. Все отношения между компонентами строятся на основе модели клиент-серверов.
4. Применение объектно-ориентированного подхода при разработке архитектуры и программировании системы.

Исследования показали, что функциональные требования могут быть представлены функциями безопасности определёнными в базовом профиле защиты безопасных информационных технологий [5].

Операционная система должна удовлетворять следующим минимальным функциональным требованиям:

1. Аудит безопасности.
2. Защита данных пользователя.
3. Идентификация и аутентификация.
4. Управление безопасностью.
5. Защита функций безопасности объекта оценки.
6. Использование ресурсов.
7. Доступ к объекту оценки.

Аудит безопасности должен включать: автоматическую реакцию аудита безопасности, генерацию данных аудита безопасности, анализ аудита безопасности, просмотр аудита безопасности, выбор событий аудита безопасности, хранение данных аудита безопасности.

Криптографическая поддержка включает в себя: управление криптографическими ключами, криптографические операции [6].

Защита данных должна: политику управления доступом, функции управления доступом, экспорт данных за пределы действий функций безопасности объекта оценки(ФБО), политику управления информационными потоками, импорт данных из-за пределов действий ФБО, передачу в пределах объекта оценки, защиту остаточной информации.

Идентификация и аутенфикация должны включать: отказы аутентификации, определение атрибутов пользователя, спецификацию секретов, аутентификацию пользователя, идентификацию пользователя, связывание пользователь-субъект.

Управление безопасностью должно включать: управление отдельными функциями ФБО, управление атрибутами безопасности, управление данными ФБО, отмену, срок действия атрибута безопасности, роли управления безопасностью.

Защита ФБО должна включать: тестирование базовой абстрактной машины, передачу данных ФБО в пределах объекта оценки, надежное восстановление, посредничество при обращениях, разделение домена, метки времени, согласованность данных ФБО между ФБО, согласованность данных ФБО при дублировании в пределах объекта оценки, самотестирование ФБО.

Защищенная операционная система должна лежать в основе каждой системы обработки информации, которая претендует на безопасность, потому что в операционной системе сосредоточены все базовые механизмы, которые, в конечном счете, определяют границы возможностей системы.

Материалы исследования обсуждались в рамках защиты курсовой работы по специальному курсу информатики на кафедре ЗИРСС АлтГТУ.

Литература

1. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем .- М.: Горячая линия-Телеком, 2000.452 с.
2. Раводин, О.М., Раводин В.О. Безопасность операционных систем. – Томск 2005, 86 с.
3. Столлингс В. Операционные системы.- М.: ВИЛЬЯМС, 2002.843 с.

4. ГОСТ Р ИСО\МЭК 15408 -2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч1-3. ИПК: Издательство стандартов, 2002.
5. Центр безопасности. Безопасность информационных технологий. Операционные системы. Базовый профиль защиты. http://www.fstec.ru/_razd/_info.htm.
6. Центр безопасности информации. Безопасность информационных технологий. Много-уровневые операционные системы. Профиль защиты. http://www.fstec.ru/_razd/_info.htm.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ СТУДЕНТОВ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ВУЗА

Русина Л.Ю. – студентка гр. КЗОИ-11
Загинайлов Ю.Н. – доцент каф. ЗИРСС

В современном демократическом обществе права человека и, в частности, право на неприкосновенность частной жизни имеют первостепенное значение. Особым институтом права на неприкосновенность частной жизни в условиях автоматизации и развития новых информационных технологий является институт персональных данных.

Закрепленные в Конституции РФ права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки на сегодняшний день практически не имеют достаточного правового, организационного и технического обеспечения. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ «Об информации, информатизации и защите информации», определяет персональные данные как категорию конфиденциальной информации, подлежащей защите. Нормативными документами Министерства образования и науки по защите информации [2] определены требования по защите персональных данных в автоматизированных системах вузов. В связи с внедрением в АлтГТУ автоматизированной информационной системы для обработки персональных данных студентов актуальной также стала задача обеспечения их безопасности в процессе сбора, обработки и хранения.

Проблема защиты персональных данных в вузе рассмотрена на примере Алтайского государственного технического университета имени И.И. Ползунова., а обеспечение безопасности персональных данных студентов в автоматизированных системах на примере ФИПИ.

В рамках научно-исследовательской работы были поставлены и решены следующие задачи:

- выполнен анализ персональных данных подлежащих защите в АИС;
- составлены перечни персональных данных для подразделений АлтГТУ, работающих с базами персональных данных;
- определены условия обработки и хранения персональных данных в подразделениях;
- определены требования по защите персональных данных;
- определен оптимальный состав и разработана структура нормативных документов по защите персональных данных в вузе;
- разработано «Положение о персональных данных в АлтГТУ» и «Перечень персональных данных».
- определены требования к подсистеме безопасности АСУ «Деканат» на факультете.
- определены средства защиты для реализации подсистемы безопасности АСУ «Деканат».

В ходе работы было выполнено теоретическое обоснование системы критериев, позволяющих оптимизировать состав и структуру нормативных документов по защите персональных данных для минимизации их количества и исключения повторения норм и правил в нескольких документах. Это в частности касается нового оригинального решения структуризации нормативных документов по трём уровням: концептуальный, процедурный, исполнительский, что соответствует современным международным стандартам в области управления качеством.

Проведенный анализ позволяет привести количество субъектов, чьи персональные данные подлежали обработке в 2004-2005 учебном году, их количество составило 20110.

В интересах комплексной защиты персональных данных студентов был произведен детальный анализ форм и условий хранения персональных данных на факультетах (на примере факультета инженерной педагогике и информатики) определен состав персональных данных и их наличие на объекте информатизации в интересах нормативного регулирования вопросов их защиты, определены требования безопасности хранения и обработки персональных данных на факультете.

На основе анализа условий разработаны «Положение о персональных данных в АлтГТУ» и «Перечень персональных данных».

«Положение о персональных данных в АлтГТУ» – это документ, регламентирующий деятельность подразделений, обрабатывающих персональные данные и определяющий требования по сбору, хранению, обработке и защите персональных данных в вузе. Оно включает в себя следующие разделы:

1. Общие положения.
2. Нормативные ссылки.
3. Понятия, используемые в Положении.
4. Персональные данные.
5. Действия держателя с персональными данными.
6. Обязанности держателя.
7. Обязанности субъекта.
8. Права субъекта.
9. Доступ к персональным данным.
10. Ответственность за неправомерные действия.

Требования к АИС определены на основе:

- Временного положения по защите информации при взаимодействии автоматизированных информационных систем Минобразования России [2];
- Руководящих документов Гостехкомиссии России [3,4];
- Специальных требований и рекомендаций по технической защите конфиденциальной информации, утверждённых Гостехкомиссией России [5].

В соответствии с положениями указанных нормативных документов АИС "Деканат" должна соответствовать классам АС 2Б или 1В в зависимости от условий обработки (уровней конфиденциальности информации и прав пользователей). В качестве системы защиты обеспечивающей защиту на уровне этих классов для АИС «Деканат» определен сертифицированный программно-аппаратный комплекс Secret Net 4.0 с электронным замком "Соболь".

Системы защиты информации семейства Secret Net комплектуются средствами аппаратной поддержки, предназначенными для идентификации пользователей до загрузки операционной системы по имени и паролю. Использование аппаратной поддержки обеспечивает также возможность запрета несанкционированной загрузки ОС с гибкого диска.

В соответствии с сертификатами, выданными Государственной технической комиссией при Президенте России, система разграничения доступа Secret Net 4.0, является программно-аппаратным средством защиты от несанкционированного доступа к информации и соответствует требованиям Руководящего документа Гостехкомиссии России "Средства вычислительной техники. Защита от несанкционированного доступа к информации". Показатели защищенности от несанкционированного доступа к информации" по третьему классу защищенности, что позволяет создать на ее базе автоматизированную систему в защищенном исполнении класса 2Б или 1В и обеспечить требуемый нормативными документами уровень защищенности персональных данных в АИС.

Следующим этапом развития является разработка нормативно-методического обеспечения для эксплуатации АИС "Деканат" в защищенном исполнении и последующая аттестация автоматизированной системы в защищенном исполнении по требованиям безопасности.

Литература

1. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ «Об информации, информатизации и защите информации».
2. «Временное положение по защите информации при взаимодействии автоматизированных информационных систем Минобразования России». М.: Министерство образования России, 1999.
3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России, М.:ГТК РФ, 1992. 25с.
4. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992. -39с.
5. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К.), М.: ГТК РФ, 2001. -22с.

АНАЛИЗ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ ВУЗАМИ

Комарова Г.Н. – студентка гр. КЗОИ-21
Баташов М.В. – ст. преп. каф. ЗИРСС

В настоящее время влияние рынка сильно сказывается на системе высшего образования России. Получив новые обязанности и свободы, вузы создают новые структуры, которые необходимы для управления в конкурентной среде. Вузы корректируют стратегические цели деятельности и вносят необходимые изменения в организационную структуру. При этом появление новых задач и служб зачастую происходит стихийно. Поэтому новые подразделения иногда выходят плохо функционирующими и слабо структурированными [3].

Для того чтобы обеспечить конкурентоспособность вуза необходимо решать задачи управления на качественно новом, системном уровне. Важность быстрого реагирования на часто меняющуюся экономическую ситуацию требует перестройки микроэкономики вуза, постановки управленческого учета, оптимизации процессов управления. Отсутствие своевременной, актуальной и достоверной информации вынуждает руководителя принимать решения в условиях неопределенности и риска. Наличие информационной системы управления, четкая структура, налаженный документооборот и внутренняя отчетность позволяют принимать решения не вслепую, а на основе необходимой информации [4].

Структура развивающегося вуза должна быть жизнеспособной, гибкой и динамичной. В этой связи актуальна разработка научно-обоснованной структуры управления образовательным процессом, которая эффективно функционирует в условиях открытого информационно-образовательного пространства, обеспечивает лёгкость доступа к изучаемой информации и конкурентоспособность выпускников на рынке труда. Для решения данной проблемы предлагается [3] проведение комплекса работ:

– сбор данных о характеристиках и взаимосвязях элементов структуры в системе управления деятельностью вуза;

– анализ эффективности функционирования различных типов структур, определение степени управленческого и информационного дублирования, влияния структуры каждого типа на качество учебного процесса;

– определение направлений повышения эффективности структуры управления образовательным процессом в вузе;

– разработка формализованной схемы решения задачи выбора эффективной структуры управления образовательным процессом в вузе;

– анализ и оценка эффективности выбранной структуры управления.

Приступая к решению такой задачи нужно четко оценить реальное состояние вуза, понять, в каком направлении он развивается.

В настоящее время еще не выработана структура типовой вузовской информационной системы. Средства и элементы технологии дистанционного обучения и открытого образования только начинают появляться в вузах, и поэтому информатизация управления преимущественно развивается применительно к традиционным технологиям обучения. По мере развития новых технологий будет изменяться состав и функциональное назначение автоматизированных систем управления в вузах.

Становится понятным, что требуется создание собственной системы управления вузом, которая будет решать как минимум следующие задачи [2]:

1. Декан факультета, основные функции:
   - создание и поддержка учебных планов по специальностям факультета;
   - контроль работы заместителей деканов и заведующих кафедрами;
   - распределение студентов по группам и закрепление за учебной группой “заместителя декана” (куратора);
   - допуск к обучению в семестре студентов, работа с должниками;
   - допуск к сессии студентов;
   - направление на отчисление студентов;
   - перевод студентов с курса на курс;
   - допуск к итоговой выпускной аттестации студентов.
2. Заместитель декана, основные функции:
   - Учет посещаемости студентами занятий;
   - Учет оплаты студентами обучения, а также прочих услуг и штрафы (при необходимости);
   - Выдача зачетных и экзаменационных ведомостей и индивидуальных разрешений студенту на сдачу / пересдачу контрольных точек, занесение результатов в систему;
   - Отметка о закрытии пропусков занятий соответствующей отработкой / оплатой студента;
   - Формирование документов работы ГАК и приложений к диплому.
3. Заведующий кафедрой, основные функции:
   - специализация преподавателей по разделам своих дисциплин с учетом проведения лекционных и практических занятий;
   - замена одного раздела на другой с сохранением кол-ва часов и структуры контрольных точек, с дальнейшим пересмотром в деканатах индивидуальных планов обучаемых для рабочих разделов;

- контроль наполнения учебного материала, вопросов для контрольных точек, наполнение базы данных часто задаваемых вопросов и перевод в состояние готовности своих дисциплин;
- планирование нагрузки преподавателей, осуществляющих преподавание по очным и заочным формам;
- ежемесячный учет фактической нагрузки преподавателей;
- контроль работы преподавателей.

4. Ведущий преподаватель, основные функции:
   - наполнение разделов лекционным материалом по своим дисциплинам;
   - наполнение вопросами и ответами контрольных точек разделов, создание сценариев тестирования, анализ степени сложности вопросов;
   - наполнение базы часто задаваемых вопросов по разделу.
5. Преподаватель:
   - оценка результата прохождения контрольных точек;
   - консультирует обучаемых;
   - формирует список часто задаваемых вопросов и ответов на них по своему разделу;
   - отслеживает процесс обучения прикрепленных студентов.

Проведенный анализ интегрированных систем обучения и управления (Аванта [6], Гекадем [5], Прометей [7]) привел к выводу о том, что таковыми они не являются. В связи с чем, возникла необходимость проведения работ в данном направлении.

Литература

1. Харашвили Анжелика Гурамовна. Формирование системы управления качеством принимаемых решений в ВУЗе.
2. http://www.tisbi.ru/, dao.tisbi.ru
3. Журнал «Менеджмент в России и за рубежом» №1 / 2004. Архипова Н.И. Совершенствование организационных структур управления как фактор стратегического развития вуза на современном этапе.
4. Гусакова Т.М. / Материалы второй научно-практической конференции «Использование информационно-коммуникационных технологий в образовании», Йошкар-Ола, 2005 г.
5. http://www.gekadem.ru
6. http://www.avanta.ru
7. http://www.prometeus.ru