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

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЮРИСПРУДЕНЦИИ

Барнаул – 2006

84(2 Рос 537)638.1

3-я Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых "Наука и молодежь". Секция «Информационные технологии». Подсекция «Информационные технологии в юриспруденции». / Алт.гос.техн.ун-т им. И.И.Ползунова. – Барнаул: изд-во АлтГТУ, 2006. – 29 с.

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

Организационный комитет конференции:
Максименко А.А., проректор по НИР – председатель, Марков А.М., зам. проректора по НИР – зам. председателя, Арзамарсова А.А. инженер Центра НИРС и молодых учёных – секретарь оргкомитета, Кантор С.А., заведующий кафедрой «Прикладная математика» АлтГТУ – руководитель секции, Астахова А.В, заведующая кафедрой «Прикладная информатика в юриспруденции» ААЭП – руководитель подсекции, Балашов А.В. – редактор.

СОДЕРЖАНИЕ

ОПЫТ АВТОМАТИЗАЦИИ ДЕЛОПРОИЗВОДСТВА ПРОКУРАТУРЫ

Катунин Ю.В. – студент гр. ПОВТ-11
Жарикова Т.А. – помощник прокурора
Индустриального района г.Барнаул
Астахова А.В. – проф. каф. ПИЮ ААЭП

Работа, представленная в данном докладе, выполнялась по заявке прокуратуры Индустриального района г. Барнаула.

Разрабатываемое программное обеспечение (ПО) предназначено для ведения делопроизводства помощником прокурора. ПО отвечает следующим требованиям:

1. Создание единой информационной базы данных о работе надзора в рамках районной прокуратуры.
2. Наличие возможности одновременной работы нескольких помощников с одной и той же информацией.
3. Наличие удобной системы и интерфейса пополнения/изменения информационной базы, т.е. внесение данных в следующих разрезах:
   - по жалобам;
   - по заявителям;
   - по проверкам решений по уголовным делам;
   - по проверкам решений по материалам доследственной проверки;
   - по проведенным проверкам исполнения законодательства, обобщениям следственной и судебной практики;
   - по результатам проверки заявлений в порядке ст. 144 УПК РФ;
   - по внесенным представлениям и результатам их рассмотрения (отсроченных друг от друга по времени);
   - по лицам, в отношении которых осуществляется уголовное преследование органами данного района (подсудимых);
   - о судье, рассматривающем то или иное уголовное дело;
   - по лицам, в отношении которых избрана мера пресечения в виде заключения под стражу;
   - по результатам судебного рассмотрения уголовных дел и пр.
4. Возможность формирования запроса к базе по большому количеству ключевых положений поиска одновременно (номер уголовного дела, материала проверки, надзорного производства, фамилия заявителя, номер статьи Уголовного кодекса и т.п.)
5. Создание следующих запросов для помощника прокурора:
   - о количестве разрешенных жалоб и обращений граждан и организаций за определенный период времени;
   - о количестве разрешенных жалоб, которые удовлетворены, отказано в удовлетворении за определенный период времени;
   - о количестве разрешенных жалоб и обращений, разрешение которых относится к компетенции определенного отдела по надзору;
   - о количестве мер прокурорского реагирования по жалобам и обращениям с разбивкой по видам за определенный период времени;
   - о количестве возбужденных уголовных дел с указанием статей УК РФ, по признакам которых они возбуждены, за определенный период времени;
   - о количестве уголовных дел, по которым принято решение об отмене постановления о приостановлении/ прекращении уголовного дела, за определенный период времени;
   - о внесенных и рассмотренных представлениях;
   - о лицах, взятых под стражу и осужденных/ отпущенных.

6. Создание ежемесячных, полугодовых и годовых отчетов для каждого помощника прокурора и по прокурорскому надзору в целом.

В результате обследования названной выше предметной области выявлены также следующие регистрационные журналы, в которых учитываются поступающие для анализа и изучения материалы и итоги деятельности по надзору за органами дознания и предварительного следствия:

1. Журнал учета отмен по приостановленным уголовным делам.
2. Журнал учета отмен по прекращенным уголовным делам.
3. Журнал учета отмен по доследственным материалам проверок.
4. Журнал учета указаний в порядке ст. 37 УПК РФ.
5. Журнал учета представлений.
6. Журнал учета отмен по материалам доследственных проверок следователей прокуратуры.
7. Журнал учета лиц, задержанных в порядке ст. 91 УПК РФ.

ПО учитывает также журналы, проходящие через канцелярию:

1. Журнал уголовных дел.
2. Журнал КУС (книга учета сообщений и заявлений о совершенных преступлениях).
3. Журнал заявителей.
4. Алфавитная книга.

Сформированная БД позволяет формировать следующие основные отчеты, которые составляются в прокуратуре:

1. Ежемесячные (на каждом надзоре).
2. Ежеквартальные (на каждом надзоре).
3. Полугодовой (по прокуратуре).
4. Годовой (по прокуратуре).

Разработанное программное обеспечение проходит в настоящее время экспериментальную проверку.

ОПЫТ РАЗРАБОТКИ И ВНЕДРЕНИЯ АРМ ЮРИСТА ОТДЕЛА КАДРОВ

Шамне А.А. – студент гр. ПОВТ-11
Астахова А.В. – проф. каф. ПИЮ ААЭП

Автор доклада анализирует пакеты прикладных программ «Босс-Кадровик» и «Кадры», ориентированные, прежде всего на точное следование существующим нормативно-правовым актам и другим предписаниям относительно деятельности кадровых служб, действующим на территории РФ. Результаты анализа позволили предложить на уровне предприятий типовую систему «Кадры», разработанную с учетом требований оперативной работы кадровых служб.

Предлагается программный интерфейс для конвертирования данных из базы данных (БД) системы «Босс-Кадровик» в БД системы «Кадры». Программное обеспечение доработано автором доклада с учетом работы с приказами, которые по некоторым организационным причинам оказались ошибочно введенными в БД.

Новый вариант системы учета кадров предусматривает также обеспечение информационной увязки с системой 1С версии «Зарплата и Кадры».

Разработанные проектные предложения и их программная реализация прошли этапы опытной эксплуатации и промышленного внедрения в нескольких кадровых службах г. Барнаула в рамках плановой деятельности ООО «Корпоративные системы».

Описанная система работает на основе СУБД Microsoft SQL Server 2000. Рекомендуется объем ОЗУ 256 Мб, процессор – не ниже 500 МГц.

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И ПРАВОВЫЕ МЕТОДЫ ИХ РЕГУЛИРОВАНИЯ

Мочалова Е.Б. – студентка гр. ПИЮ-322 ААЭП
Астахова А.В. – проф. каф. ПИЮ ААЭП

Защита информации в компьютерных системах одна из самых актуальных проблем в современном информационном обществе. Появление в уголовном кодексе главы 28 «Преступления в сфере компьютерной информации» ставит перед юристами задачу раскрытия и расследования этого вида преступлений. Неизбежным следствием появления новых общественных отношений стали правонарушения в сфере компьютерной информации, в том числе и в форме преступлений, которые представляют реальную угрозу для нормального развития и течения общественной жизни. Необходимость установления уголовной ответственности за причинения вреда в связи с использованием именно компьютерной информации вызвана повышенной уязвимостью ее по сравнению, например, с информацией зафиксированной на бумаге и хранящейся в сейфе.

В России компьютерная преступность имеет высокую степень латентности в связи с общей криминогенной обстановкой и отсутствием до недавнего времени соответствующих норм уголовного законодательства, а также специфичностью самой компьютерной сферы, требующей специальных познаний.

Остановимся на трех аспектах уголовно-правовой характеристики компьютерных преступлений.

Первый аспект «Объективные признаки компьютерных преступлений». Признаки объективной стороны применительно к каждому из составов преступлений перечислены в Главе 28 УК РФ. До настоящего времени наряду с дискуссионностью вопросов классификации компьютерных преступлений, дискуссионными остаются вопросы об объекте преступного посягательства и множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны. Кроме того, компьютерные преступления, посягая на основной объект, всегда посягают и на дополнительный объект, поскольку поражаются блага конкретного свойства: личные права и неприкосновенность частной сферы, имущественные права и интересы, общественную и государственную безопасность, конституционный строй. Эти подлежащие правовой охране интересы личности, общества и государства являются дополнительным объектом посягательства компьютерных преступлений. В качестве решения данной проблемы предлагается внести изменения в УК РФ, заключающиеся в расширении перечня способов совершения компьютерных преступлений, закрепленных непосредственно в Уголовном законе.

Второй аспект рассматриваемого вопроса «Субъективные признаки компьютерных преступлений» требует анализа субъекта и субъективной стороны составов преступлений, устанавливающих уголовную ответственность за компьютерные преступления. Согласно действующему законодательству по охране общественных отношений в сфере компьютерной информации, мотив и цели таких преступлений не являются обязательными признаками при квалификации деяний. Однако их необходимо выяснять т.к. мотивы и цели неправомерного доступа к компьютерной информации имеют существенное значение для правильного определения объекта преступного посягательства, разграничения смежных составов. Отсутствие в уголовном законе прямого указания на обязательность анализа мотивов компьютерных преступлений правомерно расценивать как пробел в законодательстве.

Третий аспект уголовно-правовой характеристики компьютерных преступлений «Спорные вопросы квалификации компьютерных преступлений». При квалификации необходимо наряду с умыслом, учитывать последствия преступления, в зависимости от которых, следует решать вопрос о вменении лицу вместе со ст.273 УК РФ соответствующей статьи Особенной части УК РФ.

Для решения данных задач, необходимо, прежде всего, обратить внимание на недочёты Российского законодательства, которые заключаются в том, что деяния лица, осуществляющего неправомерный доступ к компьютерной информации для совершения других преступлений, должны квалифицироваться по совокупности преступлений, а в УК РФ, в настоящее время не существует специальных норм, предусматривающих ответственность за преступления, совершенные с использованием компьютера либо иных высоких технологий. В качестве мер, направленных на совершенствование Уголовного кодекса, можно предложить создание таких специальных норм, по аналогии с зарубежным законодательством, которые помогут решить либо значительно снизить остроту проблемы разграничения компьютерных преступлений и преступлений с использованием компьютера и иных высоких технологий.

Литература

1. Закон РФ «Об информации, информатизации и защите информатизации», вступивший в действие с 22 февраля 1995г.
2. Закон РФ от 23 сентября 1992г. «О правовой охране программ для электронных вычислительных машин и баз данных».
3. Закон РФ от 9 июля 1993г. «Об авторском праве и смежных правах».
4. Закон РФ от 21 июля 1993г. «О государственной тайне».
5. Федеральный закон РФ от 16 февраля 1995г. № 15-ФЗ «О связи».

АВТОРСКО-ПРАВОВАЯ ОХРАНА ПРОГРАММ ДЛЯ ЭВМ

Петрушенко А.В. – студент гр. ПИЮ-322 ААЭП
Беспалова Е.Э. – ст. преп. каф. ПИЮ ААЭП

В настоящее время в России, как и во всех развитых странах, правовая охрана программ для ЭВМ и баз данных (БД) осуществляется с помощью норм авторского права. При этом с точки зрения права программы для ЭВМ приравнены к литературным произведениям, а БД к сборникам (энциклопедии, антологии). Авторско-правовая охрана программ для ЭВМ и БД имеет как достоинства, благодаря которым ей и было отдано предпочтение во всем мире, так и недостатки, в определенной степени компенсируемые применением норм других институтов права.

Под действие авторско-правовой охраны подпадает любая программа для ЭВМ или БД, созданная в результате творческого труда, независимо от ее назначения, достоинств и степени работоспособности [ст. 3. Закон РФ от 23 сентября 1992 г. N 3523-I "О правовой охране программ для электронных вычислительных машин и баз данных" (с изменениями от 24 декабря 2002 г., 2 ноября 2004 г.)]. Однако не следует забывать про недостатки авторско-правовой охраны программ для ЭВМ и БД. Основные из них – невозможность защитить от заимствования идеи и принципы, заложенные в основу программы для ЭВМ или БД (которые часто представляют собой достаточно ценную часть произведения), а также обеспечить эффективную защиту подобной программы от небуквального копирования. Указанные недостатки в определенной степени компенсируются применением норм патентного права и режима коммерческой тайны к конкретным объектам.

В нашей стране программы для ЭВМ и БД впервые получили правовую охрану в 1991 году, когда они были отнесены «Основами гражданского законодательства» (ст. 134) к объектам авторского права. Затем был принят Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» (далее – Закон о ПрЭВМ и БД), вступивший в силу с 20 октября 1992 года. В нем указывалось (ст. 2), что программы для

ЭВМ и БД являются объектами авторского права как литературные произведения и сборники, соответственно. Аналогичная норма нашла свое отражение в ст. 7 Закона РФ «Об авторском праве и смежных правах» (далее – Закон об АП и СП), который начал действовать с августа 1993 года и фактически поглотил принятый ранее Закон о ПрЭВМ и БД. Согласно п. 6 Постановления Верховного Совета Российской Федерации о порядке введения в действие Закона Российской Федерации об авторском праве и смежных правах от 9 июля 1993 года (ВВС №32, ст. 1244) законодательства бывшего СССР и Российской Федерации, существовавшие до вступления в силу Закона об АП и СП, применимы постольку, поскольку они не противоречат указанному закону. В июле 1995года в Закон об АП и СП были внесены изменения, и в настоящее время он действует в редакции от 20 июля 2004 года.

В российском законодательстве используется следующее определение программы для ЭВМ [п. 1 ст. 1 Закон о ПрЭВМ и БД]: «Программа для ЭВМ – это объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения».

Также дано определение база данных [п. 1 ст. 1 Закон о ПрЭВМ и БД]: «База данных - это объективная форма представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ»

Сторонами в отношениях, возникающих в связи с использованием компьютерных программ и БД, являются авторы, соавторы, правообладатели и пользователи.

Авторские права на программы для ЭВМ и базы данных представляют собой набор правомочий, установленных законом. В России это Закон о ПрЭВМ и БД и Закон об АП и СП. Авторское право на базу данных признается при условии соблюдения авторского права на каждое из произведений, включенных в эту БД.

Авторские права делятся на две группы. К первой относятся права, не имеющие экономического содержания,— это личные неимущественные права автора, или, как их еще называют, моральные права. Ко второй группе относятся имущественные права.

Закон РФ о ПрЭВМ и БД [ст. 9] относит к личным неимущественным правам следующие: право авторства; право на имя; право на неприкосновенность (целостность) произведения.

Действующий Закон об АП и СП предоставляет автору уже пять правомочий, относящихся к личным авторским правам. Два из них практически совпадают с приведенными выше, вместо права на неприкосновенность указано право на защиту репутации, а два оставшихся (в принципе, их можно считать единым правом) – это: право на обнародование; право на отзыв.

На практике при регулировании отношений, связанных с личными неимущественными правами, в соответствии с Постановлением ВС РФ о порядке введения в действие Закона об авторском праве и смежных правах от 9 июля 1993 года, следует руководствоваться перечнем правомочий, представленным в ст. 15 Закона об АП и СП.

Имущественные права на программу для ЭВМ и БД представляют собой совокупность правомочий, которые могут в полном объеме или частично (в период действия авторских прав) продаваться и покупаться, передаваться в дар, сдаваться в аренду и т.п. Следует помнить, что имущественные права имеют срочный характер: по истечении срока их действия (в течение жизни автора плюс пятьдесят лет после его смерти) они уже не принадлежат какому-либо конкретному лицу. Произведение становится общественным достоянием, и любому лицу позволяется свободно использовать его без выплаты авторского вознаграждения. В отличие от личных неимущественных прав имущественные права могут принадлежать как физическим, так и юридическим лицам.

В Законе о ПрЭВМ и БД (ст.10) к имущественным относятся права на осуществление или разрешение следующих действий: выпуск в свет программы для ЭВМ или базы данных; воспроизведение программы для ЭВМ или БД (полное или частичное) в любой форме, любыми способами; распространение программы для ЭВМ или БД; модификацию программы для ЭВМ или БД, в том числе ее перевод с одного языка на другой; иное использование программы для ЭВМ или БД.

Авторское право на программы для ЭВМ и БД действует с момента создания произведения в течение всей жизни автора и 50 лет после его смерти (считая с 1 января года, следующего за годом смерти автора) – в случае, если имя автора известно. Если же программа для ЭВМ или БД выпущена в свет анонимно или под псевдонимом и в течение 50 лет с момента ее опубликования имя автора не установлено однозначно, то авторское право на такое произведение действует с момента его выпуска в свет в течение 50 лет. Срок окончания действия авторского права на программу для ЭВМ или БД, созданную в соавторстве, исчисляется со времени смерти последнего автора, пережившего других соавторов. Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно.

Авторское право на произведение, впервые выпущенное в свет после смерти автора, действует в течение 50 лет после его опубликования. По окончании срока действия авторского права на программу для ЭВМ или БД она переходит в общественное достояние, что влечет за собой возможность ее свободного использования любым третьим лицом без выплаты авторского вознаграждения.

Программы для ЭВМ и БД подпадают под действие авторского права независимо от гражданства авторов и их правопреемников, если они находятся в какой-либо объективной форме на территории Российской Федерации. При этом не имеет значения, были они обнародованы или нет. Действие авторского права также распространяется на программы для ЭВМ и БД (обнародованные либо необнародованные), находящиеся в какой-либо объективной форме за пределами Российской Федерации, если их авторами или правопреемниками являются граждане Российской Федерации либо других государств, имеющих с Россией международные договоры об авторском праве.

Передача имущественных прав на произведение может осуществляться только на основании письменного договора, за исключением описанных выше случаев свободного воспроизведения и распространения законно приобретенного экземпляра. Договоры такого типа закон называет авторскими. Права могут передаваться полностью или частично, на основе авторского договора о передаче исключительных или неисключительных прав. Закон устанавливает определенные требования к авторскому договору; он должен устанавливать следующие существенные условия: объем и способы использования программ для ЭВМ или БД, порядок выплаты и размер вознаграждения, срок и территорию действия.

Любое, не санкционированное правообладателем использование программы для ЭВМ или БД, за исключением разрешенного законом, а также несоблюдение личных не имущественных прав авторов считается нарушением авторского права. Защита авторского права может осуществляться в рамках гражданского, уголовного и административного права.

По общему правилу защита авторских прав осуществляется в судебном порядке. Если хотя бы одна из участвующих в споре сторон – физическое лицо, то спор раз решается судами общей компетенции, если же обе стороны являются юридическими лицами – решения принимают арбитражные суды. По соглашению сторон спор между ними может быть передан на рассмотрение третейскому суду.

В качестве средства судебной защиты авторских прав выступает иск, в котором сторона, считающая, что ее права нарушены (истец), выдвигает свои требования к суду об отправлении правосудия, а также материально-правовые требования к стороне, по мнению истца нарушившей его право (к ответчику). Иск подается непосредственно в суд (обязательно в письменном виде) истцом или его представителем либо направляется в суд по почте, желательно заказным письмом с уведомлением о вручении.

За виновное нарушение авторских прав на программы для ЭВМ или БД, причинившее крупный ущерб, наступает уголовная ответственность. Уголовное дело может быть возбуждено по заявлению правообладателя. Преступление является оконченным с момента причинения крупного ущерба, до этого момента нарушение не подпадает под действие уголовного законодательства.

Незаконное применение экземпляров программ для ЭВМ или БД, например, их продажа, сдача в прокат или иное использование в коммерческих целях без соответствующего разрешения правообладателя влечет за собой административную ответственность. Для наступления административной ответственности достаточно доказать факт незаконного использования программ для ЭВМ или БД в коммерческих целях.

Правообладатель непосредственно или через своего представителя в течение срока действия авторского права может по своему желанию зарегистрировать программу для ЭВМ или базу данных в федеральном органе исполнительной власти по интеллектуальной собственности. Следует понимать, что факт регистрации не создает авторского права и не расширяет объема существующего авторского права. Следует учитывать, что факт регистрации создает имеющую юридическую силу презумпцию достоверности сведений, внесенных в Реестр программ для ЭВМ или Реестр баз данных, то есть такие сведения считаются достоверными, пока не доказано обратное. Свидетельство о регистрации, сведения, указанные в Реестре, и депонированные материалы могут сыграть серьезную роль в случае судебного разбирательства – при необходимости идентификации произведения. Свидетельство о регистрации используется и как доказательство законности владения авторскими правами на программу для ЭВМ или базу данных.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Маслов В.С. – студент гр. ПИЮ-322 ААЭП
Беспалова Е.Э. – ст. преп. каф. ПИЮ ААЭП

В современных условиях любая деятельность сопряжена с оперированием большими объемами информации, которое производится широким кругом лиц. Защита данных от несанкционированного доступа является одной из приоритетных задач при проектировании любой информационной системы. Следствием возросшего в последнее время значения информации стали высокие требования к конфиденциальности данных. Системы управления базами данных, в особенности реляционные СУБД, стали доминирующим инструментом в этой области. Обеспечение информационной безопасности СУБД приобретает решающее значение при выборе конкретного средства обеспечения необходимого уровня безопасности организации в целом. Для СУБД важны три основных аспекта информационной безопасности – конфиденциальность, целостность и доступность. Политика безопасности определяется администратором данных. Однако решения защиты данных не должны быть ограничены только рамками СУБД. Абсолютная защита данных практически не реализуема, поэтому обычно довольствуются относительной защитой информации - гарантированно защищают ее на тот период времени, пока несанкционированный доступ к ней влечет какие-либо последствия. Разграничение доступа к данным также описывается в базе данных (БД) посредством ограничений, и информация об этом хранится в ее системном каталоге. Иногда дополнительная информация может быть запрошена из операционных систем, в окружении которых работают сервер баз данных и клиент, обращающийся к серверу баз данных.

Управление БД производят пользователи. Пользователей СУБД можно разделить на три группы:

1. Прикладные программисты - отвечают за создание программ, использующих базу данных. В смысле защиты данных программист может быть как пользователем, имеющим привилегии создания объектов данных и манипулирования ими, так и пользователем, имеющим привилегии только манипулирования данными.

2. Конечные пользователи базы данных - работают с БД непосредственно через терминал или рабочую станцию. Как правило, конечные пользователи имеют строго ограниченный набор привилегий манипулирования данными. Этот набор может определяться при конфигурировании интерфейса конечного пользователя и не изменяться. Политику безопасности в данном случае определяет администратор безопасности или администратор базы данных (если это одно и то же должностное лицо).

3. Администраторы баз данных - образуют особую категорию пользователей СУБД. Они создают сами базы данных, осуществляют технический контроль функционирования СУБД, обеспечивают необходимое быстродействие системы. В обязанности администратора, кроме того, входит обеспечение пользователям доступа к необходимым им данным, а также написание (или оказание помощи в определении) необходимых пользователю внешних представлений данных. Администратор определяет правила безопасности и целостности данных.

Остановимся на средствах дискреционной защиты.

Дискреционное управление доступам (discretionary access control) — разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.

Дискреционная защита является многоуровневой логической защитой. Логическая защита в СУБД представляет собой набор привилегий или ролей по отношению к защищаемому объекту. К логической защите можно отнести и владение таблицей (представлением). Владелец таблицы может изменять (расширять, отнимать, ограничивать доступ) набор привилегий (логическую защиту) . Данные о логической защите находятся в системных таблицах базы данных и отделены от защищаемых объектов (от таблиц или представлений).

Администратор каждой базы занимается созданием круга возможных пользователей создаваемой им БД и разграничением полномочий этих пользователей. Данные о разграничениях располагаются в системном каталоге БД. Очевидно, что данная информация может быть использована для несанкционированного доступа и поэтому подлежит защите. Защита этих данных осуществляется средствами самой СУБД.

Набор привилегий можно определить для конкретного зарегистрированного пользователя или для группы пользователей (это могут быть собственно группы пользователей, роли и т.п.). Объектом защиты может являться таблица, представление, хранимая процедура и т.д. (подробный список объектов защиты имеется в документации к используемой СУБД). Субъектом защиты может быть пользователь, группа пользователей или роль, а также хранимая процедура, если такое предусматривается используемой реализацией. Если из используемой реализации следует, что хранимая процедура имеет «двойной статус» (она и объект защиты, и субъект защиты), то нужно очень внимательно рассмотреть возможные модели нарушителей разграничения прав доступа и предотвратить эти нарушения, построив, по возможности, соответствующую систему защиты.

Привилегии конкретному пользователю могут быть назначены администратором явно и неявно, например через роль. Роль — это еще один возможный именованный носитель привилегий. С ролью не ассоциируют перечень допустимых пользователей — вместо этого роли защищают паролями, если, конечно, такая возможность поддерживается производителем СУБД. Роли удобно использовать, когда тот или иной набор привилегий необходимо выдать (или отобрать) группе пользователей. С одной стороны, это облегчает администратору управление привилегиями, с другой — вносит определенный порядок в случае необходимости изменить набор привилегий для группы пользователей сразу.

Также кроме дискреционной защиты СУБД развиты средства мандатной защиты. Средства мандатной защиты предоставляются специальными (trusted) версиями СУБД.

Мандатное управление доступом (mandatory access control) — это разграничение доступа субъектов к объектам данных, основанное на характеризуемой меткой конфиденциальности информации, которая содержится в объектах, и на официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Рассмотрим, для чего необходима мандатная защита. Средства произвольного управления доступом характерны для уровня безопасности. Как правило, их, в принципе, вполне достаточно для подавляющего большинства коммерческих приложений. Тем не менее, они не решают одной весьма важной задачи — задачи слежения за передачей информации. Средства произвольного управления доступом не могут помешать авторизованному пользователю законным образом получить секретную информацию и затем сделать ее доступной для других, неавторизованных, пользователей. Нетрудно понять, почему это так. При произвольном управлении доступом привилегии существуют отдельно от данных (в случае реляционных СУБД — отдельно от строк реляционных таблиц), в результате чего данные оказываются «обезличенными» и ничто не мешает передать их кому угодно даже средствами самой СУБД; для этого нужно лишь получить доступ к таблице или представлению.

Физическая защита СУБД главным образом характеризует данные (их принадлежность, важность, представительность и пр.). Это в основном метки безопасности, описывающие группу принадлежности и уровни конфиденциальности и ценности данных объекта (таблицы, столбца, строки или поля). Метки безопасности (физическая защита) неизменны на всем протяжении существования объекта защиты (они уничтожаются только вместе с ним) и территориально (на диске) располагаются вместе с защищаемыми данными, а не в системном каталоге, как это происходит при логической защите.

СУБД не дает проигнорировать метки конфиденциальности при получении доступа к информации. Такие реализации СУБД, как правило, представляют собой комплекс средств как на машине-сервере, так и на машине-клиенте, при этом возможно использование специальной защищенной версии операционной системы. Кроме разграничения доступа к информации посредством меток конфиденциальности, защищенные СУБД предоставляют средства слежения за доступом субъектов к объектам защиты (аудит).

Использование СУБД с возможностями мандатной защиты позволяет разграничить доступ собственно к данным, хранящимся в информационной системе, от доступа к именованным объектам данных. Единицей защиты в этом случае будет являться, в частности, запись о договоре N, а не таблица или представление, содержащее информацию об этом договоре. Пользователь, который будет пытаться получить доступ к договору, уже никак не сможет обойти метку конфиденциальности. Существуют реализации, позволяющие разграничивать доступ вплоть до конкретного значения конкретного атрибута в конкретной строке конкретной таблицы. Дело не ограничивается одним значением метки конфиденциальности — обычно сама метка представляет собой набор значений, отражающих, например, уровень защищенности устройства, на котором хранится таблица, уровень защищенности самой таблицы, уровень защищенности атрибута и уровень защищенности конкретного кортежа.

Кроме того, защищенные СУБД позволяют разграничить доступ к информационной системе с тех или иных рабочих станций для тех или иных зарегистрированных пользователей, определить режимы работы, наложить ограничения по времени работы тех или иных пользователей с тех или иных рабочих станций. В случае реализации данных опций на прикладном уровне задача, как правило, сводится к созданию сервера приложений, который занимается отслеживанием, «кто и откуда пришел». Отдельный комплекс серверных приложений (обычно — хранимых процедур, если в СУБД отсутствует мандатная защита) обеспечивает аудит.

Таким образом, в современных условиях остро встает проблема защиты как самих СУБД, так и баз данных в них. Дискреционная и мандатная защита позволяет защитить современные БД от несанкционированного доступа, но и при этом сделать их доступными пользователям, наделив отдельных пользователей определенными привилегиями.

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ КАДРАМИ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ «АИТ:\ УПРАВЛЕНИЕ ПЕРСОНАЛОМ»

Денежкина Т. Н. – студентка гр. ПИЮ-321 ААЭП
Беспалова Е.Э. – ст. преп. каф. ПИЮ ААЭП

Кадровое делопроизводство непосредственным образом связано с деятельностью юриста. Юридически обосновываются все виды движения кадров: найма, увольнения, передвижения. В настоящее время, как и любая сфера деятельности, автоматизация кадрового документооборота является актуальной задачей на предприятии.

С появлением первых средств автоматизации были разработаны и первые программы учета и управления персоналом, число которых как в России, так и в других странах мира исчисляется сейчас сотнями. Если говорить о России, то каждое уважающее себя предприятие или организация, имевшие собственный отдел АСУ, еще в 1980-е гг. пользовались программами учета персонала собственной разработки. Эти программы опирались на различные аппаратные платформы (начиная от мэйнфреймов и заканчивая ПК) и инструментальные средства (начиная от PL-1 и заканчивая Clipper и FoxPro). С появлением новых, более совершенных, аппаратных и инструментальных средств, данные программы модифицировались и расширяли свою функциональность (особенно быстро это происходило на Западе).

Информационные технологии сегодня успешно работают практически на всех уровнях управления предприятием. Но если автоматизация бизнес-процессов – очевидный для руководства компаний путь повышения эффективности, то необходимость автоматизации работы кадровой службы осознается пока далеко не всеми. Однако именно в хаосе, царящем в сфере управления кадрами предприятия, часто кроется секрет «не успешности» предприятия. Руководителям компаний, специалистам отделов кадров и кадровым службам необходимо осваивать информационные технологии в общем, в теоретическом и практическом аспектах. Истина очевидна – пока горы бумажных табелей учета и трудовых книжек не уступят место нормальному, автоматизированному управлению кадрами в компаниях, высоких результатов в бизнесе достичь очень сложно.

Современные автоматизированные системы управления персоналом предназначены для оптимизации работы, в первую очередь, руководства и персонала кадровых служб предприятий (помимо бухгалтерии и некоторых других подразделений) и играют большую роль в повышении производительности их труда. В частности, менеджеры по персоналу при помощи таких систем избавляются от выполнения рутинных операций при работе с кадрами, подготовке и учете приказов (существуют оценки, что только на работу с документацией по персоналу кадровики тратят до 60% своего рабочего времени). Автоматизированное хранение и обработка полной кадровой информации также позволяет эффективно осуществлять подбор и перемещение сотрудников. Кроме того, автоматизированный расчет заработной платы с учетом информации о позициях штатного расписания, отпусках, больничных, командировках, льготах и взысканиях дает возможность работникам бухгалтерии точно и оперативно начислять зарплату, формировать бухгалтерские отчеты,

относить затраты на себестоимость. И это лишь некоторые из функций современных автоматизированных систем управления персоналом.

Подавляющее большинство комплексных корпоративных информационных систем (КИС) зарубежной разработки (впрочем, как и почти все отечественные КИС) построены по модульному принципу и имеют в своем составе модуль управления персоналом, реализующий автоматизированное управление кадрами (нередко управление кадрами объединено также с расчетом зарплаты). Можно назвать такие известные в мире системы, имеющие в своем составе Human Resources (HR) модули, как SAP R/3, Baan, Oracle Applications и др. Существуют и автономные программные пакеты управления персоналом, одним из примеров которых является ПО Renaissance CS Human Resources.

В настоящее время на российском рынке наблюдается подлинное многообразие предложений по разработке и поставке автоматизированных систем управления персоналом (как отечественных, так и западных). К достоинствам отечественных пакетов можно отнести их адаптированность к российской системе учета и делопроизводства, а также более низкую цену по сравнению с наиболее известными пакетами западных фирм. К преимуществу западных пакетов относится в некоторых случаях значительно более полная функциональность. Вот лишь некоторые из компаний, предлагающих на российском рынке HR- системы: АйТи; АиТСофТ; АСК; Атлант/Информ; Белтел; Бизнес Сервис-Софт; Бизнес-Консоль; Бэст; Гарант-Инфоцентр; Гектор; Гуманитарные Технологии; Инвента; Интех; Инфософт; Информконтакт; Инэк; Компьюлинк УСП; Ланкс; Ливс; Омега; Прайс/Уотерхаус Куперс; Риккон; С+; Северо-Западный Центр Новых Информационных Технологий; Си Технолоджи; Спутник Лаборатори; Трансфер Эквипмент Восток; Центр Мосвест; Центр информационных технологий Телеком-Сервис; ЭАСК; Эдвантедж Софт; Эксперт; Элко Технологии; 1С; INFIN; Oracle; Renaissance; Robertson&Blums; SAP AG и др.

В области кадрового программного обеспечения на российском рынке наиболее популярны ИСУП от компаний 1С (1С: Зарплата и кадры) и "АйТи" (БОСС-Кадровик). Помимо этого есть специализированные продукты для малого и среднего бизнеса: "АиТ Кадры", "Оазис" - "Менеджер по персоналу", программный комплекс "Кадры" компании "Финлайнс", сетевой программный комплекс "Радость кадровика" компании "ЛегПромСофт", программы для управления персоналом Центра кадровых технологий. Все они включают ведение кадровой документации, ведение отчетности в соответствии с требованиями ТК, ведение базы данных о соискателях, регистрацию движения персонала, учет аттестаций, управление мотивацией труда, ведение архива кадровой службы, учет фактически отработанного времени (табельный учёт), расчеты с персоналом по оплате труда.

Рассмотрим одну из систем управления персоналом «АиТ:\ управление персоналом» более подробно. Данный комплекс обладает расширенными функциональными возможностями и является продуктом высококачественного проектирования и разработки. Это современное автоматизированное решение, обеспечивающее эффективную и удобную работу всех служб, занятых в управлении персоналом.

Необходимо выделить преимущества программного комплекса:

1. Обеспечение согласованной работы субъектов управления персоналом, исключение возможных противоречий и дублирование файлов.
2. Возможность консолидации данных о сотрудниках при многоуровневой и территориально распределенной структуре предприятия, передача сведений при любом качестве каналов связи.
3. Возможность выбора состава программного комплекса исходя из специфики предприятия и конкретного рабочего места.
4. Гибкая настройка системы.

5. Автоматический ввод массовых данных.
6. Полная адаптация к российскому законодательству.
7. Электронные архивы.
8. Интеграция с финансовыми системами и системами управления производства.

Использование программного комплекса позволяет руководству предприятия повысить эффективность работы за счет правильной расстановки кадров, сократить время принятия управленческих решений и контролировать их исполнение, снизить затраты и произвести их полный учет. При работе с комплексом менеджерами по персоналу, в связи с **а**втоматизацией кадрового документооборота, **з**аметно снижается трудоемкость работ и повышается производительность труда и исполнительская дисциплина.

«АиТ:\ управление персоналом» состоит из нескольких модулей.

Модуль «АиТ:\Кадры» обеспечивает поддержку развернутого досье сотрудника, формирование штатного расписания и штатной расстановки, а также подбор сотрудников на штатные единицы и анализ их соответствия; документооборот персональных приказов; прием, перевод и увольнение работников; планирование аттестации и графиков отпусков.

Режим "Штатное расписание" позволяет работать в условиях организационной структуры любого типа, поддерживает ведение многоуровневой структуры предприятия с произвольным числом уровней и группировкой подразделений по филиалам. Модуль поддерживает хранение любых сведений о кадрах; ведение данных по сотрудникам осуществляется в форме кадровых карточек.

Модуль «АиТ:\Табельный» учет предназначен для учета рабочего времени на предприятии. Позволяет создавать детальные графики работ, настраивать длительность рабочего цикла, производить разбивку дней графика на рабочие и нерабочие, выполнять автоматический расчет плановых дней и часов за выбранный расчетный период.

Использование программы Табель дает возможность существенно снизить трудозатраты, а также добиться максимально оперативной передачи данных для начисления заработной платы.

Модуль "АиТ:\Персонифицированный пенсионный учет" предназначен для сбора, учета и анализа персональной информации от момента начала трудовой деятельности человека и в течение всей его жизни: доходов, стажа и отчислений в Пенсионный Фонд России. С его помощью специалист по кадрам может подготовить и отправить в пенсионный фонд необходимые отчетные документы. А также модуль позволяет подавать сведения с помощью электронной почты используя эллектронно-цифровые подписи.

Основной функцией модуля «АиТ:Штатное расписание» является ведение всех видов штатного расписания. В нем предусмотрено расширение состава карточки структурного подразделения для разделения персонала на управленческий, цеховой, а также расширение состава реквизитов карточки штатной единицы для формирования надбавок и дополнительных свойств штатной единицы.

Модуль "АиТ:\Репликация" предназначен для обеспечения централизованной работы комплекса для территориально-распределенных компаний (холдингов). Модуль осуществляет обмен данными между центральной, удаленными базами данных, ведение единой нормативно-справочной информации, получение сквозных отчетов, планирование организационной структуры, документов, контроль движения кадров.

Также существуют специальные решения, например, модули «Оценка и аттестация персонала» и «Автоматический учет рабочего времени (электронная проходная)»

Анализируя выше сказанное, можно сделать вывод, что "АиТ:\Управление персоналом" это современное автоматизированное решение, обеспечивающее эффективную и удобную работу всех служб, нацеленных на решение функций контроля и планирование персонала.

ПРАВОВЫЕ И ЭТИЧЕСКИЕ АСПЕКТЫ ЭЛЕКТРОННОГО БИЗНЕСА

Грошева Т.А. – студентка гр. ПИЮ-322 ААЭП
Лагоха А.С. – ст. преп. каф. ПИЮ ААЭП

Бурный рост электронного бизнеса поднял целый ряд новых юридических и этических вопросов, которые требуют специального рассмотрения - законы и правила, регулирующие данную отрасль, зачастую отстают от введения новых технологий на месяцы и даже на годы.

В России законодательство, регулирующее электронный бизнес, только начинает свое развитие. В связи с проблемой правового регулирования Интернета возникает вопрос, является ли Интернет сферой, которую необходимо регулировать нормами права, допустимо ли вмешательство государства в отношения, возникающие в связи с использованием Интернета.

Необходимость систематизации нормативных правовых актов, регулирующих электронно-экономический бизнес, обусловлена определением информационного законодательства в системе конституционного законодательства и круга информационных правоотношений, подлежащих правовому регулированию. Систематизация позволяет исключить субъектное понимание существующего нормативно правового массива в информационной сфере и выработать единые взгляд на рассмотрение с учетом основания систематизации как целостного образования – системы.

В основу законодательной базы электронного бизнеса положено вариант законодательства принятый в апреле 1992 года.

В реальности действующее законодательство адаптируется к особенностям сети Интернет в вопросах использования Интернета как средства массовой информации.

Основными законами применяемые в области Интернета и передаваемой информацией является Федеральным законом от 20 февраля 1995 г. «Об информации, информатизации и защите информации», а также Указом Президента РФ от 6 марта 1997 г., развивающих положения этого Закона.

Основными объектами законодательного регулирования в области электронного бизнеса является:

- *защита частной жизни;*
- *защита прав несовершеннолетних;*
- *защита прав собственности;*
- *определение прав собственности информации;*
- *свобода слова;*
- *подделка документов и другие преступления, нарушающие права потребителей;*
- *налогообложение электронной коммерции* требует отдельного пояснения.

Интернет не имеет национальных границ. В связи с этим возникает вопрос - в юрисдикции каких налоговых органов находится конкретная «электронная» сделка? Комиссия ООН по международному торговому праву подготовила образец закона об электронной коммерции, согласно которому любая компания, занимающаяся электронной коммерцией за пределами своей страны, должна быть осведомлена о действующих в странах-партнерах законах и ограничениях.

К основным объектам законодательного регулирования следует отнести и *право на информацию.* Интернет позволяет оперировать огромными объемами информации. Поэтому существует опасность несанкционированного использования частной или коммерческой информации, что наносит ущерб ее владельцу. Потребительские базы данных и списки рассылки содержат такую ценную информацию, что некоторые предприниматели соблазняются возможностью заработать на ее продаже. Уже нередки случаи мошенничеств с использованием неправомерно полученной информации о банковских счетах, кредитных карточках пользователей Интернета.

Американская маркетинговая ассоциация недавно создала кодекс Интернета для электронного бизнеса. Многие профессиональные организации в разных странах призывают своих членов соблюдать эти этические нормы поведения, а не только полагаться на регулирующую роль законодательства.

Полезным источником информации для принятия этически взвешенных решений для американских маркетологов служит Центр прикладной этики им. Марккулы в университете Санта-Клара в Калифорнии. В результате многолетних исследований был разработан «вопросник», помогающий практикам определить, каким образом их деятельность проблемы затрагивает этические вопросы.

Попытку классифицировать этические проблемы предприняли несколько авторов, опубликовавших в 1995 г. в журнале «Management Information Systems» статью «Этика управления информацией». Было выделено 4 основные группы проблем:

- *защита частной жизни (сбор, хранение и распространение информации о частных лицах);*
- *точность информации (аутентичность, надежность и точность собранной и обработанной информации);*
- *защита прав собственности (права собственности и стоимость информации, защита интеллектуальной собственности);*
- *доступ к информации (права доступа к информации и оплата такого доступа).*

В области государственной политики относительно Интернета больше вопросов, чем ответов. Число нерешенных проблем и все новые вопросы, возникающие в связи с освоением сети, заставляют многих специалистов заниматься правовыми и этическими аспектами электронного бизнеса. Надеяться только на разработку четких правовых норм в такой стремительно меняющейся области маркетинговой деятельности, как электронный бизнес, неблагоразумно, следует обратить внимание на саморегулирование этой отрасли, на выработку общих этических норм поведения, которые позволят заниматься электронным маркетингом с выгодой для компании и пользой для потребителя. Однако, на взгляд автора, определение этичного и неэтичного поведения зависит от конкретного человека, национальной культуры и законодательства конкретной страны.

ПРИМЕНЕНИЕ СПРАВОЧНО-ПОИСКОВЫХ СИСТЕМ В ПРОЦЕССЕ РЕГУЛИРОВАНИЯ ТРУДОВЫХ ПРАВООТНОШЕНИЙ

Мочалова Е.Б. – студентка гр. ПИЮ-322 ААЭП
Лагоха А.С. – ст. преп. каф. ПИЮ ААЭП

В связи с постоянно изменяющимся законодательством - ежемесячно органы власти выпускают несколько тысяч документов - информативная нагрузка в различных областях деятельности человека постоянно растет, и для разрешения возникающих спорных вопросов по юридическим вопросам не редко требуется затратить не малое количество времени. В современных условиях большую роль в поиске информации играют справочные правовые системы (СПС). Под СПС будем понимать совокупность информационно-правовых и поисковых ресурсов, интегрированных в одну систему. Это массивы документов, консультаций, вопросов-ответов, обобщение арбитражной практики (так называемые информационные банки) поисковые ресурсы, ресурсы для обновления и пр.

В 1975 г. руководство Советского Союза приняло решение о создании первой информационной базы нормативных документов. 25 июня 1975 г. вышло Постановление ЦК КПСС и Совета Министров СССР N 558 "О мерах по дальнейшему совершенствованию хозяйственного законодательства", в котором признавалось необходимым "ввести

государственный учет нормативных актов СССР и союзных республик, а также организовать централизованную информацию о таких актах". В конце 80-х - начале 90-х годов началось динамичное развитие российского законодательства и одновременно широкое распространение персональных компьютеров. Многие специалисты (юристы, бухгалтеры, аудиторы, руководители организаций) ощутили острую потребность в полной и актуальной правовой информации. Качественный уровень СПС в России не только не уступает, но и по ряду параметров превышает зарубежные аналоги - за 30 лет проделан путь от простейших электронных архивов, предназначенных для хранения информации, до аналитических систем с развитым инструментарием поиска и анализа информации, ежедневно используемым многими специалистами.

Большое значение справочно-поисковые системы играют в трудовых правоотношениях, что связанно с обширным кругом задач, решаемых кадровой службой по вопросам документирования трудовой деятельности, под которой, в частности, следует понимать: ***приём на работу, перевод на другую работу, увольнение, предоставление отпусков, командирование***. Квалифицированное ведение документации по личному составу относится к числу необходимых профессиональных навыков работника кадровой службы, при этом документирование любых процедур должно проводится с соблюдением установленных общегосударственных правил оформления документов.

Трудовые правоотношения регулируются многими нормативными актами, применение которых необходимо и обязательно для исполнения, что приводит к нормальному функционированию любой организации в целом. Так, ***ст. 5 Федерального закона от 20.02.95 № 24-ФЗ "Об информации, информатизации и защите информации" (СЗ РФ, 1995, № 8, ст. 609)*** гласит: "Документирование информации является обязательным условием включения информации в информационные ресурсы. Документирование информации осуществляется в порядке, устанавливаемом органами государственной власти, ответственными **за** ***организацию делопроизводства, стандартизацию документов и их массивов, безопасность Российской Федерации"***. ***Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ*** устанавливает необходимость документирования следующих документов: ***приказ*** (***распоряжение***) ***о приеме на работу*** (форма № Т-1), ***личная карточка*** (форма № Т-2) , ***учетная карточка научного работника*** (форма № Т-4), ***приказ (распоряжение) о переводе на другую работу*** (форма №Т-5), ***приказ (распоряжение) о предоставлении отпуска*** (форма №Т-6) и многие другие**.**

Справочно-поисковая система ГАРАНТ позволяет найти все необходимые формы документов, описание правил их заполнения с помощью поиска по реквизитам, просто заполнив поле номер документа.

Много споров возникает по поводу трудовых правоотношений, что связано с тем, что каждый из нас в будущем или сегодня занимается трудовой деятельностью и поэтому заинтересован в получении необходимых знаний. В современный век технологий решать такие задачи, а также многие другие, помогают справочные поисковые системы, которые из большого количества информации, с наименьшими затратами времени помогают найти нужный правовой документ. Поисковые системы помогаю найти ни только документ, но и основные сведения о нём, что включает в себя комментарии юристов, информацию о сроках вступления законопроекта в силу и его изменении. Справочные системы более 30 лет назад вошли на Российский рынок, постоянно модернизируя свою работу для наиболее эффективного взаимодействия с пользователем. Выбор той или иной ИПС зависит от задач, решаемых в рамках конкретной предметной области, от удобства интерфейса системы, от полноты баз данных.

КОМПЛЕКСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Линник В.Г. – студент гр. ПИЮ-322 ААЭП
Лопухов В.М. – доцент каф. ПИЮ ААЭП

Последнее время заголовки не только компьютерных, но и обычных изданий пестрят упоминаниями о новых вирусах, нападениях хакеров и других страшных опасностях, которые грозят современным информационным ресурсам.

Для предотвращения любых попыток нанесения ущерба информационным ресурсам современного предприятия необходимо построить комплексную систему информационной безопасности предприятия, важнейшей составной частью которой является программное обеспечение.

Построение программного обеспечения системы начинается с "внешнего контура" предприятия в виде "забора с воротами", который информирует о возможных проходах внутрь и наружу. В наиболее распространенном случае "внешним контуром" для информационной автоматизированной системы современного предприятия являются точки соединения внутренней локальной сети с внешней или с Интернет. А роль "забора с воротами" здесь выполняет Firewall, также называемый межсетевым экраном или брандмауэр.

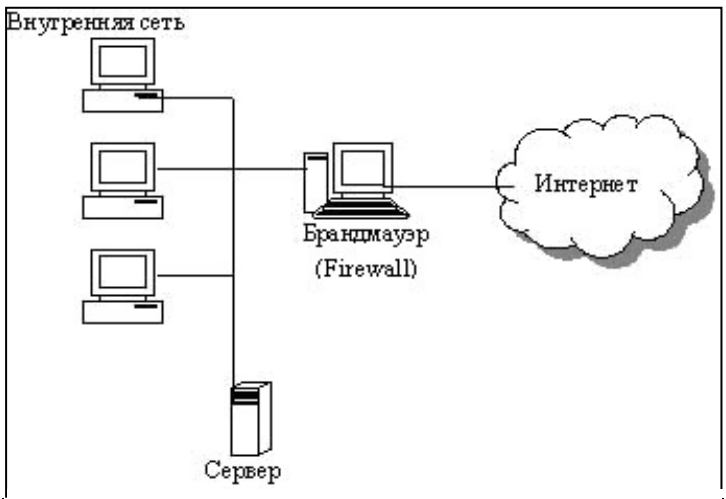


Рис.1. Типовое размещение брандмауэра в локальной сети

Firewall – это программно-аппаратный комплекс, который позволяет пользователю закрыть все порты входа-выхода, кроме тех, которые нужны ему для работы, В классическом случае это компьютер с двумя сетевыми картами, одна из которых соединена с внутренней сетью, а вторая с внешней. В память этого компьютера загружена программа, которая управляет TCP/IP портами и контролирует, кто или что, имеет право пользоваться этими портами и в каких целях.

Но, построив "забор с воротами" вокруг автоматизированной информационной системы предприятия, рано успокаиваться. Нужно поставить в воротах "систему наблюдения", которая будет следить, не пытаются ли, под видом своих, проникнуть внутрь чужие. А также, установить в воротах "металлодетекторы", чтобы предотвратить пронос через ворота (в любом направлении) запрещенных материалов. Такой "системой наблюдения" в информационной безопасности служит Intrusion Detection System - система обнаружения попыток вторжения. А роль "металлодетектора" выполняет Content Inspection System — система проверки содержимого входящего и исходящего сетевого трафика.

Для защиты информационной системы предприятия по "внешнему контуру" компания Computer Associates предлагает программные продукты: eTrust Firewall, eTrust Intrusion Detection System и eTrust Content Inspection System. Также необходимо обеспечивать внутреннюю защиту информационной системы, которая по важности не уступает внешней, поскольку известно, что львиная доля потерь, связанных с нарушением секретности, происходит по вине сотрудников предприятия. Поэтому очень важно, не только разработать эффективные правила информационной безопасности и довести их до сведения каждого сотрудника, но и строго следить за их выполнением. Для этих целей компания Computer Associates также предлагает программные продукты серии eTrust.

Система контроля доступа eTrust Access Control позволяет управлять доступом и защищать процессы, привилегированные программы, сетевые соединения, терминалы и ресурсы.

Для проверки надежности построенной системы безопасности на предприятии можно использовать eTrust Policy Compliance — систему поиска уязвимостей в системе, которая определяет "дыры" в системе безопасности и автоматически генерирует скрипты, которые их закрывают.

Для облегчения непростого труда администраторов существуют два удобных инструмента: eTrust Admin и eTrast Audit.

eTrast Admin представляет собой централизованное средство администрирования объектов в разнородной среде. Этот продукт позволяет создавать, модифицировать и удалять объекты, такие как учетные записи пользователей.

eTrust Audit предназначен для сбора и анализа информации из системных журналов. Это программый продукт позволяет обрабатывать информацию для удобного просмотра и создания отчетов, а также выполнять заранее определенные действия в случае обнаружения следов подозрительных действий.

Построение системы информационной безопасности современного предприятия, которая состоит из целого ряда компонентов — это сложный и ответственный процесс, требующий приложения серьезных знаний, опыта, времени и средств. Простота управления системой защиты информационной системы является одним из важных условий информационной безопасности. Построив комплексное программное обеспечение системы защиты информации на базе продуктов одного производителя, например компании Computer Associates, можно избежать проблем с несовместимостью компонент системы между собой и значительно упростить процесс внедрения и последующей эксплуатации комплексной системы информационной безопасности современного предприятия как юридической, так и экономической направленности.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В МУНИЦИПАЛЬНЫХ ОРГАНАХ

Ялин А.И. – студент гр. ПИЮ-322 ААЭП
Лопухов В.М. – доц. каф. ПИЮ ААЭП

На протяжении всей своей деятельности предприятия, работающие в государственной сфере, сталкиваются с необходимостью хранения и обработки информации. Некоторая хранимая информация подходит под разряд конфиденциальной, т.е. доступ к которой ограничен в соответствии с законом. Конфиденциальность этой информации гарантирует безопасность государства и общества, которая зависит от нормальной работы органов государственной власти и местного самоуправления.

В органах государственной власти и органах местного самоуправления финансирование идет из бюджета, что накладывает определенное ограничение на возможность реализовывать защиту информации в полной мере. Конечно такие органы как ФСБ и т.п. имеют достаточно хорошую систему защиты информации, но организация защиты информации в некоторых других органах государственной власти и органах местного самоуправления оставляет желать лучшего.

Автором был проведен анализ на предмет информационной безопасности учреждения местного самоуправления, которое располагалось в одноэтажном кирпичном доме и занимало всю его территорию. Данное учреждение располагает конфиденциальной информацией различного характера, защита которой устроена следующим образом:

- окна с обычной деревянной рамой снаружи защищены железной решеткой, закрепленной в кирпичах;
- две двери, наружная железная и деревянная внутренняя;
- окна, входные двери и двери кабинетов защищены сигнализацией, срабатывающей при попытке проникновения в помещение;
- в кабинетах стоят железные сейфы, находящиеся в плохом состоянии;
- некоторые кабинеты оснащены компьютерами, которые запрашивают пароль на вход в систему и пароль для работы со специализированным программным обеспечением (если программы имеют такое средство защиты);
- в ночное время в здании находится сторож, имеющий при себе следующие средства обеспечения безопасности: пистолет, резиновая дубинка, наручники.

Простой осмотр такого здания изнутри и снаружи дает понять, что проникновение в здание и выполнение своих целей не составит особого труда для злоумышленника.

Рекомендации по обеспечению информационной безопасности:

1) В рабочие часы учреждение посещает множество людей по вопросам различного рода. Пройти может любой желающий, так как отсутствует персонал, который мог бы вести наблюдение за посетителями и контролировать их доступ в запрещенные зоны. Рекомендуется нанять сотрудника, который будет в дневное время следить за порядком в помещении.

2) Рекомендуется поменять старые сейфы на современные огнеупорные сейфы с электронными замками и замками ключевого типа.

3) Двери кабинетов хоть и оснащены сигнализацией, но из-за плохого технического состояния не составляют особого препятствия для проникновения вовнутрь. В связи с этим рекомендуется заменить двери кабинетов на новые, по возможности металлические, с замками ключевого типа.

4) Возможна установка приборов видео наблюдения, для повышения безопасности при оставлении здания персоналом в ночное время и нерабочие дни. По возможности приборы наблюдения должны быть установлены в каждом кабинете и коридоре. Количество и качество приборов зависит от размера средств, выделенных на приобретение и установку аппаратуры видеонаблюдения.

5) Телефонные линии проведены во всех комнатах здания. Линии не защищены от прослушивания, что позволяет легко прослушивать телефонные разговоры чиновников. В настоящее время существует множество приборов способных не только защищать телефонные линии от прослушивания, но и находить место расположения жучков, а также уничтожать их (подавители, блокираторы, анализаторы, детекторы поля, сканеры, маскираторы, скремблеры). Выбор устройства полностью зависит от размера средств, которые учреждение готово потратить на его приобретение.

Для отечественных линий лучше всего использовать отечественные приборы, специально адаптированные для российских линий связи. Могут быть разработаны индивидуальные системы защиты телефонных аппаратов от прослушивания, которые будут выполнять определенные заказчиком функции.

6) Данное учреждение располагает несколькими персональными компьютерами различной модели и комплектации. На персональных компьютерах установлены различные операционные системы и различное программное обеспечение. Каждый сотрудник имеет специализированное ПО, состав которого определяется выполняемыми обязанностями. Создание документов происходит в основном с помощью программ MS Office. У пользователей есть доступ в Интернет через телефонную линию для информационного обмена с различными организациями, например, с банком и т.п. При входе в систему установлен пароль для разграничения доступа. Локальная сеть в пределах здания не организована за ненадобностью.

Антивирусные программы установлены не на всех ПК, а обновление антивирусных баз ведется не регулярно.

Рекомендуется использовать брандмауэр (firewall) для предотвращения вторжения в систему злоумышленников. Брандмауэр:

- вынуждает все сетевые соединения проходить через шлюз, где они могут быть проанализированы и оценены с точки зрения безопасности, и предоставляет другие меры усиленной аутентификации вместо паролей;
- ограничивает доступ к тем или иным системам или доступ к Интернету от них, блокировать определенные сервисы TCP/IP, или обеспечивать другие меры безопасности;
- устанавливается на границе защищаемой сети и фильтрует все входящие и исходящие данные, пропуская только авторизованные пакеты;
- обнаруживает попытки вторжения и проверяет содержимое входящего и исходящего сетевого трафика и тем самым повышает уровень безопасности, распознавая программы которые пытаются проникнуть в систему под видом «своих».

Для предотвращения проникновения вредоносных программ (вирусов) рекомендуется использовать антивирусные программы (сканеры, ревизоры и т.д.) с постоянно обновляемыми автоматически антивирусными базами. Так же необходимо проводить периодическую профилактику вирусных заражений, проверять всю входящую информацию.

Для обеспечения защиты от пользователя, не имеющего право доступа, рекомендуется помимо установки пароля на вход в систему устанавливать пороли в прикладных программах (если они позволяют это), а также пароли на «скринсейверы», специальные папки и файлы. Необходима периодическая смена паролей, которые должны состоять не менее чем из семи символов различного вида.

При передаче сообщений необходимо использовать электронную цифровую подпись и методы шифрования сообщений.

Рекомендуется использовать лицензионные программные продукты, что в современное время при недостаточном финансировании не выполняется, а поэтому существует риск потери и искажения информации.

Рекомендуется содержать штатного сотрудника, владеющего профессиональными знаниями по установке ПО и обслуживанию ПК. Из-за возможности системного сбоя и потери важной информации во время работы неопытного пользователя необходимо разграничить права доступа к информации на права администратора (профессионального настройщика оборудования) и ограниченные права пользователя (человека, непосредственно выполняющего свою работу в данном учреждении).

При использовании MobilRec возможно хранение жесткого диска с конфиденциальной информацией в несгораемом сейфе. Копии конфиденциальной информации необходимо хранить на сменных носителях информации, например CD.

7) Утечка информации может произойти непосредственно через сотрудников данного учреждения путем ее разглашения. Регулирование данного вопроса реализуется административными методами и полностью ложится на менеджера по кадрам, который должен ознакомить персонал с правилами обращения с конфиденциальной информацией, разъяснить ее важность и ответственность за невыполнение своих обязанностей в сфере защиты информации, определить круг лиц имеющих право доступа к конфиденциальной информации. Список конфиденциальной информации и ответственность за несоблюдение этих информационной безопасности оформляется юридическим документом.

Все меры защиты информации должны применяться в соответствии с законодательством РФ и ГОСТ, в частности с федеральным законом «Об информации, информатизации и защите информации». Разработанные автором рекомендации по обеспечению информационной безопасности исследованного муниципального учреждения переданы в администрацию данного учреждения.

ОБ ОДНОМ ПОДХОДЕ К ПРОГНОЗИРОВАНИЮ ПРАВОНАРУШЕНИЙ

Мочалова Е.Б. – студентка гр. ПИЮ-322 ААЭП
Шарикова Т.Г. – доц. каф. ПИЮ ААЭП

Правовая статистика как наука изучает количественную сторону массовых правовых и других юридически значимых явлений и процессов в целях раскрытия их качественного своеобразия, тенденций и закономерностей их развития в конкретных условиях места и времени [1]. Юристы в своей практической деятельности имеют дело с конкретными фактами (преступность, судимость, административные правонарушения, гражданско-правовые споры и др.), статистический анализ которых – необходимое условие их профессиональной деятельности. Он позволяет выявить законы распределения и динамики правонарушений, дает возможность прогнозировать состояние на будущее, позволяет оценить эффективность деятельности правоохранительных и судебных органов, получить другую важную информацию, необходимую для совершенствования отношений правового общества [2].

В современных условиях управляющие решения должны приниматься лишь на основе тщательного анализа имеющейся информации, следовательно, актуальность прогнозирования динамики правонарушений, не вызывает сомнения.

Для решения подобных задач, связанных с анализом данных о правонарушениях, предназначен мощный аппарат прикладной статистики. В табличном процессоре MS Excel реализован ряд статистических функций, позволяющих построить линию тренда временного ряда, сгладить значения ряда с неравноотстоящими узлами.

Исследуем возможность прогнозирования динамики изменения некоторого показателя. В таблице 1 приведен пример временного ряда, отражающего процесс развития наблюдаемого явления во времени [3]. Составными элементами этого ряда являются показатели уровня ряда и моменты времени (дни месяца).

Таблица 1

Динамика изменения статистического показателя в течение декабря месяца

Дата	1.12	2.12	5.12	6.12	7.12	8.12	9.12	10.12	14.12
Значение показателя	31,89	31,89	31,91	31,95	31,93	31,93	31,95	31,95	31,970
Дата	15.12	16.12	19.12	20.12	21.12	22.12	23.12	26.12	30.12
Значение показателя	30,92	30,97	30,95	30,95	30,96	30,96	30,97	30,97	29,07

Анализ скорости и интенсивности развития наблюдаемого явления во времени осуществляется с помощью аналитических показателей, например, с помощью средних, одним из которых является сглаживание. Сглаживание всегда включает некоторый способ локального усреднения данных, при котором несистематические компоненты взаимно погашают друг друга. Самый общий метод сглаживания - скользящее среднее, в котором каждый член ряда заменяется простым или взвешенным средним n соседних членов, где n – ширина "окна". Для сглаживания рядов с неравнооотстоящими узлами, примером которого является ряд из табл. 1, обычно используется среднее хронологическое значение [4]:

$$\bar{y} = \frac{\sum_{i=1}^{n-1}(y_{i+1} + y_i)\cdot(t_{i+1} - t_i)}{2\sum_{i=1}^{n-1}(t_{i+1} - t_i)}$$

где y_i – значение наблюдаемого показателя, t_i – дата (момент времени).

Вычислив средние хронологические значения показателя для каждого месяца текущего года, мы можем перейти к временному ряду, отражающему динамику изменения показателя в течение года (табл. 2). Для полученного ряда можно построить линию тренда и перейти к

следующему этапу – прогнозированию изменения исследуемого показателя с течением времени.

Таблица 2

Динамика изменения статистического показателя по месяцам текущего года

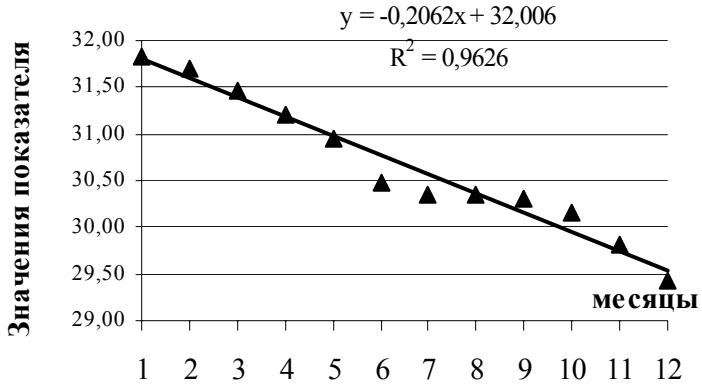
Месяц	Среднее хронологическое	Расчетное значение
Январь	31,82	31,80
Февраль	31,70	31,59
Март	31,46	31,39
Апрель	31,21	31,18
Май	30,94	30,98
Июнь	30,47	30,77
Июль	30,36	30,56
Август	30,34	30,36
Сентябрь	30,30	30,15
Октябрь	30,16	29,94
Ноябрь	29,81	29,74
Декабрь	29,42	29,53
Прогноз на два месяца последующего года		
Январь	–	29,33
Февраль	–	29,13

С использованием функции Excel – линия линейного тренда, получена следующая аналитическая зависимость:

y = -0,2062x + 32,006,

где *x* – период времени (месяц), *y* – среднее хронологическое значение исследуемого показателя.

На рисунке приведены полученные в результате предварительной обработки статистические данные, а также график и уравнение аппроксимирующей их линии тренда.



Полученный тренд позволил получить прогноз значения интересующего нас показателя на два месяца последующего года (Табл. 2).

Широкому внедрению методов анализа и прогнозирования данных способствовало развитие информационных технологий, основанных на использовании возможностей персональных компьютеров. Распространение статистических программных пакетов позволило сделать доступными и наглядными многие методы обработки данных, что широко используется на практике при решении задач правовой статистики.

Литература

1. Приказ Минюста РФ от 14 июня 2001 г. № 181 “О введении в действие системы статистической отчетности министерства юстиции российской федерации”.
2. Андерсен В. Статистический анализ временных рядов. – М: Мир, 1976. – 155 с.
3. Судебная статистика: Преступность и судимость (современный анализ данных уголовной судебной статистики России 1923-1997 годов)/Под ред. И.Н. Андрюшечкиной. – М.: Российский Юридический Издательский дом, 1998. – 64 с.
4. Громыко Г.Л. Теория статистики. – М: Изд-во Инфра-М, 2000 . – 413 с.

ИСПОЛЬЗОВАНИЕ ЯЗЫКА HTML ПРИ РАЗРАБОТКЕ ЭЛЕКТРОННЫХ УЧЕБНИКОВ

Дубовых И.А. – студент гр. ПИЮ-322 ААЭП
Линник В.Г. – студент гр. ПИЮ-322 ААЭП
Лагоха А.С. – ст. преп. каф. ПИЮ ААЭП

Данные тезисы отражают опыт авторов доклада по использованию языка HTML по разработке электронных изданий для юридического факультета Алтайской Академии Экономики и Права.

Современная система образования все активнее использует информационные технологии и компьютерные телекоммуникации. Особенно динамично развивается система дистанционного образования, чему способствует ряд факторов, и, прежде всего – оснащение образовательных учреждений мощной компьютерной техникой и развитие сообщества сетей «Интернет».

Развитие информационных технологий предоставило новую, уникальную возможность проведения занятий – внедрение дистанционной формы обучения. Как правило, в дистанционной форме обучения применяются электронные учебники и учебные пособия.

Электронные материалы учебного характера могут представлять собой: аудио- и видеоматериалы, тексты в HTML формате, слайд-фильмы (электронные презентации), тренажеры, задачники, тесты и прочие. Электронные пособия также могут содержать большое количество упражнений и примеров, могут подробно иллюстрироваться в динамике различные виды информации. Кроме того, при помощи электронных учебников осуществляется контроль знаний - компьютерное тестирование.

Электронные учебники и учебные пособия представляют собой переложенный на компьютерную основу учебный материал. «Интеллектуальность» компьютеров позволяет создавать средства обучения, обладающие возможностями взаимодействия с пользователем, настройки на его индивидуальность. При этом компьютер берет на себя часть функций преподавателя, делая пособие эффективным средством обучения. Электронные книги могут включать информационную, справочную, тренажерную и контролирующую компоненту, иметь иллюстративный (пассивный) или интерактивный (диалоговый) характер, дополнять или заменять бумажные пособия.

Таким образом, в процессе использования электронных учебников происходит:

- индивидуализация процесса обучения, учитывающая психологические и творческие особенности личности обучаемого;
- повышение эффективности обучения;
- увеличение доли активного самостоятельного изучения материала и повышение ответственности за обучение самого студента;
- объективизация самооценки знаний студентов.

Авторами статьи был разработан ряд электронных учебных пособий. На пример, электронное учебное пособие по дисциплине «Методы оптимизации» содержит:

– теоретический материал по темам: «Метод золотого сечения», «Симплекс метод», «Решение транспортной задачи», «Геометрический метод решения задачи линейного программирования»;
– примеры практических задач по каждой теме;
– задания для практикума (по вариантам);
– ссылки на программы для решения практических задач.

В настоящее время разработанные электронные пособия используются при выполнении заданий, заданных в рамках самостоятельной работы студентов (СРС).

НЕКОТОРЫЕ АСПЕКТЫ СОЗДАНИЯ ЭЛЕКТРОННОГО УЧЕБНИКА ПО ТЕМЕ “ХРЕСТОМАТИЯ ПО ИСТОРИИ ГОСУДАРСТВА И ПРАВА ЗАРУБЕЖНЫХ СТРАН”

Шаханов С.Н. – студент гр. ПИЮ- 331 ААЭП
Тетерин Ф.И. – студент гр. ПИЮ-331 ААЭП
Шатилов С.П. – доцент кафедры
“Теории и истории государства и права” ААЭП

Возможность повышения эффективности обучения при использовании информационных технологий является в наше время актуальной задачей.

Существующие на сегодняшний день электронные учебники по истории государства и права зарубежных стран немногочисленны и имеют определенные недостатки. В некоторых, например, дан обширный материал с большим количеством иллюстраций, схем и диаграмм, тестами для самоконтроля, однако практически всю информацию, данную в электронном виде, можно прочитать и в традиционном учебнике. Кроме того, огромное количество материала, выходящего далеко за рамки государственных стандартов по дисциплинам естественнонаучного цикла юридических специальностей вузов, делает электронный учебник громоздким и малопригодным в условиях реального учебного процесса. Нам представляется, что электронный учебник должен быть менее объемным, более конкретным и хорошо структурированным.

В связи с вышесказанным, была поставлена задача разработки хорошо структурированного в соответствии с целями и задачами дисциплины "История государства и права зарубежных стран", электронного учебника для студентов юридического факультета Алтайской Академии Экономики и Права. В соответствии с поставленной задачей, нами был разработан гипертекстовый учебник, охватывающий все темы курса, который можно использовать как для непосредственного обучения, так и в качестве конспекта-справочника.

С технологической точки зрения учебник включает: содержание со списком всех параграфов курса; ссылки на теоретические разделы, выделенные шрифтом или фоном с целью облегчить визуальный поиск в тексте.

Учебник хорошо структурирован, что позволяет быстро перемещаться с помощью ссылок между различными разделами, облегчает поиск информации и обеспечивает:
– интуитивно понятную навигацию по курсу;
– возможность возврата к открытому ранее параграфу;
– изменение визуальных размеров учебника на экране наиболее удобным для пользователя образом, а также на полный экран;
– копирование текста в распространенные форматы файловых документов;
– распечатку текстов из учебника на принтере.

Приведем примеры структуры пособия.

Учебное пособие состоит из двух частей:
1) Государство и право древнего мира.
2) Государство и право средних веков.

Часть первая содержит разделы: древний Восток и античность, а вторая: Византия, западная Европа, арабский халифат, средневековый Китай и Япония.

Раздел, посвященный древнему Востоку, в свою очередь, включает главы: древний Египет (О служебных обязанностях везира) [1], Месопотамия (Законы Хаммураби) [2], древняя Индия (Артхашастра Каутильи) [3], древний Китай (Циньское уложение о наказаниях) [4].

Раздел, посвященный античности, включает главы: Древняя Греция (Гортинские законы) [5], древний Рим (Тит Ливии о реформе Сервия Туллия) [6].

Всего при подготовке электронного учебника была использована информация из более чем пятнадцати литературных источников.

Разработанный нами электронный учебник обеспечивает возможность студенту самостоятельно пополнять свои знания по выбранному разделу, а преподавателю - сосредоточить внимание на студентах с низким и средним уровнями подготовки, что позволяет наиболее эффективно донести информацию до студентов.

Следует отметить, что основной недостаток электронного учебника – отсутствие иллюстраций. Планируется дальнейшая доработка, связанная с поиском необходимых рисунков и иллюстраций и включением их в структуру учебника.

Реализация электронного учебника проводилась в 2004/2005 уч.г. на базе второго курса юридического факультета ААЭП, специальность “Прикладная информатика в юриспруденции”. Использование учебника показало, что он способствует формированию информационной культуры будущего юриста, наилучшему усвоению навыков работы с компьютером, повышению эффективности учебного процесса.

Познакомиться с электронным учебником можно на сайте академии: www.aael.altai.ru.

Литература

1. Хрестоматия по истории Древнего мира / Под ред. В. В. Струве; Пер. В. В. Струве. М., 1950. Ч. I. Древний Восток. С. 82-87.
2. Законы Вавилонии, Ассирии и Хеттскою царства / Пер. и коммент. И. М. Дьяконова // Вестник древней истории. 1952. № 3. С. 309—311.
3. Хрестоматия по истории Древнего мира / Под ред. В. В. Струве; Пер. Г. Ф. Ильина. М., 1950. Ч. I. Древний Восток. С. 294-299.
4. Крашенинникова Н. А. История права Востока: Курс лекций. М., 1994.
5. Хрестоматия по истории Древнего мира / Под ред. В. В. Струве. М., 1951. Т. П. Греция и эллинизм. С. 78 — 87.
6. Тит Ливии. Римская история от основания города // Хрестоматия по истории Древнего Рима / Под ред. С. Л. Утченко. М., 1962. С. 49-50.
7. Коран / Пер. И. Ю. Крачковского. М., 1990.

ЭТАПЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВНУТРЕННИХ УГРОЗ

Пишненко А.Г. – аспирант кафедры САПР
Левкин И.В. – к.ф.-м..н., доцент кафедры САПР

Мировая практика свидетельствует о том, что невозможно создать абсолютно защищенную информационную систему. Для обеспечения высокой степени защиты компьютерной информации необходим комплексный подход к информационной безопасности, при котором законодательные, организационные, программно-технические меры и средства защиты используются одновременно, дополняя друг друга.

На основе анализа имеющихся публикаций, посвященных вопросам компьютерной преступности и способам борьбы с нею все множество потенциальных угроз безопасности информации можно разделить на внешние и внутренние. Большинство литературных источников утверждают, что основная опасность исходит именно от внешних угроз. Такая опасность существует и ее нельзя недооценивать. Однако по зарубежной и отечественной статистике до 70-80% всех компьютерных преступлений связывают именно с внутренними нарушениями. Поэтому, говоря об обеспечения информационной безопасности, не стоит забывать и о возможных последствиях непреднамеренных действий (ошибок) со стороны персонала организации или предприятия, ведущих, например, к случайному уничтожению важной информации или сбою системы.

В связи с этим, актуальным является задача обеспечения защиты не только от внешних, но и от внутренних угроз. Эта задача решается в несколько этапов:

1. обеспечение физической защиты компьютерной системы;
2. настройка защиты на уровне аппаратных средств;
3. определение файловой и операционной систем;
4. назначение прав пользователя;
5. настройка политики безопасности пользователя;
6. контроль событий системы.

На первом этапе обеспечивается физическая защита компьютерной системы для контроля несанкционированного доступа к системному блоку ПК. Для этого иногда достаточно прикрутить все винты корпуса компьютера, а места стыков заклеить или поставить пломбы. Нарушение их целостности является признаком вскрытия системного блока.

Вторым этапом обеспечения безопасности компьютера является настройка интерфейсов связи, дисков и других устройств, что позволяет блокировать загрузку ПК с дискеты или с любого другого носителя информации, копировать и удалять данные. Это реализуется с помощью настроек BIOS. Для этого необходимо: установить пароль на BIOS; включить загрузку системы только с жесткого диска и блокировать загрузку с других носителей информации; отключить режим автоопределения дисков; отключить порты, такие как ИК, COM, LPT, USB, а также неиспользуемые слоты.

Следующим этапом является логическое форматирование жесткого диска и установка операционной системы. Целью логического форматирования является создания на диске файловой системы, которая должна обеспечить сочетание производительности, надежности и эффективности безопасности информации. Выбор файловой системы определяется операционной системой. Выбор операционной системы также напрямую зависит от базовых требований к безопасности, в том числе и от реализованных в ней инструментов политики безопасности.

После установки файловой и операционной систем на четвертом этапе администратором создаются учетные записи пользователей, для каждой из которых определяются имя, пароль и время входа в систему. Также для каждой записи администратором назначаются права доступа к компьютерным ресурсам, как в масштабах домена, так и на локальном компьютере. Если существуют учетные записи пользователей с одинаковыми правами, то они объединяются в группы. С помощью введения квот на дисковом пространстве определяется объем данных, которые сможет хранить пользователь.

На пятом этапе определяются следующие настройки:

- политика учетных записей, в том числе, настройка политики паролей, политики блокировки учетных записей;
- локальная политика, с помощью которой настраивается политика аудита, назначаются права пользователя и локальные параметры безопасности;
- журнал событий, который отображает события системы и безопасности;
- системные службы, где устанавливаются параметры загрузки и управления доступом для всех служб;

- параметры управление доступом к разделам реестра системы;
- политика ограниченного использования программ;
- настройка безопасности файловой системы, в том числе настройка параметров доступа к файлам и папкам.

Таким образом, все вышеперечисленные действия позволяют: обеспечить целостность и сохранность данных в неискаженном виде, исключая их случайное уничтожение; ограничить доступ к конфиденциальной, не подлежащей разглашению информации; обеспечить работоспособное состояние операционной системы и прикладных программ.

На завершающем этапе обеспечения безопасности компьютерных систем осуществляется контроль системных событий, которые регистрируются в системных журналах и активизируются автоматически при запуске системы. В журналах отражаются любые значительные происшествия в работе системы или приложениях, о которых следует уведомить системного администратора. Контроль системных событий позволяет вовремя обнаружить несанкционированные, непреднамеренные действия, и предотвратить внутренние угрозы безопасности компьютерной системы.

Таким образом, обеспечение комплексной защиты от внутренних угроз должно быть решено как на программном, так и на аппаратном уровне. Все вышеперечисленные этапы реализации защиты безопасности независимы друг от друга, и последовательность их выполнения определяется администратором. Предлагаемые этапы реализуют грамотную политику комплексной защиты компьютерных систем от внутренних угроз, которая в том числе должна обеспечивать правильное распределение прав доступа пользователей, своевременную смену паролей, мониторинг и контроль соблюдения политик безопасности.

В свою очередь, не стоит забывать, что обеспечение безопасности – это не разовая акция, а постоянный процесс, который должен обеспечиваться в компьютерной системе в течение всего рабочего цикла.

Автором данной работы разрабатывается автоматизированная система мониторинга работы пользователей с целью диагностики компьютерных сетей.