ПРОБЛЕМЫ И КОЛЛИЗИИ В ПРАВОВОМ РЕГУЛИРОВАНИИ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ: КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пырх А.В., Пыжик В.В.

Характерной особенностью развития общества в современных условиях является активное развитие процессов информатизации, обусловливающих развитие автоматизированных систем и средств коммуникации, средств распространения и обмена информацией посредством в т.ч. глобальной сети Интернет и т.д. Одной из основных целей государственной политики в области информатизации является создание органами государственной власти необходимых правовых условий, обеспечивающих развитие процессов информатизации для защиты прав и законных интересов граждан и государства, с целью перехода к новому этапу развития страны - построению информационного общества и вступлению республики в мировое информационное сообщество. Как указано в Концепции государственной политики в области информатизации [1], система информационного законодательства выступает одним из системообразующих факторов всей государственной политики в этой сфере. Таким образом, становление информационного законодательства является одной из важнейших задач государственной политики в области информатизации и основным способом в решении проблем правового обеспечения информационного общества на национальном уровне [2; с. 41]. Следовательно, вторым направлением является разработка теоретических основ информационного права - новой комплексной отрасли права, обеспечивающей эффективное регулирование общественных отношений в информационной сфере, а также исследование основных предметов правового регулирования этого права - информационных отношений, основных объектов информационных отношений - информации, информационных процессов, информационных систем [2; с. 42]. На данный момент времени оно уже включено в Номенклатуру специальностей научных работников Республики Беларусь [3] в состав специальности 12.00.14 "Административное право; финансовое право; информационное право". Однако, информационное право не является ни частью административного, ни частью финансового права, поэтому было бы целесообразно либо выделить его в отдельную специальность, либо, что наиболее приемлемо, - вернуть специальность 12.00.13 "Управление в социальных экономических системах (юридические аспекты); правовая информатика; применение математических методов и вычислительной техники в юридической деятельности" и присоединить его к ней, либо, в крайнем случае, ввести его в состав специальности 12.00.01 "Теория и история права и государства; история правовых учений". В сферу информационного права попадает: правовое регулирование вопросов, связанных с телекоммуникациями, информационными технологиями и передачей информации, в том числе правовое регулирование предоставления информации в глобальных информационных сетях; защита интеллектуальной собственности; правовые вопросы, связанные с созданием информации, ее распространением и предоставлением в пользование; предупреждение преступлений в вышеназванных сферах [2; с. 44]. К сожалению, законодательство в области информатизации не развивается достаточно планомерно, Закон "Об информатизации" был принят 6 сентября 1995 г. [4], а наиболее развитым и системным является законодательство в области создания и развития государственной системы правовой информации. Более того, в области информатизации в настоящий момент технологическая составляющая преобладает над правовой регламентацией вопросов создания и использования информационных ресурсов. Не находят своевременной правовой регламентации такие вопросы, как сертификация информационной продукции и средств технического и технологического комплекса, информационная безопасность, защита персональных данных и информационных ресурсов от несанкционированного доступа, правовая защита результатов интеллектуального труда, электронный документооборот и т.д.

В связи с тем, что в стадии разработки находится Программа информатизации Республики Беларусь, предусматривающая раздел по правовому обеспечению информатизации, по инициативе НЦПИ в проект Указа Президента Республики Беларусь "Об одобрении Государственной программы подготовки проектов нормативных правовых актов Республики Беларусь на 2003-2005 годы" внесены предложения по разработке правовых актов, регламентирующих деятельность в области информационных технологий, что в дальнейшем позволит обеспечить вхождение Республики Беларусь в информационное пространство мирового сообщества. Так, данным проектом Указа предусматриваются разработка и принятие нового комплексного закона "Об информации и информатизации", регулирующего прежде всего не сферу технократическую, а сферу создания и доступа к информационным ресурсам.

В принципе, приоритетные направления деятельности органов государственного управления в сфере информатизации определены в Концепции государственной политики в области информатизации [1]. В соответствии с ними должна развиваться и законодательная поддержка процессов информатизации.

Однако информатизация деятельности государственных и коммерческих органов, появление Интернета ведут не только к прогрессу, но и к использованию этих технологий в совершенно иных целях, в том числе и в преступных. Появление такого явления, как компьютерная преступность, обусловило разработку теоретических и практических аспектов борьбы с этим новым видом преступности. При этом необходимо было дать комплексную оценку подобного явления, выработать методики раскрытия и расследования преступлений, связанных с посягательством на компьютерную информацию.

Для организации эффективной борьбы с компьютерными преступлениями прежде всего необходимо было определить отношения, складывающиеся в информационной сфере, характеризующиеся несколькими

аспектами. Это - субъективный (право, принадлежащее конкретному лицу) и объективный (правовые нормы, регламентирующие дозволения на совершение определенных действий субъекта) состав нарушений, а также перечень деяний (нарушений) в сфере компьютерной информации и информационных технологий. Европейским Советом был согласован и утвержден Список правонарушений, рекомендованный странам-участницам ЕС для разработки единой уголовной стратегии по разработке законодательства, связанного с компьютерными преступлениями. Минимальный список нарушений содержит несколько видов компьютерных преступлений:

- компьютерное мошенничество;
- подделка компьютерной информации;
- повреждение данных ЭВМ или программных средств ЭВМ;
- компьютерный саботаж;
- несанкционированный доступ к информации;
- несанкционированный перехват данных;
- несанкционированное использование защищенных компьютерных программ;
- несанкционированное производство схем;
- изменение данных ЭВМ или программ ЭВМ;
- компьютерный шпионаж;
- несанкционированное использование ЭВМ;
- несанкционированное использование защищенных программ ЭВМ [5; с. 225].

Определение этих видов противоправных деяний в информационной сфере направлено, прежде всего, на обеспечение информационной безопасности государства. Развитие и распространение компьютерных систем и сетей, сопровождающиеся ростом правонарушений, связаны с кражами, злоупотреблениями, модификацией и несанкционированным доступом к данным, хранящимся в памяти компьютеров и передаваемых по линиям связи, что и определяет состав этих преступлений. Так, в 1998 году неустановленными взломщиками была предпринята попытка несанкционированного доступа к информационным ресурсам Администрации Президента Республики Беларусь. В 2000 году в нескольких торговых точках г. Минска впервые были совершены мошеннические действия с использованием поддельных пластиковых кредитных карт типа "MasterCard". Преступники использовали поддельные карточки в магазинах, где имелись устройства для считывания реквизитов [6; с. 361]. В настоящее время поток подобного рода преступлений все больше увеличивается. Поэтому организация эффективной борьбы с преступностью, в частности, с компьютерной, в особенности с ее организованными проявлениями, является первостепенной задачей. Отнесение "развития информационных технологий и защиты сведений, составляющих государственную, служебную, коммерческую и иную, охраняемую законом тайну, развитие современных информационных технологий, обеспечение безопасности информационных систем и сетей и т.д." в соответствии с Концепцией национальной безопасности Республики Беларусь к "жизненно важным интересам Республики Беларусь в информационной сфере" ставит проблему борьбы с компьютерной преступностью в разряд приоритетных [7]. В этой связи обеспечение информационной безопасности становится важным элементом национальной и международной безопасности. Это понятие включает в себя не только защиту информационных ресурсов от несанкционированного доступа, но и общие принципы функционирования информационных ресурсов страны, защите важнейших информационных и телекоммуникационных систем, обеспечивающих эффективность деятельности наиболее важных отраслей промышленности, банковской сферы, государственных органов и т.д.

Развитие научных исследований по этой группе преступлений, а также совершенствование законодательства по уголовно-правовой защите за последнее время характеризуются активизацией научных разработок и совершенствованием законодательства. Так, в новом Уголовном кодексе Республики Беларусь содержится специальная глава "Преступления против информационной безопасности", в которой в соответствии со ст. 349-355 закреплены нормы, устанавливающие уголовную ответственность за несанкционированный доступ к компьютерной информации, модификацию компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией, изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети. Вместе с тем, компьютерные преступления характеризуются высокой степенью латентности, сложностью сбора улик по установленным фактам, сложностью обеспечения доказательств для рассмотрения дел этой категории в суде.

Одной из важнейших задач информатизации республики является развитие системы электронного документооборота и его повсеместное внедрение в деятельность всех предприятий, организаций, учреждений и государственных структур. Существенное значение в эффективности информационной безопасности имеет электронная цифровая подпись, которая должна входить в состав документа на электронных носителях, поскольку конечным продуктом, реализующим преступный замысел, часто является документ, изготовленный с помощью компьютерных средств. Вопросы формирования документов на электронных носителях отображает Закон Республики Беларусь от 10 января 2000 г. "Об электронном документе", регламентирующий правоотношения в сфере электронного документооборота с четким предъявлением требований к электронному документу, его структуре и т.д.

Самым основным является то обстоятельство, что электронный документ приравнен к документу на бумажном носителе и имеет с ним одинаковую юридическую силу. Если по законодательству Республики Беларусь требуется, чтобы документ был "письменным" в "письменном виде" или в "письменной форме", то при соблюдении определенных условий электронный документ считается соответствующим этим требованиям (ст. 11 Закона "Об электронном документе [8]).

Изготовление документа с помощью компьютера распадается на два этапа и предполагает наличие конкретного сочетания аппаратных и программных средств. Вначале информация вводится в компьютер с клавиатуры или иным способом (например, введена с дискеты или глобальной сети) [5; с. 362]. Затем она

корректируется и может быть распечатана с использованием печатающих средств компьютера. При перенесении информации для ее последующего вывода на печатающее устройство возможно тиражирование информации. При этом происходит также и тиражирование авторских признаков, сохраняющихся в электронном документе, и особенностей операторской работы. При таких условиях большое значение начинает играть подтверждение достоверности электронного документа. Подлинность электронного документа обеспечивается, если имеются надежные доказательства целостности и неизменности информации, зафиксированной в электронном документе, такие, как электронная цифровая подпись (далее - ЭЦП).

ЭЦП - удобное и полезное средство, но ей присущи также органические недостатки, связанные с тем, что ключ подписи не является полным аналогом собственноручной подписи и не является неотъемлемым атрибутом идентификации личности. В случае утраты контроля за подписью конкретным человеком эти недостатки могут использоваться в преступных целях. В результате подпись может быть скопирована и использована в преступных целях.

Интересно отметить то обстоятельство, что в рамках Российской Федерации признается существование электронной цифровой подписи, принадлежащей только физическому лицу, в Республике Беларусь ЭЦП может принадлежать и юридическому лицу. Так как ЭЦП еще не используется на практике, трудно сказать, является ли преимуществом данный факт. Но уже можно увидеть некоторые проблемы, которые будут возникать в связи с применением ЭЦП. Подпись является атрибутом документа и должна следовать за документом или за пакетом документов, который сам на самом деле будет являться документом. Но вопрос о пакетах документов: подписывать и обрабатывать ли каждый из документов или в целом всю их пачку, не рассмотрен законодателем.

Кроме того, необходимо предусмотреть вопрос о регистрации ЭЦП у системного администратора, уполномоченного на осуществление такого вида деятельности в информационных системах. Этот вопрос встает особенно остро, так как необходимо уже сейчас определить, какие конкретно учреждения, органы и организации будут осуществлять функцию по сертификации этих средств защиты, а также какие органы будут осуществлять функции "электронного нотариуса".

Список использованных источников:

1. Национальный реестр правовых актов Республики Беларусь, 1999 г. - № 28, 1/231.
2. Сатолина М.Н. Вопросы правового обеспечения государственной политики в области информатизации.// Вестник молодежного научного общества, 2000 г., № 3, с. 40-47.
3. Постановление Государственного высшего аттестационного комитета Республики Беларусь от 5.12.1995 г. № 125 "Аб зацвярджэнні Наменклатуры спецыяльнасцяў навуковых работнікаў Рэспублікі Беларусь" в ред. постановления Государственного высшего аттестационного комитета Республики Беларусь от 4.05.2000 г. № 11-Д "О внесении изменений и дополнений в Номенклатуру специальностей научных работников Республики Беларусь".// Национальный реестр правовых актов Республики Беларусь, 2000 г., № 52, 8/3478.
4. Ведомости Верховного Совета Республики Беларусь, 1995 г., № 33, ст. 428.
5. Компьютерная преступность и информационная безопасность/ Под общей редакцией А.П.Леонова. - Мн.: Арил, 2000 г.
6. Черненко И.Т. О состоянии борьбы с компьютерной преступностью в Республике Беларусь.//Российско-белорусский науч.-практ. журнал "Управление защитой информации". - 2002. - Т. 6. - № 3, с. 360-368.
7. Указ Президента Республики Беларусь от 17.07.2001 г. № 390 "Об утверждении Концепции национальной безопасности Республики Беларусь". //Национальный реестр правовых актов Республики Беларусь, 2001 г. - № 69, 1/2852.
8. Закон Республики Беларусь от 10.01.2000 г. "Об электронном документе". //Национальный реестр правовых актов Республики Беларусь, 2000 г., № 7, 2/132.

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ WebVR В УЧЕБНОМ ПРОЦЕССЕ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Стогначёв Р. В., Чаускин Р.С.

В настоящее время существует множество подходов и практик по улучшению учебного процесса. Одни из них направлены на улучшение и доработку уже существующих методик, другие на инновационно новый подход в данной области. Технология WebVR - Web Virtual Reality относится как-раз ко второму типу.

WebVR технология и одноимённая JavaScript библиотека позволяют создавать приложения, способные погрузить пользователя в виртуальный мир. Для этого потребуется устройство, способное отображать 3d изображение, такое как Oculus Rift или Google Cardboard и специально разработанное П.О.

Используя данный подход можно смоделировать различные ситуации которые трудно и ресурсоёмко производить в повседневной реальности. В пределах университета это могут быть практические занятия студентов обучающихся для работы на АЭС, или студентов военных специальностей, которые могут отрабатывать навыки работы с военной техникой в виртуальном мире, и переходить к реальной практике уже после уверенного закрепления материала.

Сегодня в мире уже известны приборы погружения человека в виртуальлною реальность, есть множество различных симуляторов. Преимущество технологии WebVR перед уже существующими технологиями заключается в том, что данный метод позволяет располагать приложение в одном месте(на сервере) и предоставлять доступ конечному пользователю через сеть Интернет (или внутреннюю сеть учреждения), используя свой П.К. .Тогда как все известные симуляторы виртуальной реальности требуют покупку дорогостоящего оборудования и пригодны обычно для узкого спектра задач.

На рисунке 1 и 2 приведено сравнение использования двух технологий