Тема: «Правовые основы обеспечения информационной безопасности»

Цель урока: *знакомство с правовыми нормами информационной деятельности человека, с особенностями информационной деятельности человека и проблемами, возникающими при взаимодействии общества и человека при рассмотрении информационного продукта как объекта собственности; рассмотреть правовые нормы информационной деятельности человека и познакомиться с составляющими информационной безопасности*.

Лицензионное соглашение, информационная безопасность, защита информации.

В современном обществе большинство людей занято деятельностью в информационной сфере, то есть сфере деятельности, связанной с созданием, преобразованием и потреблением информации. В основе производства, распространения, преобразования и потребления информации лежат информационные процессы сбора, создания, обработки, накопления, хранения, поиска информации в обществе**,** а также процессы создания и применения информационных систем и технологий.

При выполнении рассмотренных информационных процессов возникают социальные (общественные) отношения, которые подлежат правовому регулированию. Соответственно объектом правовых взаимоотношений выступает информация.

Закон РФ № 3523-1 «О правовой охране программ для ЭВМ и баз данных» дает юридически точное определение понятий, связанных с авторством и распространением компьютерных программ и баз данных. Он определяет, что ***авторское право*** распространяется на указанные объекты, являющиеся результатом творческой деятельности автора. Автор (или авторы) имеет исключительное право на выпуск в свет программ и баз данных, их распространение, модификацию и иное использование. Однако ***имущественные права*** на указанные объекты, созданные в порядке выполнения служебных обязанностей или по заданию работодателя, принадлежат работодателю. Имущественные права, в отличие от авторских, могут быть переданы иному физическому или юридическому лицу на договорной основе.

Закон РФ №149-ФЗ «Об информации, информационных технологиях и защите информации» регулирует отношения, возникающие при: осуществлении права на поиск, получение, передачу и производство информации; применении информационных технологий; обеспечении защиты информации. В частности, в статье 8 «Право на доступ к информации» утверждается право гражданина на получение из официальных источников информации о деятельности государственных органов, об использовании бюджетных средств, о состоянии окружающей среды, и пр., а также любой информации, непосредственно затрагивающей его права и свободы. Ограничение доступа к информации устанавливается только федеральными законами, направленными на обеспечение государственной безопасности.

В статье 12 «Государственное регулирование в сфере применения информационных технологий», в частности, отмечается, что обязанностью государства является создание условий для эффективного использования в Российский Федерации информационно-телекоммуникационных сетей, в том числе Интернета.

Особое внимание обратим на статью 3, в которой среди принципов правового регулирования в информационной сфере провозглашается принцип неприкосновенности частной жизни, недопустимость сбора, хранения использования и распространения информации о частной жизни лица без его согласия.

В 2006 году вступил в силу **закон №152-0ФЗ «О персональных данных»,** целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных (с использованием средств автоматизации или без использования таких), в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В 1996 году в Уголовный кодекс был впервые внесён раздел «Преступления в сфере компьютерной информации». Он определил меру наказания за некоторые виды преступлений:

- ✓ неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации;
- ✓ создание, распространение или использование вредоносных компьютерных программ;
- ✓ нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование информации.

В современном информационном обществе информация является товаром. Производство программ и информационных ресурсов ведется в индустриальных масштабах, над ними работают коллективы профессиональных программистов.

Основой правовых отношений между пользователем и собственником программного обеспечения является ***лицензия*** — это документ, определяющий порядок использования и распространения программного обеспечения, защищённого авторским правом.

Производимые программные продукты по условиям распространения можно разделить на четыре группы:

- ✓ лицензируемые;
- ✓ условно бесплатные (shareware, trial, демо);
- ✓ распространяемые бесплатно (freeware);
- ✓ распространяемые свободно в виде исходных кодов (free software).

Форма, в которой распространяется программный продукт, называется его ***дистрибутивом***. Дистрибутивы ***лицензируемых*** программ распространяются фирмой-продавцом на основании договора с покупателем на платной основе.

Некоторые фирмы-разработчики предлагают ***условно бесплатные*** программные продукты (shareware) в целях рекламы. Пользователю предоставляется версия программы с ограниченным сроком действия (trial-программа перестает работать по истечении определенного срока или количества запусков, если за нее не произведена оплата) или версия программы с ограниченными функциональными возможностями (демоверсия).

Фирмы-разработчики программного обеспечения могут быть также заинтересованы в широком распространении бесплатных программ (freeware). К таким программным продуктам относятся: новые, ещё недоработанные версии программ, требующие широкого тестирования; программы, представляющие принципиально новые технологии (что позволяет разработчику провести маркетинговые исследования); дополнения к ранее выпущенным программным продуктам, расширяющие их возможности или исправляющие найденные ошибки; устаревшие версии программ; драйверы к новым устройствам.

Программы с открытым кодом (free software, свободное программное обеспечение) распространяются с разрешением использовать, копировать и распространять их (в том числе с модификациями безвозмездно или за плату). Это также означает общедоступность исходных текстов программ, в которые любой желающий может вносить изменения.

Программа считается свободно распространяемой, если пользователи располагают следующими четырьмя свободами:

- ✓ свободой запуска программы в любых целях;

- ✓ свободой изучения работы программы и ее адаптации к своим нуждам;
- ✓ свободой копирования и распространения;
- ✓ свободой улучшать программу и публиковать эти улучшения для пользования всеми желающими, причем как для исходной, так и для улучшенной программы должны быть опубликованы исходные коды.

Однако при всем этом остается единственное ограничение: никто не может присвоить себе права на эту программу, поскольку не является единственным ее автором, и никто не может запретить другим лицам пользоваться ею.

По мере продвижения к информационному обществу всё более острой становится проблема защиты права личности, общества и государства на конфиденциальность определённых видов информации. Другими словами, всё более острой становится проблема **информационной безопасности:** защищённости информации и поддерживающей инфраструктуры информационной системы от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб субъектам информационных отношений (владельцам и пользователям информации) в рамках данной информационной системы.

Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная, или например, физическая). Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных.

Доступность информации — это состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно и в течение приемлемого времени. К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

Целостность информации — это свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в смысловом отношении от данных в исходных документах, т. е. если не произошло их случайного или намеренного искажения, или разрушения.

Конфиденциальность информации — это статус, предоставленный информации или данным и определяющий требуемую степень их защиты. К конфиденциальным данным можно отнести, например, личную информацию пользователей, учётные записи (имена и пароли), данные о кредитных картах, данные о разработках и различные внутренние документы, бухгалтерские сведения. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы это информация должна быть недоступна.

Это достигается, в основном, посредством многоэтапного процесса управления рисками, который позволяет идентифицировать основные средства и нематериальные активы, источники угроз, уязвимости, потенциальную степень воздействия и возможности управления рисками. Этот процесс сопровождается оценкой эффективности плана по управлению рисками.

Для того чтобы стандартизовать эту деятельность, научное и профессиональное сообщества находятся в постоянном сотрудничестве, направленном на выработку базовой методологии, политик и индустриальных стандартов в области технических мер защиты информации, юридической ответственности, а также стандартов обучения пользователей и администраторов. Эта стандартизация в значительной мере развивается под влиянием широкого спектра законодательных и нормативных актов, которые регулируют способы доступа, обработки, хранения и передачи данных.

Проблемы информационной безопасности в России регламентируются **Доктриной информационной безопасности Российской Федерации**, согласно которой под информационной безопасностью Российской Федерации понимается состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В доктрине выделены четыре основные составляющие национальных интересов Российской Федерации в информационной сфере:

- ✓ соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею;
- ✓ обеспечение духовного обновления России; сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;
- ✓ информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, её официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;
- ✓ развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи; обеспечение потребностей внутреннего рынка её продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- ✓ защита информационных ресурсов от несанкционированного доступа; обеспечение безопасности информационных и телекоммуникационных систем, как уже развёрнутых, так и создаваемых на территории России.

В доктрине описаны правовые, организационно-технические и экономические методы обеспечения информационной безопасности Российской Федерации, приведены основные положения государственной политики и представлены организационные основы обеспечения информационной безопасности нашей страны.

Тема: «Защита информации. Антивирусные программы»

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Различают **несанкционированное** и **непреднамеренное** воздействие на информацию.

Несанкционированным является воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. Такого рода воздействие на информацию или ресурсы информационной системы может осуществляться с помощью вредоносных программ (вирусов).

Компьютерный вирус — это специальная программа, способная самопроизвольно присоединяться к другим программам и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов; искажение результатов вычислений; засорение или стирание памяти; создание помех в работе компьютера. Наличие вирусов проявляется в разных ситуациях. Некоторые программы перестают работать или начинают работать некорректно. На экран выводятся посторонние сообщения, сигналы и другие эффекты.

Работа компьютера существенно замедляется. Структура некоторых файлов оказывается испорченной.

Имеются несколько признаков классификации существующих вирусов. Например, по способу заражения различают троянские программы, утилиты скрытого администрирования, Intended-вирусы и т. д. Троянские программы получили свое название по аналогии с троянским конем. Назначение этих программ — имитация каких-либо полезных программ, новых версий популярных утилит или дополнений к ним. При их записи пользователем на свой компьютер троянские программы активизируются и выполняют нежелательные действия. Разновидностью троянских программ являются утилиты скрытого администрирования. По своей функциональности и интерфейсу они во многом напоминают системы администрирования компьютеров в сети, разрабатываемые и распространяемые различными фирмами — производителями программных продуктов. При инсталляции эти утилиты самостоятельно устанавливают на компьютере систему скрытого удаленного управления. В результате возникает возможность скрытого управления этим компьютером. Реализуя заложенные алгоритмы, утилиты без ведома пользователя принимают, запускают или отсылают файлы, уничтожают информацию, перезагружают компьютер и так далее. Возможно использование этих утилит для обнаружения и передачи паролей и иной конфиденциальной информации, запуска вирусов, уничтожения данных. К Intended-вирусам относятся программы, которые не способны размножаться из-за существующих в них ошибок. К этому классу также можно отнести вирусы, которые размножаются только один раз. Заразив какой-либо файл, они теряют способность к дальнейшему размножению через него.

По деструктивным возможностям вирусы разделяются на:

1. Неопасные, влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическим и звуковыми эффектами.
2. Опасные, которые потенциально могут привести к нарушениям в структуре файлов и сбоям в работе компьютера.
3. Очень опасные, в алгоритм которых специально заложены процедуры уничтожения данных и возможность обеспечивать быстрый износ движущихся частей механизмов.

Для борьбы с вирусами существуют программы, которые можно разбить на основные группы: мониторы, детекторы, доктора, ревизоры и вакцины.

Программы мониторы (***программы-фильтры***) располагаются резидентно в оперативной памяти компьютера, перехватывают и сообщают пользователю об обращениях операционной системы, которые используются вирусами для размножения и нанесения ущерба. Пользователь имеет возможность разрешить или запретить выполнение этих обращений. К преимуществу таких программ относится возможность обнаружения неизвестных вирусов. Использование программ-фильтров позволяет обнаруживать вирусы на ранней стадии заражения компьютера. Недостатками программ являются невозможность отслеживания вирусов, обращающихся непосредственно к BIOS, а также загрузочных вирусов, активизирующихся до запуска антивируса при загрузке DOS, и частая выдача запросов на выполнение операций.

Программы-детекторы проверяют, имеется ли в файлах и на дисках специфическая для данного вируса комбинация байтов. При ее обнаружении выводится соответствующее сообщение. Недостаток — возможность защиты только от известных вирусов.

Программы-доктора восстанавливают зараженные программы путем удаления из них тела вируса. Обычно эти программы рассчитаны на конкретные типы вирусов и основаны на сравнении последовательности кодов, содержащихся в теле вируса, с кодами проверяемых программ. Программы-доктора необходимо периодически обновлять с целью получения новых версий, обнаруживающих новые виды вирусов.

Программы-ревизоры анализируют изменения состояния файлов и системных областей диска. Проверяют состояние загрузочного сектора и таблицы FAT; длину, атрибуты и время создания файлов; контрольную сумму кодов. Пользователю сообщается о выявлении несоответствия.

Программы-вакцины модифицируют программы и риски так, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает программы или диски уже зараженными. Существующие антивирусные программы в основном относятся к классу гибридных (детекторы-доктора, доктора-ревизоры и пр.).

Так же информация может быть утеряна, искажена или блокирована **непреднамеренно**, например, из-за ошибочного действия пользователя или сбоя оборудования. Для предотвращения этого создаются резервные копии программ и документов. А большинство современных средств информационных технологий предусматривают автоматическое сохранение информационного продукта в ходе его разработки.

Защита от случайной потери или изменения информации осуществляется в основном следующими материалами:

— обязательным запросом на подтверждение команды, приводящей к изменению содержания какого-либо файла или группы файлов;

— установкой атрибутов, ограничивающий возможность изменения файла (например, с помощью атрибута *«только для чтения»);*

— возможностью отменить последнее действие;

— разграничением доступа пользователей к ресурсам, в частности с помощью системы паролей.