Содержание:

Введение

В информационном обществе главным ресурсом является информация. Именно на основе владения информацией о самых различных процессах и явлениях можно эффективно и оптимально строить любую деятельность.

Важно не только произвести большое количество продукции, но произвести нужную продукцию в определённое время. С определёнными затратами и так далее. Поэтому в информационном обществе повышается не только качество потребления, но и качество производства; человек, использующий информационные технологии, имеет лучшие условия труда, труд становится творческим, интеллектуальным и так далее.

В настоящее время развитые страны мира (США, Япония, страны Западной Европы) фактически уже вступили в информационное общество. Другие же, в том числе и Россия, находятся на ближних подступах к нему.

В качестве критериев развитости информационного общества можно выбрать три: наличие компьютеров, уровень развития компьютерных сетей и количество населения, занятого в информационной сфере, а также использующего информационные и коммуникационные технологии в своей повседневной деятельности.

Информация сегодня стоит дорого и её необходимо охранять. Массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру накопителей и наносящих ущерб хранимой в компьютере информации.

Информацией владеют и используют её все люди без исключения. Каждый человек решает для себя, какую информацию ему необходимо получить, какая информация не должна быть доступна другим и т.д. Человеку легко, хранить информацию, которая у него в голове, а как быть, если информация занесена в «мозг машины», к

которой имеют доступ многие люди.

Для предотвращения потери информации разрабатываются различные механизмы её защиты, которые используются на всех этапах работы с ней. Защищать от повреждений и внешних воздействий надо и устройства, на которых хранится секретная и важная информация, и каналы связи.

Повреждения могут быть вызваны поломкой оборудования или канала связи, подделкой или разглашением секретной информации. Внешние воздействия

возникают как в результате стихийных бедствий, так и в результате сбоев оборудования или кражи.

Глава 1. Понятие компьютерной информации.

Компьютерная информация — это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ. Совокупность данных, зафиксированных на материальном носителе и/или передаваемых по электронным каналам связи с реквизитами, позволяющими идентифицировать эту информацию и ее автора. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа либо порождаться в процессе информационного взаимодействия Сторон без каких-либо прообразов.

В уголовном законодательстве используются термины и выражения разного вида, в частности, общеупотребительные, юридические и технические. Как составной термин «компьютерная информация» не может быть целиком отнесен к одному классу. Он опирается на весьма развитое общеупотребимое понятие «информация», применение которого, однако, в правовой деятельности, как правило, сопровождается отсылкой к его легальному определению в ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации». Специальное значение употребленного в УК РФ термина «информация» подчеркивается данным к нему определением «компьютерная». Таким образом, компьютерная информация, о которой идет речь в ст. 273 УК РФ - это разновидность информации, защищаемой специальными нормами уголовного закона от определенных воздействий и определенных последствий воздействия.

Представление компьютерной информации осуществляется с помощью языка, содержащего всего два символа алфавита — 0 и 1. Инженеров такой способ представления информации привлек простотой технической реализации

проблемы кодирования. Легко различимые состояния — есть электрический сигнал (1) или нет сигнала (0) позволяют разными способами двоичного кодирования и декодирования, в основе которых лежат логика и математика, распознать и обработать техническими средствами для достижения поставленной задачи любые сведения (сообщения, данные).

Глава 2. Классификация и характеристика вирусов

Угроза информационному ресурсу возрастает с каждым днем, подвергая в панику ответственных лиц в банках, на предприятиях и в компаниях во всем мире. И угроза эта исходит от компьютерных вирусов, которые искажают или уничтожают жизненно важную, ценную информацию, что может привести к очень серьёзным последствиям.

Компьютерный вирус — вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, и распространять свои копии по разнообразным каналам связи. Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов и даже удаление операционной системы, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

Ныне существует немало разновидностей вирусов, насчитывают на данный момент около 100 000, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через локальные и глобальные (Интернет) сети. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

-по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);

файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.

-по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Android);

-по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);

-по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);

-по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

Вирусы распространяются, копируя своё тело и обеспечивая его последующее исполнение: вписывая себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск через реестр и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды, — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении, для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплойтом, использующим уязвимость.

После того как вирус успешно внедрился в коды программы, файла или документа, он будет находиться в состоянии сна, пока обстоятельства не заставят компьютер или устройство выполнить его код. Чтобы вирус заразил ваш компьютер, необходимо запустить заражённую программу, которая, в свою очередь, приведёт к выполнению кода вируса. Это означает, что вирус может оставаться бездействующим на компьютере без каких-либо симптомов поражения.

Однако, как только вирус начинает действовать, он может заражать другие файлы и компьютеры, находящиеся в одной сети. В зависимости от целей программиста-вирусописателя, вирусы либо причиняют незначительный вред, либо имеют разрушительный эффект, например, удаление данных или кража конфиденциальной информации.

Глава 3.Защита компьютера от вирусов

МЕТОДЫ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

-общие средства защиты информации, которые полезны также и как страховка от порчи дисков, неправильно работающих программ или ошибочных действий пользователя;

-профилактические меры, позволяющие уменьшить вероятность заражения вирусов;

-специальные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

-копирование информации - создание копий файлов и системных областей диска;

- средства разграничения доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователя.

Общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы). ДЕТЕКТОРЫ позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах

на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны".

Программа Scan McAfeeAssociates и Aidstest позволяют обнаруживать всего несколько тысяч вирусов, но всего их более 80 тысяч! Некоторые программы-детекторы, например, NortonAntiVirus или AVSP, могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам. Тем не менее, невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова - в ней могут сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, неизвестные программам-детекторам.

Многие программы-детекторы (в том числе и Aidstest) не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Дело в том, что для чтения диска они используют функции DOS, перехватываются вирусом, который говорит, что все хорошо. Правда, Aidstest и др. программы могут выявить вирус путем просмотра оперативной памяти, но против некоторых "хитрых" вирусов это не помогает. Так что надежный диагноз программы-детекторы дают только при загрузке DOS с защищенной от записи дискеты, при этом копия программы-детектора также должна быть запущена с этой дискеты.

Некоторые детекторы, скажем, ADinf "Диалог-Наука", умеют ловить "невидимые" вирусы, даже когда они активны. Для этого они читают диск, не используя вызовы DOS. Этот метод работает не на всех дисководах.

Большинство программ-детекторов имеют функцию "доктора», т.е. пытаются вернуть зараженные файлы или области диска в их исходное состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или, удаляются.

Большинство программ-докторов умеют "лечить" только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам

лечения новых вирусов.

К таким программам относится AVSP «Диалог-МГУ".

ПРОГРАММЫ-РЕВИЗОРЫ имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Чтобы проверка состояния программ и дисков проходила при каждой загрузке операционной системы, необходимо включить команду запуска программы-ревизора в командный файл AUTOEXEC.BAT. Это позволяет обнаружить заражение компьютерным вирусом, когда он еще не успел нанести большого вреда. Более того, та же программа-ревизор сможет найти поврежденные вирусом файлы.

Многие программы-ревизоры являются довольно "интеллектуальными" - они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Понятно, что в нормальной ситуации такие изменения практически никогда не встречаются, поэтому программа-ревизор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они вызваны именно вирусом.

Следует заметить, что многие программы-ревизоры не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Но некоторые программы-ревизоры, например, ADinf фи "Диалог-Наука", все же умеют делать это, не используя вызовы DOS для чтения диска (правда, они работают не на всех дисководах). Увы, против некоторых "хитрых" вирусов все это бесполезно.

Для проверки того, не изменился ли файл, некоторые программы-ревизоры проверяют длину файла. Но эта проверка недостаточна - некоторые вирусы не изменяют длину зараженных файлов. Более надежная проверка - прочесть весь файл и вычислить его контрольную сумму. Изменить файл так, чтобы его контрольная сумма осталась прежней, практически невозможно.

В последнее время появились очень полезные гибриды ревизоров и докторов, т.е. ДОКТОРА-РЕВИЗОРЫ - программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние. Такие программы могут быть гораздо более универсальными, чем программы-доктора, поскольку при лечении они используют заранее сохраненную информацию о состоянии файлов и областей дисков. Это позволяет им вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы.

Но они могут лечить не от всех вирусов, а только от тех, которые используют

"стандартные", известные на момент написания программы, механизмы заражения файлов.

Существуют также ПРОГРАММЫ-ФИЛЬТРЫ, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о

них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

ПРОГРАММЫ-ВАКЦИНЫ, или ИММУНИЗАТОРЫ, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Глава 4. Защита от несанкционированного доступа

Современные компании располагают значительными объемами информации. В сегодняшних реалиях она является основным ресурсом. Базы данных нуждаются в надежной охране от преступного использования, которое представляет собой серьезную угрозу для деятельности и существования компании. Поэтому так важно обеспечить защиту данных от несанкционированного доступа. Это комплекс мероприятий, направленных на контроль полномочий пользователей. В компании вводится ограничение использования сведений, которые не нужны сотрудникам для выполнения прямых обязанностей. Контролировать необходимо действия как с бумажными документами, так и со сведениями на электронных носителях информации.

Для того чтобы создать надежную систему защиты информации нужно определить возможные способы получения данных.

Несанкционированный доступ к информации (НСД) может быть получен разными способами. Прямое хищение документов или взлом операционных систем компьютеров составляют лишь малую часть возможных вариантов. Наиболее уязвимыми считаются электронные средства хранения информации, так как для них могут быть использованы удаленные методы управления и контроля.

Возможные варианты получения незаконного доступа:

подключение к системам связи (телефонные линии, интеркомы, проводные переговорные устройства);

хищение документации, в том числе ее копирование (тиражирование) с враждебными целями;

непосредственное использование компьютеров, внешних накопителей или иных устройств, содержащих информацию;

внедрение в операционную систему через Интернет, в том числе с использованием шпионских программ, вирусов и прочего вредоносного программного обеспечения;

использование сотрудников компании (инсайдеров) в качестве источников сведений.

Подключение к действующему каналу связи позволяет получать сведения косвенным способом, без непосредственного доступа к базам данных. Наиболее защищенными от вторжения извне считаются оптоволоконные линии, но и к ним можно присоединиться после некоторых подготовительных операций. Целью

злоумышленников в этом случае становятся рабочие переговоры сотрудников – например, при проведении следственных мероприятий или при совершении финансовых операций.

Часто для получения нужных сведений злоумышленники используют сотрудников компаний. В ход идут разные способы убеждения и мотивации – от подкупа до более жестких методов (запугивание, шантаж). В группу риска входят сотрудники, у которых возник конфликт с коллегами или с администрацией компании. Эти работники могут иметь авторизованный доступ к информации, позволяющий им получать определенные сведения без ограничений. Аутентификация пользователей в данном случае не является эффективной мерой защиты, поскольку она способна отсечь только посторонних.

Еще одна внутренняя угроза – кража носителей с ценными сведениями, например, программным кодом, который является разработкой компании. На это способны только доверенные лица, имеющие доступ к конфиденциальным данным в физическом или электронном виде.

Параллельно с развитием средств защиты информации ведутся разработки новых методов НСД. Необходимо понимать, что изученные методы незаконного получения данных не считаются перспективными. Наибольшую опасность представляют новые и малоизученные способы доступа к ресурсам компании, против которых пока нет эффективных методик борьбы. Поэтому считать средства защиты от несанкционированного доступа излишней мерой не следует. Это не попытка перестраховаться, а следствие правильного понимания размеров угрозы.

Методы защиты компьютеров от несанкционированного доступа делятся на программно-аппаратные и технические. Первые отсекают неавторизованных пользователей, вторые предназначены для исключения физического проникновения посторонних людей в помещения компании.

Создавая систему защиты информации (СЗИ) в организации, следует учитывать, насколько велика ценность внутренних данных в глазах злоумышленников.

Для грамотной защиты от несанкционированного доступа важно сделать следующее:

отсортировать и разбить информацию на классы, определить уровни допуска к данным для пользователей;

оценить возможности передачи информации между пользователями (установить связь сотрудников друг с другом).

В результате этих мероприятий появляется определенная иерархия информации в компании. Это дает возможность разграничения доступа к сведениям для сотрудников в зависимости от рода их деятельности.

Аудит доступа к данным должен входить в функционал средств информационной безопасности. Помимо этого, программы, которые компания решила использовать, должны включать следующие опции:

аутентификация и идентификация при входе в систему;

контроль допуска к информации для пользователей разных уровней;

обнаружение и регистрация попыток НСД;

контроль работоспособности используемых систем защиты информации;

обеспечение безопасности во время профилактических или ремонтных работ.

Идентификация и аутентификация пользователей

Для выполнения этих процедур необходимы технические средства, с помощью которых производится двухступенчатое определение личности и подлинности полномочий пользователя. Необходимо учитывать, что в ходе идентификации необязательно устанавливается личность. Возможно принятие любого другого идентификатора, установленного службой безопасности.

После этого следует аутентификация – пользователь вводит пароль или подтверждает доступ к системе с помощью биометрических показателей (сетчатка глаза, отпечаток пальца, форма кисти и т. п.). Кроме этого, используют аутентификацию с помощью USB-токенов или смарт-карт. Этот вариант слабее, так как нет полной гарантии сохранности или подлинности таких элементов.

Протоколы секретности для бумажной документации

Несмотря на повсеместную цифровизацию, традиционные бумажные документы по-прежнему используются в организациях. Они содержат массу информации – бухгалтерские сведения, маркетинговую информацию, финансовые показатели и прочие критические данные. Заполучив эти документы, злоумышленник может проанализировать масштабы деятельности организации, узнать о направлениях

финансовых потоков.

Для защиты документации, содержащей сведения критической важности, используются специальные протоколы секретности. Хранение, перемещение и копирование таких файлов производится по специальным правилам, исключающим возможность контакта с посторонними лицами.

Защита данных на ПК

Для защиты информации, хранящейся на жестких дисках компьютеров, используются многоступенчатые средства шифрования и авторизации. При загрузке операционной системы используется сложный пароль, который невозможно подобрать обычными методами. Возможность входа в систему пользователя со стороны исключается путем шифрования данных в BIOS и использования паролей для входа в разделы диска.

Для особо важных устройств следует использовать модуль доверенной загрузки. Это аппаратный контроллер, который устанавливается на материнскую плату компьютера. Он работает только с доверенными пользователями и блокирует устройство при попытках включения в отсутствие владельца.

Также применяются криптографические методы шифрования данных, превращающие текст «вне системы» в ничего не значащий набор символов.

Эти мероприятия обеспечивают защиту сведений и позволяют сохранить их в неприкосновенности.

Определение уровней защиты

С методической точки зрения процесс защиты информации можно разделить на четыре этапа:

предотвращение – профилактические меры, ограничение доступа посторонних лиц;

обнаружение – комплекс действий, предпринимаемых для выявления злоупотреблений;

ограничение – механизм снижения потерь, если предыдущие меры злоумышленникам удалось обойти;

восстановление – реконструкция информационных массивов, которая производится по одобренной и проверенной методике.

Каждый этап требует использования собственных средств защиты информации, проведения специальных мероприятий. Необходимо учитывать, что приведенное разделение условно. Одни и те же действия могут быть отнесены к разным уровням.

Глава 5. Правовая защита информации

Информация является объектом, по поводу которой возникают определенные отношения, имеющие социальное значение и нуждающиеся в регулировании со стороны общества и государства. Это послужило основой для формирования самостоятельной отрасли правовых отношений - информационного права. Одной из форм реализации информационного права является защита информации. Правовая защита информации - защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением. Поэтому правовая база должна обеспечивать основные функции:

1. Разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации.
2. Определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране и порядка регулирования деятельности предприятий и организаций в этой области.
3. Создание полного комплекса нормативно-правовых руководящих и методических материалов (документов), регламентирующих вопросы обеспечения информационной безопасности как в стране в целом, так и на конкретном объекте.
4. Определение мер ответственности за нарушение правил защиты.
5. Определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

В настоящее время основополагающее значение в области информационного права имеют следующие законодательные акты:

- Гражданский кодекс Российской Федерации.

- Кодекс Российской Федерации об административных правонарушениях.

- Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.

- Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации»;

- Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»

- Федеральный закон № 17-ФЗ от 3 февраля 1996 г. «О банках и банковской деятельности»;

- Федеральный закон № 63-ФЗ от 6 апреля 2011 г. «Об электронной подписи»;

- Федеральный закон № 152-ФЗ от 27 июля 2006 г. «О персональных данных»;

- Федеральный закон № 98-ФЗ от 29 июля 2004 г. «О коммерческой тайне»;

- Федеральный закон № 126-ФЗ от 7 июля 2003 г. «О связи»;

- Федеральный закон № 77-ФЗ от 29 декабря 1994 г. «Об обязательном экземпляре документов»;

- Федеральный закон № 125-ФЗ от 1 октября 2004 г. «Об архивном деле в Российской Федерации»;

- Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;

- Закон РФ № 2124-1 от 27 декабря 1991 г. «О средствах массовой информации»;

- Закон РФ № 5485-1 от 21 июля 1993 г. «О государственной тайне»;

- Закон РФ № 2124-1 от 27 декабря 1991 г. «О средствах массовой информации»;

- Закон РФ № 5485-1 от 21 июля 1993 г. «О государственной тайне»;

- Закон РФ №176-ФЗ от 24 июня 1999 г. «О почтовой связи»;

- Закон РФ от 11.03.92 г. № 2487-1 «О частной детективной и охранной деятельности».

Заключение

Подводя итоги, следует упомянуть о том, что известно множество случаев, когда фирмы (не только зарубежные) ведут между собой настоящие «шпионские войны», вербуя сотрудников конкурента с целью получения через них доступа к информации, составляющую коммерческую тайну. Регулирование вопросов, связанных с коммерческой тайной, еще не получило в России достаточного развития. Имеющееся законодательство все же не обеспечивает соответствующего современным реалиям регулирования отдельных вопросов, в том числе и о коммерческой тайне. В то же время надо отдавать себе отчет, что ущерб, причиненный разглашением коммерческой тайны, зачастую имеет весьма значительные размеры (если их вообще можно оценить). Наличие норм об ответственности, в том числе уголовной, может послужить работникам предостережением от нарушений в данной области, поэтому целесообразно подробно проинформировать всех сотрудников о последствиях нарушений. Хотелось бы надеяться что создающаяся в стране система защиты информации и формирование комплекса мер по ее реализации не приведет к необратимым последствиям на пути зарождающегося в России информационно - интеллектуального объединения со всем миром.

Список используемой литературы

1. Безруков Н.Н. Компьютерные вирусы. - М.: Наука, 1991
2. Мостовой Д.Ю. Современные технологии борьбы с вирусами // Мир ПК.
3. А.А. Энгельгардт Компьютерная информация как предмет преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации
4. https://ru.wikipedia.org/wiki/Компьютерный_вирус#Распространение
5. https://ru.wikipedia.org/wiki/Компьютерная_безопасность
6. Об информации, информатизации и защите информации: Федеральный Закон // Российская газета. - 1995. - 22 февраля