Информация и закон

Н.Ю. Смелая

Автор: Смелая Н.Ю., учитель информатики средней школы № 6 г. Арсеньева Приморского края.

Предмет: Информатика.

Класс: 9.

Тема: Защита информации. Правовая охрана программ и данных.

Профиль: Общеобразовательный.

Уровень: Общий.

Текст задачи. За время становления повсеместной информатизации общества получило распространение новое для мировой практики преступление. Эти преступления объединены общим признаком: предметом посягательства стала компьютерная информация. Число таких преступлений постоянно растёт. Как называются такие преступления? Какие действия, связанные с информацией, вы считаете наказуемыми? Приведите примеры названных нарушений. Составьте «антирейтинг», присваивая каждому нарушению «баллы вредоносности». Какие из перечисленных нарушений вы считаете наиболее опасными по последствиям? Есть ли эффективные способы защиты информации? Если есть, то какие?

а) Выделите ключевые слова для информационного поиска.

б) Найдите и соберите необходимую информацию.

в) Обсудите и проанализируйте собранную информацию.

г) Сделайте выводы.

д) Сравните ваши выводы с выводами известных людей.

Возможные информационные источники

Web-сайты:

http://www.internet-law.ru/law/inflaw/inf.htm — федеральный закон

http://ru.wikipedia.org/wiki/Information_security — информационная безопасность

http://www.rfbr.ru/default.asp?doc_id=5497 — методы и средства защиты информации

http://www.ci.ru/inform9_97/aiti1.htm — защита информации — проблема № 1

Культурный образец

http://articles.excelion.ru/science/info/21758469.html

Зенковский А.К. Защита информации в компьютерных системах.

Прогресс подарил человечеству великое множество достижений, но тот же прогресс породил и массу проблем. Человеческий разум, разрешая одни проблемы, непременно сталкивается при этом с другими, новыми, и этот процесс обречён на

бесконечность в своей последовательности. Хотя, если уж быть точным, новые проблемы — это всего лишь обновлённая форма старых…

Вечная проблема — защита информации. На различных этапах своего развития человечество решало эту проблему с присущей для данной эпохи характерностью. Изобретение компьютера и дальнейшее бурное развитие информационных технологий во второй половине XX века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества. Главная тенденция, характеризующая развитие современных информационных технологий — рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь…

Причин активизации компьютерных преступлений и связанных с ними финансовых потерь достаточно много, существенные из них:

— переход от традиционной «бумажной» технологии хранения и передачи сведений на электронную и недостаточное при этом развитие технологии защиты информации в таких технологиях;

— объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам;

— увеличение сложности программных средств и связанное с этим уменьшение их надёжности и увеличение числа уязвимостей.

Любое современное предприятие независимо от вида деятельности и формы собственности не в состоянии успешно развиваться и вести хозяйственную деятельность без создания на нём условий для надёжного функционирования системы защиты собственной информации…

Можно с уверенностью утверждать, что создание эффективной системы защиты информации сегодня вполне реально. Надёжность защиты информации, прежде всего, будет определяться полнотой решения целого комплекса задач, речь о которых будет продолжена дальше.

Информация как объект защиты

Построение надёжной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени её конфиденциальности, анализа потенциальных угроз её безопасности и установление необходимого режима её защиты.

Федеральным законом «Об информации, информатизации и защите информации» определено, что информационные ресурсы, т.е. отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектом отношений физических, юридических лиц и государства, подлежат обязательному учёту и защите, как всякое материальное имущество собственника. При этом собственнику предоставляется право самостоятельно в пределах своей компетенции устанавливать режим защиты информационных ресурсов и доступа к ним.

Закон также устанавливает, что «конфиденциальной информацией считается такая документированная информация, доступ к которой огра-

ничивается в соответствии с законодательством Российской Федерации». При этом федеральный закон может содержать прямую норму, согласно которой какие-либо сведения относятся к категории конфиденциальных или доступ к ним ограничивается. Так, Федеральный закон «Об информации, информатизации и защите информации» напрямую относит к категории конфиденциальной информации персональные данные (информацию о гражданах). Закон РСФСР «О банках и банковской деятельности в РСФСР» ограничивает доступ к сведениям по операциям, счетам и вкладам клиентов и корреспондентов банков (статья 25).

Однако не ко всем сведениям, составляющим конфиденциальную информацию, применима прямая норма. Иногда законодательно определяются только признаки, которым должны удовлетворять эти сведения. Это, в частности, относится к служебной и коммерческой тайне, признаки которых определяются Гражданским кодексом РФ (статья 139):

— соответствующая информация неизвестна третьим лицам;

— к ней нет свободного доступа на законном основании;

— меры по обеспечению её конфиденциальности принимает собственник информации.

В настоящее время отсутствует какая-либо универсальная методика, позволяющая чётко относить ту или иную информацию к категории коммерческой тайны. Можно только посоветовать исходить из принципа экономической выгоды и безопасности предприятия — чрезмерная «засекреченность» приводит к необоснованному подорожанию необходимых мер по защите информации и не способствует развитию бизнеса, когда как широкая открытость может привести к большим финансовым потерям или разглашению тайны. Законопроектом «О коммерческой тайне» права по отнесению информации к категории коммерческой тайны предоставлены руководителю юридического лица.

Федеральный закон «Об информации, информатизации и защите информации», определяя нормы, согласно которым сведения относятся к категории конфиденциальных, устанавливает и цели защиты информации:

— предотвращение утечки, хищения, искажения, подделки информации;

— предотвращение несанкционированных действий по уничтожению, искажению, блокированию информации;

— сохранение государственной тайны, конфиденциальности документированной информации.

Определившись в необходимости защиты информации, непосредственно приступают к проектированию системы защиты информации.

Организация защиты информации

Отдельный раздел законопроекта «О коммерческой тайне», посвящённый организации защиты коммерческой информации, определяет необходимый комплекс мероприятий по её защите:

— установление особого режима конфиденциальности;

— ограничение доступа к конфиденциальной информации;

— контроль за соблюдением установленного режима конфиденциальности.

Конкретное содержание указанных мероприятий для каждого отдельно взятого предприятия может быть различным по масштабам и формам. Это зависит в первую очередь от производственных, финансовых и иных возможностей предприятия, от объёмов конфиденциальной информации и степени её значимости. Существенно то, что весь перечень указанных мероприятий обязательно должен планироваться и использоваться с учётом особенностей функционирования информационной системы предприятия.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации. Как правило, особый режим конфиденциальности подразумевает:

— организацию охраны помещений, в которых содержатся носители конфиденциальной информации;

— установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;

— установление пропускного режима в помещения, содержащие носители конфиденциальной информации;

— закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;

— установление порядка пользования носителями конфиденциальной информации (учёт, хранение, передача другим должностным лицам, уничтожение, отчётность);

— организацию ремонта технических средств обработки конфиденциальной информации;

— организацию контроля за установленным порядком.

Требования устанавливаемого на предприятии особого режима конфиденциальности оформляются в виде организационно-распорядительных документов и доводятся для ознакомления до сотрудников предприятия.

Ограничение доступа к конфиденциальной информации способствует созданию наиболее эффективных условий сохранности конфиденциальной информации. Необходимо чётко определять круг сотрудников, допускаемых к конфиденциальной информации, к каким конкретно сведениям им разрешён доступ и полномочия сотрудников по доступу к конфиденциальной информации.

Как показывает практика работы, для разработки необходимого комплекса мероприятий по защите информации желательно привлечение квалифицированных экспертов в области защиты информации.

Традиционно для организации доступа к конфиденциальной информации использовались организационные меры, основанные на строгом соблюдении сотрудниками процедур допуска к информации, определяемых соответствующими инструкциями, приказами и другими нормативными документами. Однако с развитием компьютерных систем эти меры перестали обеспечивать необходимую безопасность информации. Появились и в настоящее время широко применяются специализированные программные и программно-аппаратные средства защиты информации, которые позволяют максимальные

но автоматизировать процедуры доступа к информации и обеспечить при этом требуемую степень её защиты. Подробнее на существующих средствах защиты информации мы остановимся ниже.

Контроль за соблюдением установленного режима конфиденциальности предусматривает проверку соответствия организации защиты информации установленным требованиям, а также оценку эффективности применяемых мер защиты информации. Как правило, контроль осуществляется в виде плановых и внеплановых проверок силами своих сотрудников или с привлечением других организаций, которые специализируются в этой области. По результатам проверок специалисты по защите информации проводят необходимый анализ с составлением отчёта, который включает:

— вывод о соответствии проводимых на предприятии мероприятий установленным требованиям;

— оценка реальной эффективности применяемых на предприятии мер защиты информации и предложения по их совершенствованию.

Обеспечение и реализация перечисленных выше мероприятий потребуют создания на предприятии соответствующих органов защиты информации. Эффективность защиты информации на предприятии во многом будет определяться тем, насколько правильно выбрана структура органа защиты информации и квалифицированны его сотрудники. Как правило, органы защиты информации представляют собой самостоятельные подразделения, однако на практике часто практикуется и назначение одного из штатных специалистов предприятия ответственным за обеспечение защиты информации. Однако такая форма оправдана в тех случаях, когда объём необходимых мероприятий по защите информации небольшой и создание отдельного подразделения экономически не выгодно.

Созданием органов защиты информации на предприятии завершается построение системы защиты информации, под которой понимается совокупность органов защиты информации или отдельных исполнителей, используемые ими средства защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Средства защиты информации

Как уже отмечалось выше, эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

— средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;

— средства, обеспечивающие защиту информации при передаче её по каналам связи;

— средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;

— средства, обеспечивающие защиту от воздействия программ-вирусов;

— материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Основное назначение средств защиты первой группы — разграничение доступа к локальным и сетевым информационным ресурсам автоматизированных систем. СЗИ этой группы обеспечивают:

— идентификацию и аутентификацию пользователей автоматизированных систем;

— разграничение доступа зарегистрированных пользователей к информационным ресурсам;

— регистрацию действий пользователей;

— защиту загрузки операционной системы с гибких магнитных дисков и CD-ROM;

— контроль целостности СЗИ и информационных ресурсов.

В качестве идентификаторов пользователей применяются, как правило, условные обозначения в виде набора символов. Для аутентификации пользователей применяются пароли.

Ввод значений идентификатора пользователя и его пароля осуществляется по запросу СЗИ с клавиатуры. Многие современные СЗИ используют и другие типы идентификаторов — магнитные карточки, радиочастотные бесконтактные карточки, смарт-карточки, электронные таблетки Touch Memory и другие. Отдельно стоит сказать об использовании в качестве идентификатора индивидуальных биологических параметров (отпечаток пальца, радужная оболочка глаза), присущих каждому человеку. Использование в качестве идентификаторов индивидуальных биологических параметров характеризуется, с одной стороны, высшим уровнем конфиденциальности, а с другой — очень высокой стоимостью таких систем.

Разграничение доступа зарегистрированных пользователей к информационным ресурсам осуществляется СЗИ в соответствии с установленными для пользователей полномочиями. Как правило, СЗИ обеспечивают разграничение доступа к гибким и жёстким дискам, логическим дискам, директориям, файлам, портам и устройствам. Полномочия пользователей устанавливаются с помощью специальных настроек СЗИ. По отношению к информационным ресурсам средствами защиты могут устанавливаться такие полномочия, как разрешение чтения, записи, создания, запуска исполняемых файлов и другие.

Системы защиты информации предусматривают ведение специального журнала, в котором регистрируются определённые события, связанные с действиями пользователей, например запись (модификация) файла, запуск программы, вывод на печать и другие, а также попытки несанкционированного доступа к защищаемым ресурсам и их результат.

Особо стоит отметить наличие в СЗИ защиты загрузки операционной системы с гибких магнитных дисков и CD-ROM, которая обеспечивает защиту самих средств защиты от «взлома» с использованием специальных технологий. В различных СЗИ сущес-

твуют программные и аппаратно-программные реализации этой защиты, однако практика показывает, что программная реализация не обеспечивает необходимой стойкости.

Контроль целостности средств защиты и защищаемых файлов заключается в подсчёте и сравнении контрольных сумм файлов. При этом используются различной сложности алгоритмы подсчёта контрольных сумм.

Несмотря на функциональную общность средств защиты информации данной группы, СЗИ различных производителей различаются:

— условиями функционирования (операционная среда, аппаратная платформа, автономные компьютеры и вычислительные сети);

— сложностью настройки и управления параметрами СЗИ;

— используемыми типами идентификаторов;

— перечнем событий, подлежащих регистрации;

— стоимостью средств защиты.

С развитием сетевых технологий появился новый тип СЗИ — межсетевые экраны (firewalls), которые обеспечивают решение таких задач, как защита подключений к внешним сетям, разграничение доступа между сегментами корпоративной сети, защита корпоративных потоков данных, передаваемых по открытым сетям.

Защита информации при передаче её по каналам связи осуществляется средствами криптографической защиты (СКЗИ). Характерной особенностью этих средств является то, что они потенциально обеспечивают наивысшую защиту передаваемой информации от несанкционированного доступа к ней. Помимо этого, СКЗИ обеспечивают защиту информации от модификации (использование цифровой подписи и имитовставки).

Как правило, СКЗИ функционируют в автоматизированных системах как самостоятельное средство, однако в отдельных случаях СКЗИ может функционировать в составе средств разграничения доступа как функциональная подсистема для усиления защитных свойств последних.

Обеспечивая высокую степень защиты информации, в то же время применение СКЗИ влечёт ряд неудобств:

— стойкость СКЗИ является потенциальной, т.е. гарантируется при соблюдении ряда дополнительных требований, реализация которых на практике осуществляется довольно сложно (создание и функционирование ключевой системы, распределение ключей, обеспечение сохранности ключей, необходимость в получении лицензии ФАПСИ на право эксплуатации средств, планирование и организация мероприятий при компрометации ключевой системы);

— относительно высокая стоимость эксплуатации таких средств.

В целом при определении необходимости использовать средства криптографической защиты информации, необходимо учитывать то, что применение СКЗИ оправданно в случаях явного перехвата действительно конфиденциальной информации.

Для защиты информации от утечки по физическим полям используются следующие методы и средства защиты:

— электромагнитное экранирование устройств или помещений, в которых расположена вычислительная техника;

— активная радиотехническая маскировка с использованием широ-

кополосных генераторов шумов, которые широко представлены на нашем рынке.

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако этот способ требует значительных капитальных затрат и практически не применяется.

И несколько слов о материалах, обеспечивающих безопасность хранения, транспортировки носителей информации и защиту их от копирования. В основном это специальные тонкоплёночные материалы с изменяющейся цветовой гаммой или голографические метки, которые наносятся на документы и предметы (в том числе и на элементы компьютерной техники автоматизированных систем). Они позволяют:

— идентифицировать подлинность объекта;

— контролировать несанкционированный доступ к ним.

Средства анализа защищённости компьютерных сетей

Широкое развитие корпоративных сетей, интеграция их с информационными системами общего пользования помимо явных преимуществ порождает новые угрозы безопасности информации. Причины возникновения новых угроз характеризуются:

— сложностью и разнородностью используемого программного и аппаратного обеспечения корпоративных сетей;

— большим числом узлов сети, участвующих в электронном обмене информацией, их территориальной распределённостью и отсутствием возможности контроля всех настроек;

— доступностью информации корпоративных систем внешним пользователям (клиентам, партнёрам и пр.) из-за её расположения на физически соединённых носителях.

Применение описанных выше средств защиты информации, а также встроенных в операционные системы механизмов защиты информации не позволяет в полной мере ликвидировать эти угрозы. Наличие постоянных или временных физических соединений является важнейшим фактором, который влияет на повышение уязвимостей корпоративных систем из-за брешей в используемых защитных и программных средствах и утечки информации вследствие ошибочных или неграмотных действий персонала.

Обеспечение требуемой защиты информационных ресурсов предприятий в этих условиях достигается применением дополнительных инструментальных средств. К их числу относятся:

— средства анализа защищённости операционных систем и сетевых сервисов;

— средства обнаружения опасных информационных воздействий (атак) в сетях.

Средства анализа защищённости операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме того, средствами данного класса проводится контроль

целостности и неизменности программных средств и системных установок и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.

К числу средств анализа данного класса относится программное средство администратора ОС Solaris ASET (Automated Security Tool), которое входит в состав ОС Solaris, пакет программ COPS (Computer Oracle and Password System) для администраторов Unix-систем и система System Scanner (SS) фирмы Internet Security System Inc. для анализа и управления защищённостью операционных систем Unix и Windows NT/ 95/98.

Использование в сетях Internet/ Intranet протоколов TCP/IP, которые характеризуются наличием в них неустранимых уязвимостей, привело к появлению в последнее время новых разновидностей информационных воздействий на сетевые сервисы и представляющих реальную угрозу защищённости информации. Средства анализа защищённости сетевых сервисов применяются для оценки защищённости компьютерных сетей по отношению к внутренним и внешним атакам. По результатам анализа защищённости сетевых сервисов средствами генерируются отчёты, включающие в себя список обнаруженных уязвимостей, описание возможных угроз и рекомендации по их устранению. Поиск уязвимостей основывается на использовании базы данных, которая содержит широко известные уязвимости сетевых сервисных программ и может обновляться путём добавления новых уязвимостей.

К числу средств анализа данного класса относится программа SATAN (автор В. Венема), Netprobe фирмы Qualix Group и Internet Scanner фирмы Internet Security System Inc.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищённости и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети.

Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

Методический комментарий

Данная задача — межпредметная и может быть использована учителями информатики и обществознания.

Информационный поиск девятиклассники проводят по ключевым словам «информация», «защита», «закон» и фразе «защита информации». Поставленные в задаче вопросы позволят значительно расширить и углубить знания учащихся об информации и правовой деятельности человека.