УДК 004

Кыбыраев А.О. *- ОФ РГСУ,* ***Кудуев А.Ж.*** *- ОшМУ*
Сулайманов А. А. *- ОшГУ,* ***Абдыкалык кызы Ж****. - ОГЮИ*

О компьютерных преступлениях и методах защиты информации

Проблема обеспечения информационной безопасности актуальна с тех пор, как люди стали обмениваться информацией, накапливать ее и хранить. Во все времена возникала необходимость надежного сохранения наиболее важных достижений человечества с целью передачи их потомкам. Аналогично возникала необходимость обмена конфиденциальной информацией и надежной ее защиты.

В современном обществе проблема информационной безопасности особенно актуальна, поскольку информация стала частью жизни современного общества. Развитие современного общества во многом определяется теми информационными процессами, которые в нем протекают.

С началом массового применения компьютеров проблема информационной безопасности приобрела особую остроту. С одной стороны, компьютеры стали носителями информации и, как следствие, одним из каналов ее получения как санкционированного, так и несанкционированного. С другой стороны, компьютеры как любое техническое устройство подвержены сбоям и ошибкам, которые могут привести к потере информации. Под *информационной безопасностью* понимается защищенность информации от случайного или преднамеренного вмешательства, наносящего ущерб ее владельцам или пользователям.

С повышением значимости и ценности информации соответственно растет и важность ее защиты. С одной стороны, информация стала товаром, и ее утрата или несвоевременное раскрытие наносит материальный ущерб. С другой стороны, информация - это сигналы управления процессами в обществе, в технике, а несанкционированное вмешательство в процессы управления может привести к катастрофическим последствиям.

Для анализа возможных угроз информационной безопасности, на наш взгляд, можно рассмотреть следующие составные части автоматизированной системы обработки информации:

- аппаратные средства - компьютеры и устройства обмена информацией между ними (внутренние и внешние устройства, устройства связи и линии связи);
- программное обеспечение – системное и прикладное программное обеспечение;
- данные (информация) – хранимые временно и постоянно на внутренних и внешних носителях, печатные копии, системные журналы;
- персонал – обслуживающий персонал и пользователи.

Защита информации – это комплекс мер по ограничению доступа к информации пользователей и программ, по обеспечению ее подлинности, целостности в процессе передачи (обмена) и хранения.[]

Компьютерная преступность (преступление с использованием компьютера) - представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом, компьютерная информация является предметом или средством совершения преступления. Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии, компьютерных преступлений, как преступлений специфических не существует. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная

система или компьютерная сеть. Компьютерные преступления условно можно разделить на две большие категории:

- преступления, связанные с вмешательством в работу компьютеров;
- преступления, использующие компьютеры как необходимые технические средства (орудие преступления).

Хакер («компьютерный пират»), - лицо, совершающее систематические несанкционированные доступы в компьютерные системы и сети с целью развлечения, мошенничества или нанесения ущерба (в том числе и путем распространения компьютерных вирусов). С одной стороны «хакер» - это человек, который прекрасно знает компьютер и пишет хорошие программы, а с другой, - незаконно проникающий в компьютерные системы с целью получения информации.

Английский глагол «to hack» применительно к компьютерам может означать две вещи - взломать систему или починить ее. В основе этих действий лежит нечто общее - понимание того, как устроен компьютер и программы, которые на нем работают.

Таким образом, слово «хакер» совмещает в себе, по крайней мере, два значения: одно - окрашенное негативно («взломщик»), другое - нейтральное или даже хвалебное («ас», «мастер»). Другими словами, хакеров можно разделить на «плохих» и «хороших».

«Хорошие» хакеры двигают технический прогресс и используют свои знания и умения на благо человечества. Ими разработано большое число новых технических и программных систем.

Им, как водится, противостоят «плохие»: они читают чужие письма, воруют чужие программы и всеми доступными способами вредят прогрессивному человечеству.

«Плохих» хакеров можно условно разделить на четыре группы. Первая, состоящая в основном из молодежи, - люди, взламывающие компьютерные системы просто ради собственного удовольствия. Они не наносят вреда, а такое занятие весьма полезно для них самих - со временем из них получаются превосходные компьютерные специалисты.

Во время экономических потрясений, которые пережили Россия и Кыргызстан в последние годы, огромное количество действительно высококлассных специалистов осталось не у дел. В этот период и было написано то великое множество вирусов, которыми прославилась Россия. В большинстве своем отечественные хакеры не получают выгоды от взломов, хотя есть и исключения. Так например, только в Москве выявлено более 360 человек, незаконно оплачивающих коммуникационные услуги. Юридическая тонкость момента, сидя дома, человек совершает преступление на территории США. Привлечь их к ответственности в соответствии с законодательством США очень сложно: тут можно годами разбираться.

Способ «троянский конь» состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять прежнюю работоспособность. С помощью «троянского коня» преступники, например, отчисляют на свой счет определенную сумму с каждой операции.

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима.

Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку

хищение сопряжено с изъятием ценностей из фондов организации. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путем краж и обмена краденым. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться.

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Ниже приведены названия способов совершения подобных преступлений, соответствующие кодификатору Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен НЦБ более чем 100 стран.

Для решения проблем защиты информации в сетях прежде всего нужно уточнить возможные причины сбоев и нарушений, способные привести к уничтожению или нежелательной модификации данных. К ним, в частности, относятся:

- сбои оборудования (кабельной системы, электропитания, дисковых систем, систем архивации данных, работы серверов, рабочих станций, сетевых карт и т.д.);
- потери информации из-за некорректной работы ПО;
- заражение системы компьютерными вирусами;
- ущерб, наносимый организации несанкционированным копированием, уничтожением или подделкой информации, доступом посторонних лиц к конфиденциальным данным;
- потери информации, связанные с неправильным хранением архивных данных;
- ошибки обслуживающего персонала и пользователей (случайное уничтожение или изменение данных, некорректное использование программного и аппаратного обеспечения).

Защита информации является ключевой задачей в современных условиях взаимодействия глобальных и корпоративных компьютерных сетей. В реальном мире много внимания уделяется физической безопасности, а в мире электронного обмена информацией необходимо заботиться также о средствах защиты данных.

Усложнение методов и средств организации машинной обработки, повсеместное использование глобальной сети Интернет приводит к тому, что информация становится все оболе уязвимой. Этому способствуют такие факторы, как постоянно возрастающие объемы обрабатываемых данных, накопление и хранение данных в ограниченных местах, постоянное расширение круга пользователей, имеющих доступ к ресурсам, программам и данным, недостаточный уровень защиты аппаратных и программных средств компьютеров и коммуникационных систем и т.п.

Учитывая эти факты, защита информации в процессе ее сбора, хранения, обработки и передачи приобретает исключительно важное значение. Ошибки в работе и выход из строя компьютерных систем могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся наиболее актуальными на сегодняшний день. Известно много мер, направленных на предупреждение преступления. Необходимо наиболее эффективно использовать всевозможные подходы к сохранению конфиденциальной информации с целью сохранения информационной целостности организации.

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку сигнализации и многое другое.

К организационным мерам отнесем охрану вычислительного центра, тщательный подбор персонала, наличие плана восстановления работоспособности центра после выхода его из строя, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра и т.д.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение.

Залог успеха предотвращения компьютерной преступности заключается в реализация всех перечисленных выше мер и методов защиты информации и программных средств. Все данные меры позволят решить проблему незаконного доступа и помешают злоумышленнику завладеть чужими конфиденциальными реквизитами.

Литература

1. *Информатика / Курносов А.П., Кулев С.А., Улезько А.В. и др*.; под ред. А.П. Курносова. – М.: КолосС, 2005.
2. Компьютерные сети и средства защиты информации: Учебное пособие/ Камалян А.К., Кулев С.А., Назаренко К.Н., Ломакин С.В., Кусмагамбетов С.М.; Под ред. д.э.н., профессора А.К. Камаляна. – Воронеж: ВГАУ, 2003.
3. *Леонтьев В. П.* Новейшая энциклопедия персонального компьютера 2005. – М.: ОЛМА-ПРЕСС Образование, 2005.
4. *Черняков М.В., Петрушин А.С.* Основы информационных технологий. Учебник для вузов: - М.: ИКЦ «Академкнига», 2007.
5. http://soft/compulenta/ru
6. http://litek.ru/catalog/acronis/homeRe.html