$$P_n(t) = \frac{(l\,t)^n}{n!} e^{-l\,t}\ ,\ (n = 0, 1, 2, 3, \ldots),$$

где λ – среднее число отказов в единицу времени, или интенсивность отказов, λ = const; $\lambda = \overline{\Lambda}$, где $\overline{\Lambda}$ – параметр потока отказов, который определяется по статистической формуле:

$$\overline{\Lambda} = \frac{n}{N\Delta t},$$

где N – общее число отказавших элементов, или число восстановлений, остается неизменным. Отказавшие элементы заменяются новыми.

Поток отказов восстанавливаемой системы является простейшим.

Для ремонтируемых объектов удобный для практики критерий надежности – наработка на отказ T_0. Значения этого параметра определяются по результатам обработки статистических данных, полученных в ходе эксплуатации системы.

Если устройство проработало суммарное время t_Σ и имело при этом n отказов в работе, то наработка на отказ вычисляется следующим образом:

$$\overline{T}_0 = \frac{t_\Sigma}{n}.$$

Если испытывались N однотипных объектов, то суммируется время исправной работы по всем объектам и делится на общее число отказов:

$$\overline{T}_0 = \frac{\sum_{i=1}^{N} t_i}{\sum_{i=1}^{N} n_i}.$$

Для простейшего потока параметр потока отказов имеет вид

$$\overline{\Lambda} = \frac{1}{\overline{T}_0}.$$

Восстановление отказавшего элемента требует времени, которым нельзя пренебречь. Среднее время восстановления системы T_B – это математическое ожидание продолжительности восстановления системы после отказа, т. е. среднее время вынужденного простоя, вызванного устранением отказа.

$$T_B = \int_0^\infty t \cdot P_B dt = \int_0^\infty (1 - F_B)\, dt,$$

где P_B – плотность вероятности времени восстановления; F_B – функция распределения времени восстановления.

Основной характеристикой системы является коэффициент готовности $K_Г$, который для установившегося режима эксплуатации определяется как вероятность того, что система будет исправна в произвольный момент в промежутках между плановыми техническими обслуживаниями

$$K_Г = \frac{T_0}{T_0 + T_B}.$$

Формулы для статистических оценок времени восстановления $\overline{T}_B$ и коэффициента готовности $\overline{K}_Г$ имеют следующий вид:

$$\overline{T}_B = \frac{1}{N}\sum_{i=1}^{N} t_{B_i},\ \overline{K}_Г = \frac{\overline{T_0}}{\overline{T_0} + \overline{T_B}},$$

где N – число восстановлений системы; t_{B_i} – время восстановления (ремонта) системы после i-го отказа.

Вероятностные методы оценки различных характеристик информационных систем целесообразно использовать на всех стадиях их жизненного цикла, так как это представляет большой практический интерес и является важной составляющей при подготовке специалистов, использующих современные информационные технологии.

1. Герасименко В.А., Малюк А.А. Основы защиты информации. М., 1997.
2. Шиверский А.А. Защита информации: проблемы теории и практики. М., 1996.
3. Ярочкин В.И. Информационная безопасность. М., 2000.
4. Вентцель Е.С. Теория вероятностей. М., 2006.
5. Когельман Л.Г., Михеев М.Ю., Трубицков С.В. Защита информации : учеб. пособие. Пенза, 2004.
6. ГОСТ 27.002–89. Надежность в технике. Основные понятия. Термины и определения. Введ. 1990.07.01. М., 1989.

А.А. Юхник, П.Л. Боровик

О НЕКОТОРЫХ ПОДХОДАХ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Проблема информационной безопасности в деятельности органов внутренних дел не является новой, поскольку обеспечение собственной безопасности – задача первостепенной важности для любой системы независимо от ее сложности и назначения. Однако в условиях, когда

защищаемый объект представляет собой информационную систему или когда средства нападения имеют форму информационных воздействий, необходимо разрабатывать и применять совершенно новые технологии и методы защиты.

Не останавливаясь на социальных, правовых и экономических аспектах данной проблемы, рассмотрим актуальные вопросы обеспечения информационной безопасности в деятельности органов внутренних дел.

Во-первых, современные средства компьютерной техники (СКТ) за последние годы приобрели значительную вычислительную мощь, но одновременно с этим стали гораздо проще в эксплуатации. Это означает, что пользоваться ими стало намного легче, поэтому все большее количество новых, как правило неквалифицированных, людей получает доступ к СКТ, что приводит к снижению средней квалификации пользователей. Эта тенденция существенно облегчает задачу нарушителям, так как в результате «персонализации» СКТ большинство пользователей имеют личные компьютеры и осуществляют их администрирование самостоятельно. Большинство из них не в состоянии постоянно поддерживать безопасность своих систем на должном уровне, так как это требует соответствующих знаний, навыков, а также времени и средств. Повсеместное распространение сетевых технологий объединило отдельные машины в локальные сети, совместно использующие общие ресурсы, а применение технологии «клиент – сервер» и кластеризации преобразовало такие сети в распределенные вычислительные среды. Поскольку безопасность сети определяется защищенностью всех входящих в нее компьютеров и сетевого оборудования, то правонарушителю достаточно расстроить работу только одного компонента, чтобы скомпрометировать всю сеть.

Одним из новых направлений для преступной деятельности в информационной сфере является использование глобальных коммуникационных информационных систем с удаленным доступом к совместно используемым ресурсам сетей. Вполне закономерно, что подобная информационная сеть, объединившая огромное число людей, с возможностью подключения к ней любого человека, становится не только предметом преступного посягательства, но и очень эффективным средством совершения преступлений.

Используя интернет в качестве среды для противоправной деятельности, преступники очень часто делают акцент на возможностях, которые им дает компьютерная сеть для обмена информацией, в том числе криминального характера. Аналогичная ситуация складывается и при использовании компьютерных минипроцессоров, составляющих основу современной мобильной или так называемой сотовой телефонной

связи. Однако следует отметить, что большинство ее видов при эксплуатации позволяют оперировать лишь аудио- и небольшими по объему частями текстовой информации, в то время как подключение этих устройств к цифровым каналам интернета позволяет передавать не только аудио-, но и видео-, а также практически неограниченные объемы текстовой и графической информации.

Интернет привлекает преступников и возможностью осуществлять в глобальных масштабах информационно-психологическое воздействие на людей. Преступное сообщество весьма заинтересовано в распространении своих доктрин и учений, в формировании общественного мнения, благоприятного для укрепления позиций представителей преступного мира, и в дискредитации правоохранительных органов.

Во-вторых, прогресс в области аппаратных СКТ сочетается с еще более бурным развитием программного обеспечения. Проблема информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности правоохранительных органов технических средств обработки и передачи данных, прежде всего вычислительных систем. Как показывает практика, большинство распространенных современных программных СКТ, используемых в органах внутренних дел, не отвечает даже минимальным требованиям безопасности. В первую очередь это выражается в наличии изъянов в работе средств защиты и наличии огромного числа различных «недокументированных» возможностей. После их выявления многие изъяны устраняются с помощью обновления версий или дополнительных средств, однако то постоянство, с которым выявляются все новые и новые изъяны, не может не вызывать опасений. В настоящий момент можно утверждать, что большинство систем предоставляют злоумышленникам широкие возможности для осуществления нарушений.

В-третьих, развитие гибких и мобильных технологий обработки информации привело к тому, что практически исчезает грань между обрабатываемыми данными и исполняемыми программами за счет появления и широкого распространения виртуальных машин и интерпретаторов. Так, например, практически любое программное приложение от текстового процессора (MS Word) до обозревателя Internet Explorer не просто обрабатывает данные, а интерпретирует интегрированные в них инструкции специальных языков программирования, т. е., по сути дела, является отдельной виртуальной машиной с привычной архитектурой, для которой можно создавать средства нападения, вирусы и т. д. Это повышает возможности злоумышленников по созданию средств внедрения в чужие системы и затрудняет задачу защиты подобных систем, так как наличие таких «вложенных» систем требует и реализации защиты для каждого уровня.

Кроме того, практически все системы защиты основаны на «латании дыр», обнаруженных в процессе эксплуатации, что предопределяет их отставание от динамично развивающихся угроз. Так, например, для большинства коммерческих продуктов (в первую очередь это касается операционных систем) характерна практика закрытия «внезапно» обнаружившихся пробелов в системах защиты с помощью различных программных «заплаток». По мнению отдельных исследователей данной проблемы, отсутствие системной и научной базы информационной безопасности проявляется уже в том, что не существует даже единой общепринятой терминологии, которая бы адекватно воспринималась всеми специалистами в области безопасности. Поэтому часто теория и практика функционируют в разных плоскостях.

Особую роль и место в деятельности по защите компьютерной информации занимают мероприятия по созданию комплексной защиты, учитывающей естественные каналы утечки информации (КУИ) из средств электронно-вычислительной техники, образующиеся спонтанно или в силу специфических обстоятельств. В современных условиях насыщенности деятельности сотрудников правоохранительных органов самыми разнообразными СКТ крайне необходимо понимать опасность возникновения КУИ с ограниченным доступом именно через технические средства ее обработки. Более того, СКТ относятся едва ли не к наиболее уязвимым и незащищенным от несанкционированного доступа техническим устройствам.

Действительно, с точки зрения защиты информации СКТ являются прекрасным примером для изучения естественных КУИ, обусловленных природой процессов, протекающих в самих СКТ, и их техническими особенностями.

Учитывая роль, которую играют СКТ в современном обществе вообще, а также тенденцию к их использованию правоохранительными органами для обработки информации с ограниченным доступом в частности, необходимо детально рассмотреть принципы образования естественных КУИ при эксплуатации СКТ.

Известно, что современные СКТ могут работать как независимо друг от друга, так и взаимодействуя с другими по компьютерным сетям, причем последние могут быть не только локальными, но и глобальными. С учетом этого полный перечень тех участков, в которых могут находиться подлежащие защите данные, может иметь следующий вид:

непосредственно в оперативной или постоянной памяти СКТ;

на съемных магнитных, магнитооптических, лазерных и других носителях;

на внешних устройствах хранения информации коллективного доступа (RAID-массивы, файловые серверы и т. п.);

на экранах устройств отображения (дисплеи, мониторы, консоли);

в памяти устройств ввода/вывода (принтеры, графопостроители, сканеры);

в памяти управляющих устройств и линиях связи, образующих каналы сопряжения компьютерных систем и сетей.

Естественные КУИ образуются как при работе СКТ, так и в режиме ожидания. Анализ физической природы многочисленных преобразователей и излучателей показывает, что источниками таких каналов являются электромагнитные поля, наводимые токи и напряжения в проводных системах (питания, заземления и соединительных), переизлучение обрабатываемой информации на частотах паразитной генерации элементов и устройств технических СКТ, переизлучение обрабатываемой информации на частотах контрольно-измерительной аппаратуры, несовершенство программного либо аппаратного обеспечения.

Что касается искусственных КУИ, то они создаются преднамеренно с применением активных методов и способов получения информации. Активные способы предполагают намеренное создание технического КУИ с использованием специальных технических средств, к которым можно отнести: незаконное подключение к каналам, проводам и линиям связи; умышленное применение таких конструктивно-схемных решений, которые приводят к увеличению электромагнитных излучений в определенной части спектра; установка аппаратных, программных либо аппаратно-программных закладок; использование компьютерных вирусов и иных вредоносных программ для модификации, уничтожения или блокирования информации; установка элементной базы, выходящей из строя; высокочастотное навязывание и облучение, размещение в СКТ закладок на речь или обрабатываемую информацию (замаскированные под какие-либо электронные блоки).

Анализируя различные подходы к обеспечению информационной безопасности при использования СКТ в деятельности органов внутренних дел, следует обратить внимание на следующие возможные способы ее обеспечения:

электромагнитное экранирование помещений в широком диапазоне частот;

доработка СКТ с целью уменьшения уровня побочных электромагнитных излучений;

криптографическое закрытие (шифрование), а также стеганографические методы;

активная радиотехническая маскировка, предполагающая формирование и излучение маскирующего сигнала в непосредственной близости от защищаемого СКТ.

Одним из радикальных способов защиты информации, особенно при передаче ее на большие расстояния по линиям связи, является криптографическое закрытие, т. е. шифрование, осуществляемое либо программно, либо аппаратно с помощью встраиваемых средств.

Кроме того, современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке методов стеганографии, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций и использования их в необъявленных целях. Эти методы, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео- или аудиосигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах), причем в отличие от криптографии данные методы скрывают сам факт передачи информации.

Таким образом, для поддержания режима информационной безопасности наиболее важны программно-технические и организационные меры, так как известно, что основная угроза компьютерным системам исходит от них самих: ошибки программного обеспечения, сбои оборудования, неудовлетворительная работа сотрудников, а также руководителей организаций и учреждений, относящихся к системе органов внутренних дел.

Особый интерес, на наш взгляд, с точки зрения соблюдения информационной безопасности вызывает статус пользователей СКТ. Дело в том, что значительная часть информационных потерь приходится на случайные и преднамеренные ошибки сотрудников, использующих СКТ. В силу своей возможной халатности и небрежности они могут ввести заведомо неверные данные, пропустить ошибки в программном обеспечении, создав тем самым брешь в системе защиты. Все это заставляет задуматься о том, что внутренняя угроза, исходящая непосредственно от пользователей СКТ, значительнее и опаснее внешних воздействий. Кроме того, информационная безопасность не сможет обеспечиваться без строгого распределения функций пользователей СКТ, администраторов локальных сетей и серверов, а также руководителей учреждений правоохранительных органов.

Раздел III

ТЕОРЕТИЧЕСКИЕ, ПРАВОВЫЕ И ПРИКЛАДНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

А.А. Бабкин, Д.Ю. Крюкова

ГЛОНАСС НА СЛУЖБЕ В УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЕ РОССИИ

Уголовно-исполнительная система (УИС) Российской Федерации является элементом правоохранительной системы страны и представляет собой целостную совокупность учреждений и органов, выполняющих функции по исполнению назначенных судами уголовных наказаний и иных мер уголовно-правового характера, а также судебных решений о применении меры уголовно-процессуального пресечения в виде содержания под стражей, охране и конвоированию осужденных и лиц, подозреваемых и обвиняемых в совершении преступлений.

За последние годы система подверглась значительным изменениям, направленным в первую очередь на реформирование принципов, методов, нормативно-правовой базы, концепции осуществления исполнения наказаний, в том числе и со стороны внедрения средств и методов слежения и контроля за осужденными на основе новейших технологий. На сегодняшний день имеется необходимость в анализе современных информационных технологий, применяемых в пенитенциарной практике. Не все информационные технологии могут быть использованы в условиях российских исправительных учреждений. Это связано как с субъективными, так и объективными причинами. Из субъективных можно выделить следующие причины: недостаточная техническая оснащенность, несовершенство нормативно-правовой базы, особенности исполнения наказания, связанного с лишением свободы, и др. К объективным относятся особенности работы с отдельными категориями осужденных, часто не позволяющими применять технические средства для их дальнейшей реабилитации и ресоциализации.

На изменение ситуации направлен проект концепции развития УИС России до 2020 г., предусматривающий совершенствование инфраструктуры информационно-телекоммуникационного и других видов обеспечения функционирования и развития системы передачи и обработки данных, систем информационной безопасности и защиты ин-