но уязвимы с точки зрения безопасности, информационные системы органов внутренних дел не исключение.

При рассмотрении безопасности информационных систем обычно выделяют две группы проблем: сетевая безопасность и безопасность компьютера. Под сетевой безопасностью понимают все вопросы, связанные с взаимодействием устройств в сети, это, прежде всего, защита данных в момент их передачи по линиям связи и защита от несанкционированного удаленного доступа в сеть. К безопасности компьютера относят все проблемы защиты данных, хранящихся и обрабатывающихся компьютером, которая рассматривается как автономная система. Эти проблемы решаются средствами операционных систем и приложений таких, как базы данных, а также встроенными аппаратными средствами компьютера.

На практике сегодня существует два подхода к обеспечению безопасности компьютера:

1) использование только встроенных в операционную систему (ОС) и приложения средств защиты;

2) применение, наряду со встроенными, дополнительных механизмов защиты. Этот подход заключается в использовании так называемых технических средств добавочной защиты – программных, либо программно-аппаратных комплексов, устанавливаемых на защищаемые объекты.

С учетом существующей статистики угроз можно утверждать, что встроенных в ОС и приложения механизмов защиты недостаточно. По оценкам специалистов в современных универсальных ОС не выполняются в полном объеме требования к защите информации в автоматизированных системах. Это значит, что они не могут без использования технических средств добавочной защиты применяться для защиты информации. При этом следует отметить, что основные проблемы защиты здесь вызваны не невыполнимостью ОС требований к отдельным механизмам защиты, а принципиальными причинами, обусловленными реализуемой в ОС концепцией защиты. Концепция эта основана на реализации распределенной схемы администрирования механизмов защиты, что само по себе является невыполнением формализованных требований к основным механизмам защиты.

Таким образом, наиболее эффективным способом безопасности компьютера является подход применения дополнительных механизмов защиты.

К этим механизмам можно отнести программы управления доступом (рассматривая весь класс таких программ). Механизмы управления доступом являются основой защиты ресурсов, обеспечивая решение задачи разграничения доступа субъектов к защищаемым информационным и техническим ресурсам. Однако при применении только программных механизмов защиты в общем случае невозможно осуществлять контроль активности одной программы над другой, запущенной на том же компьютере, что может привести к несанкционированному доступу к информации. Поэтому данная функция должна возлагаться на аппаратную компоненту системы защиты – плату, устанавливаемую в свободный слот защищаемого компьютера.

С учетом сказанного можем сделать вывод, что преимуществом реализации технологии защиты информации является программно-аппаратный подход. Этот подход оказывает противодействие всей совокупности угроз информационной безопасности, причем противодействие осуществляется вне зависимости от того, какой способ доступа использован злоумышленником, т. е. задача защиты решается в общем виде.

Отдельно следует отметить необходимость повышения квалификации сотрудников, эксплуатирующих средства защиты. При этом необходимо понимать, что процесс защиты информации непрерывен, равно как непрерывен процесс изменения угроз информационной безопасности.

Таким образом, одним из важнейших условием защищенности компьютерной информации является квалификация администраторов безопасности и сотрудников эксплуатирующих служб, которая, по крайней мере, не должна уступать квалификации злоумышленников. В противном случае не помогут никакие средства защиты.

УДК 343.985

А.Н. Лепёхин

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ В БОРЬБЕ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

Проблемы борьбы с современной преступностью, и в том числе компьютерной, являются достаточно актуальными и предполагают решения ряда первостепенных задач и в первую очередь информационного обеспечения управленческой деятельности посредством использования компьютерных технологий обработки и анализа различных данных. Одним из эффективных средств решения подобной научно-практической задачи является использование программно-технических средств информационно-аналитической работы. Объективно, что задачами любой современной информационно-аналитической системы являются эффективное хранение, обработка и анализ данных.

Следует отметить, что в настоящее время накоплен определенный опыт в этой области.

Эффективное хранение информации достигается наличием в составе информационно-аналитической системы целого ряда источников данных. Обработка и объединение информации достигается применением инструментов извлечения, преобразования и загрузки данных. Анализ данных осуществляется при помощи современных инструментов анализа данных.

Проблема анализа исходной информации для принятия управленческих решений оказалась настолько серьезной, что появилось отдельное направление или вид информационных систем – информационно-аналитические системы (ИАС), под которыми понимают комплекс аппаратных, программных средств, информационных ресурсов, методик, которые используются для обеспечения автоматизации аналитических работ в целях обоснования принятия управленческих решений и других возможных применений [1, с. 38].

Разнообразие источников данных и необходимость их использования в каждом конкретном случае объясняется потребностью поразному хранить информацию в зависимости от стоящих перед правоохранительными органами задач. Классифицируя источники данных по типам и назначению, каждый из них можно условно отнести к одной из трех групп: транзакционные источники данных, хранилища данных, витрины данных.

Данные в ИАС могут заноситься как вручную, так и автоматически. На этапе первоначальной фиксации данные поступают через системы сбора и обработки информации в так называемые транзакционные базы данных или операционные базы данных (БД).

Поскольку транзакционные источники данных, как правило, не согласованы друг с другом, то для анализа таких данных требуется их объединение и преобразование. Поэтому на следующем этапе решается задача консолидации данных, их преобразования и очистки, в результате чего данные поступают в аналитические базы данных. Аналитические базы данных, например хранилища данных или витрины данных, и есть те основные источники, из которых аналитик получает информацию, используя соответствующие инструменты информационного анализа.

Наряду с общими функциональными требованиями информационно-аналитическая система структурного подразделения правоохранительных органов должна обеспечивать пользователям доступ к аналитической информации, защищенной от несанкционированного использования. Таким образом, классическая архитектура информационно-аналитической системы насчитывает следующие уровни: сбор и первичная обработка данных; извлечение, преобразование и загрузка данных;

хранение данных; представление данных в витринах данных; анализ данных; Web-портал (для правоохранительных органов – защищенный).

Следует отметить, что в настоящее время на рынке информационных технологий представлен широкий спектр инструментальных средств, предназначенных для быстрой реализации компонентов архитектуры ИАС. Использование таких инструментов позволяет не разрабатывать аналитические приложения заново, а воспользоваться готовыми современными технологиями и, следовательно, сократить время и затраты на их создание [2, с. 12–17].

Таким образом, решение задачи информационно-аналитического обеспечения борьбы с преступностью определяется правильным подбором инструментов информационного анализа, а также средств поддержки процессов извлечения, преобразования, загрузки и хранения данных. При этом в ходе реализации ИАС правоохранительных органов могут быть использованы программные решения как разных производителей (смешанные), так и одного производителя (платформенно-базированные) для разрешения практических задач информационного обеспечения принятия управленческих решений.

1. Белов В.С. Информационно-аналитические системы. Основы проектирования и применения : учеб. пособие / Моск. гос. ун-т экономики, статистики и информатики. М., 2005.

2. Волков И.В., Галахов И.Ю. Архитектура современной информационно-аналитической системы // Директор информ. службы. М., 2002. № 3.

УДК 681.3

А.Л. Осипенко

НАУЧНОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ СЕТЕВОЙ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

Среди приоритетных направлений деятельности полиции в последние годы руководством МВД России особо выделяется противодействие преступности в сфере информационных технологий, что вполне оправдано с учетом очевидных тенденций повышения ее социальной опасности. Число преступлений, связанных с использованием сети Интернет, неуклонно растет, все чаще они приобретают «резонансный» характер. Преступность активно осваивает преимущества, предлагаемые сетью Интернет. Выступая в прошлом году на 22-й сессии Комиссии ООН по предупреждению преступности и уголовному правосудию в Вене, представитель России А. Змеевский отметил, что за год жерт-