ба будет причиняться с использованием глобальных компьютерных систем. Вместе с тем наши возможности в выявлении и раскрытии данного вида преступлений не в полной мере соответствуют требованиям времени. С внедрением международных компьютерных систем преступность становится интернациональной, не признающей границ. В связи с этим необходимо инициировать проведение совместных международных встреч правоохранительных органов по подготовке специалистов в области раскрытия и расследования компьютерных преступлений, обмену имеющимся опытом в этой области для получения научных разработок и методических рекомендаций.

С учетом возникающих проблем выявления и расследования преступлений с использованием компьютерной техники в целях повышения эффективности получения и использования информации правоохранительными органами при расследовании преступлений против информационной безопасности необходимо:

1) внести предложение по разработке нормативных правовых актов, регламентирующих международное сотрудничество правоохранительных органов стран СНГ при расследовании преступлений против информационной безопасности и иных преступлений с целью увеличения эффективности такого взаимодействия;

2) включать в состав следственно-оперативных групп по расследованию конкретных резонансных преступлений сотрудника, отвечающего за анализ информации и осуществить подготовку квалифицированных сотрудников по техническим вопросам, производить обмен полученными данными специалистов по проведению компьютерно-технических экспертиз в области криминалистического исследования высокотехнологического оборудования, программного обеспечения;

3) использовать лицензионное профильное техническое обеспечение, позволяющее проводить процессуальные действия в минимальные сроки, исключающие уничтожение и модификацию информации;

4) разработать методические рекомендации по своевременной профилактике преступлений, в которых фигурирует компьютерная техника, телекоммуникационные сети и программное обеспечение.

Использование нового технического потенциала, лицензионного технического обеспечения, методических рекомендаций, применение значимой информации, качественных компьютерно-технических экспертиз в установленные сроки, предоставят дополнительные возможности по улучшению доказательственной базы расследуемых уголовных дел, усовершенствуют возможности профилактических мероприятий по пресечению хищений путем использования компьютерной техники и выявлению преступлений против информационной безопасности.

УДК 004.9

В.В. Лавренов

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Успешное выполнение правоохранительных задач в условиях формирования новой социально-экономической и политической ситуации в стране неразрывно связано с обеспечением эффективности управления органами внутренних дел, способствует созданию нормальных условий для функционирования всей инфраструктуры общества. Стабильный правопорядок в стране образует соответствующие общественные предпосылки для социально-экономического и научно-технического прогресса, духовного и нравственного развития.

Эффективность функционирования системы напрямую зависит от информационных процессов, составляющих основу управления, так как любой управленческий цикл осуществляется на основе поступающей в систему информации. Совершенствование системы управления в современных условиях невозможно без использования современных информационных технологий, поскольку именно вопросы обработки информации являются критическими.

Повышение роли информационного обеспечения управленческой деятельности органов внутренних дел обусловлено сложностью выполняемых задач, резкими изменениями оперативной обстановки. Все это вызывает необходимость обработки большого объема информации в короткие сроки.

От полноты и объективности информации, получаемой органами внутренних дел, зависит правильность принимаемых управленческих решений, что, в свою очередь, непосредственно связано с вопросами усиления борьбы с преступностью. Результативность работы органов внутренних дел по предупреждению, раскрытию, расследованию преступлений невозможна без своевременного, достаточного и качественного обеспечения информацией.

Масштабы применения и приложения информационных технологий в органах внутренних дел таковы, что наряду с проблемами производительности, надежности и устойчивости функционирования информационных систем остро встает вопрос о защите циркулирующей в системах информации от несанкционированного доступа. Мировая статистика фактов несанкционированного доступа к информации показывает, что большинство современных информационных систем достаточ-

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.