склонны к риску; есть большая вероятность того, что они воспользуются выпавшей возможностью, – объяснил он. – Поэтому крайне важно понимать поведение своих детей».

Проведение профилактической работы среди несовершеннолетних сотрудниками образовательных учреждений весьма эффективно в отношении детей старшего школьного возраста, но несовершеннолетние, которые только знакомятся с глобальным информационным пространством, нуждаются в непрерывной индивидуальной работе со стороны своих родителей. Представляется, что для достижения успеха в вопросе недопущения совершения преступлений в информационной сфере несовершеннолетними особое значение имеет осведомленность родителей в данной области, установка доверительных отношений между родителями и детьми, а также использование специального программного обеспечения, позволяющего не только контролировать, но и ограничивать деятельность ребенка в сети Интернет и др. Очевидно, что контроль и подробное разъяснение ответственности за совершение противоправных деяний в информационной сфере, а также приведение действительных примеров, будет способствовать уменьшению количества совершения преступлений несовершеннолетними в данной области.

Таким образом, непрерывная и целенаправленная работа с несовершеннолетними является залогом успеха в профилактике совершения компьютерных преступлений подрастающим поколением. С целью объективного ведения статистического учета компьютерных преступлений, совершенных лицами моложе указанного возраста, правильнее было бы предусматривать уголовную ответственность за некоторые компьютерные преступления с наступлением частичной (неполной) дееспособности (лицо в возрасте 14 лет).

УДК 343.97

В.В. Лавренов, старший преподаватель
кафедры правовой информатики Академии
МВД Республики Беларусь
VicLavrenov@mail.ru

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ ФАКТОРНОГО И КОРРЕЛЯЦИОННОГО АНАЛИЗА ПРИ ПОСТРОЕНИИ ЭФФЕКТИВНОЙ СИСТЕМЫ ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

Согласно Концепции информационной безопасности Республики Беларусь трансформация социума в информационное общество порождает новые риски, вызовы и угрозы, которые напрямую затрагивают

вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов. Реагирование на риски и вызовы в информационной сфере осуществляется всеми без исключения государственными органами и организациями в соответствии с областью их деятельности согласно непосредственному предназначению максимально полно и оперативно. Государственное реагирование на риски, вызовы и угрозы в информационной сфере предполагает сбор информации об используемых технологиях, способах деструктивных информационных воздействий и совершения киберпреступлений, анализ, оценку и прогнозирование состояния безопасности данной сферы, выявление реализующихся вызовов и угроз, локализацию негативных последствий и восстановление нанесенного вреда (ущерба), при этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством.

Математика, будучи абстрактной наукой, обладает универсальным характером, и потому ее достижения применимы ко многим отраслям знаний, в том числе и к общественным наукам, и к юриспруденции, особенно в тех областях, где возможен процесс формализации знаний, при этом следует отметить, что основным полем совершения преступлений в сфере высоких технологий является киберпространство, которое организовано и функционирует по строгим «законам математики». В этой связи для повышения эффективности борьбы с компьютерной преступностью, наряду с традиционными методами борьбы особую значимость приобретает познание закономерностей развития криминологических и социально-правовых явлений, основанных на применении научных методов исследования.

Все явления и процессы, связанные с компьютерной преступностью, находятся во взаимосвязи и взаимообусловленности. Одни из них непосредственно связаны между собой, другие косвенно. Важный методологический вопрос в современном мире – выявление, изучение и измерение факторов, влияющих на компьютерную преступность. При этом представляется, что наибольшим потенциалом в исследовании компьютерной преступности обладает факторный анализ, осуществляемый посредством эконометрической методики исследования, что позволяет научно обосновать стратегию и методику противодействия компьютерной преступности, а также прогнозировать ее уровень и те явления, которые ее порождают и обусловливают.

Указанная нами позиция основывается на том, что факторный анализ является апробированной наукой совокупностью методов и моделей, изучающих и объясняющих связи между наблюдаемыми количественными и качественными признаками, измеряющих степень влияния факторов на изменение результативного показателя. Говоря по другому, факторный анализ – это изучение взаимосвязи результата и факторов (причин).

Вместе с тем, как показывает практика применения теоретических конструкций, для достижения результата, позволяющего отобразить связи в реальной жизни с результатами теоретических расчетов необходимо применение корреляционного анализа – метода обработки статистических данных, с помощью которого измеряется теснота связи между двумя или более переменными, что особенно важно для исследования социальных явлений (в том числе преступности) и особенно в киберпространстве.

Корреляционный анализ тесно связан с регрессионным, с его помощью определяют необходимость включения тех или иных факторов в уравнение множественной регрессии, а также оценивают полученное уравнение регрессии на соответствие выявленным связям.

С помощью факторного анализа можно решить две основные задачи: сделать описание компьютерной преступности кратко и в то же время всесторонне. Используя факторный анализ можно выявить факторы, отвечающие за наличие связей между исследуемыми переменными. Указанное позволяет, например, при проведении аналитической работы, сопутствующей профилактике, раскрытию, расследованию компьютерных преступлений, анализировать оценки, полученные по нескольким шкалам, выявлять среди них сходные между собой и имеющие высокий коэффициент корреляции, что позволяет предполагать о существовании латентной переменной, с помощью которой можно объяснить наблюдаемое сходство полученных оценок. Такая латентная переменная и является тем фактором, который влияет на многочисленные показатели других переменных, что приводит к возможности и необходимости отметить его как наиболее общий, более высокого порядка. Таким образом, можно выделить две цели факторного анализа при исследовании преступлений в сфере высоких технологий:

определение взаимосвязей между переменными, их классификация, т. е. «объективная R-классификация»;

сокращение числа переменных.

Для выявления наиболее значимых факторов целесообразно применять метод главных компонентов. С помощью этого метода можно уменьшить размерность данных путем замены взаимосвязанных (коррелируемых) компонентов на не связанные факторы. Другой важной характеристикой метода является возможность ограничиться наиболее информативными главными компонентами и исключить остальные из анализа, что упрощает интерпретацию результатов.

Факторный анализ проводится в несколько этапов.

При проведении первого этапа осуществляется анализ проблемного поля в целях отбора факторов, например, обусловливающих совершение компьютерных преступлений. Второй заключается в классификации и систематизации указанных факторов. На третьем строится структура связей между результативным и факторными показателями. На четвертом проводится расчет влияния факторов и оценка роли каждого из них в изменении величины результативного показателя. Заключительным, пятым, этапом является использование факторной модели на практике.

Таким образом, с помощью факторного и корреляционного анализа из всей совокупности факторов можно выделить значимые факторы, которые достаточно точно влияют на компьютерную преступность. Для построения эффективной системы борьбы с компьютерной преступностью, выбора оптимальных мер ее профилактики требуется научное сопровождение, информационное обеспечение, важное место в котором принадлежит анализу факторов, способствующих негативным изменениям компьютерной преступности.

УДК 343.985

Д.Н. Лахтиков, кандидат юридических наук, доцент, начальник кафедры правовой информатики учреждения образования «Академия Министерства внутренних дел Республики Беларусь»
dzymitriy@yandex.by

НЕКОТОРЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

В настоящее время наблюдается устойчивый рост преступлений, совершаемых с использованием информационно-коммуникационных технологий, при этом не только преступлений против информационной безопасности и хищений с использованием компьютерной техники, но более «традиционных», таких как мошенничества, вымогательства и др.

Проблема противодействия данным преступлениям привлекает все большее внимание исследователей различных отраслей научного знания, при этом необходимость противодействия данному виду преступ-