Вопрос 3. Неформальная модель нарушителя как носителя угроз безопасности.

Преступления, в том числе и компьютерные, совершаются людьми. Пользователи системы и ее персонал, с одной стороны, являются составной частью, необходимым элементом КИС. С другой стороны, они — основная причина и движущая сила нарушений.

Как свидетельствует мировой опыт, развитие и распространение компьютерных систем сопровождается ростом правонарушений, связанных с кражами, злоупотреблениями, модификацией, неправомерным доступом к данным.

Первое компьютерное преступление в бывшем СССР было зарегистрировано в 1979 году в Вильнюсе. Ущерб государству от хищения составил 78 584 рубля. Данный факт был занесен в международный реестр правонарушений подобного рода и явился отправной точкой в развитии нового вида преступлений в России. Второе подобное деяние было совершено в 1982 году в Нижнем Новгороде. Еще одно из нашумевших первых компьютерных преступлений относится к1981 году. Экономистом Брестского областного производственного объединения были совершены хищения денежных средств путем внесения в электронные бухгалтерские документы ложных данных. Всего таким образом было похищено 22 960 рублей. 13

По оценкам западных аналитиков, ежегодный, общемировой ущерб от проникновения вирусов, червей, троянских коней составляет от 8 до 12 млрд. долларов. Достаточно вспомнить, как в 2001 году весь мир был захвачен вирусом «I love you» (ущерб — 2 млрд. долларов), а затем отличилась «Nimda» (ущерб — до 1 млрд. долларов). По различным оценкам, ежедневно в мире неизвестные умельцы создают от 2 до 10 новых вирусов.14

Нарушитель — это лицо, предпринявшее попытку выполнения запрещенных действий по ошибке, незнанию или осознанно со злым умыслом и использующее для этого различные возможности и средства. Злоумышленником называют нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Неформальная модель нарушителя системы определяет: категории лиц, в числе которых может оказаться нарушитель; возможные цели нарушителя и их градацию по важности и опасности; предположения о квалификации нарушителя; оценка его технической вооруженности; ограничения и предположения о характере его действий.

По отношению к системе всех нарушителей делят на две группы:

- внутренние (работники организации);
- внешние (посторонние лица)

Классифицировать нарушителей можно также по уровню знаний о системе, по уровню возможностей, по времени действия, по месту действия (классификации Гайковича, В.Ю., Ершова, Д.В.).

Важную роль при определении нарушителя играют **мотивы и цели совершения преступлений,** связанные с социально-психическими и криминалистическими характеристиками личности, и, входя в группу субъективных факторов, решающим образом влияют на выбор средств достижения цели, определяют характер действий преступника и содержание способа совершения преступления.

Наиболее распространенные мотивы совершения компьютерных преступлений:

- корысть (66%);
- политические мотивы (17%);
- чисто любознательный интерес (7%);
- хулиганские побуждения и озорство (5%);
- месть (5%).

Наиболее типичные цели преступников: подделка счетов и фальсификация платежных документов; хищение денежных средств и материальных ценностей; легализация преступных доходов; незаконное получение кредитов; осуществление незаконных валютных операций; продажа конфиденциальной информации.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Построение модели нарушителя является составной частью работы обеспечению информационной безопасности и позволяет повысить уровень защищенности информации.