

УДК 342.742:004.681

Я.В. Невойт, Л.Н. Мазуренко, В.А. Хорошко, В.С. Чередниченко

*Государственный университет информационно-коммуникационных технологий, Киев*

## МОДЕЛЬ ПОТЕНЦИАЛЬНО-ОПАСНОЙ ГРУППЫ ДЛЯ ПРЕДУПРЕЖДЕНИЯ УТЕЧКИ ИНФОРМАЦИИ

*В работе рассматриваются и анализируются модели преступного механизма, размещения, действия преступной группы и службы безопасности защищаемого объекта.*

**Ключевые слова:** преступная группа, служба безопасности, объект, внутренний нарушитель, внешний нарушитель.

### Введение

Стремительное развитие информационных технологий стало одним из криминогенных факторов, детерминирующих наиболее опасную форму преступности – организованную транснациональную.

Переход на методы электронного управления технологическими процессами послужил основанием для появления нового вида терроризма, которое проявляется во вмешательстве в работу компонентов телекоммуникационных сетей, функционирующих в их среде компьютерных программ, несанкционированной модификации компьютерных данных, что вызывает дезорганизацию работы этих средств, а также несанкционированное получение информации.

В настоящее время сотрудник объекта является основным источником информации для группы, планирующей совершить преступление на объект или самостоятельно совершить преступление.

Каждый человек адаптирован к физической, социальной и нравственно-психологической среде, в которой протекает его жизнь. Для преступника можно утверждать об отсутствии правильной адаптации к внешней среде. Это рассогласование можно рассматривать как результат деформации ряда звеньев психологического процесса мотивации в принятии решений (потребностей, интересов, целей, средств их достижения) [1].

В условиях современного кризиса в экономике, социальной и духовной жизни микросреда личности (семья, коллеги, круг общения) испытывать особую напряженность, подчас разрушая правовые и общественные нормы поведения. В значительной степени это происходит под влиянием фактов несправедливости, грубости, жесткости, нечестных поступков, нередко оказывающихся для кого-либо выгодными и поощряющимися друзьями и окружением, но не одобряемыми общественной моралью. Особенно значима в формировании личности роль государственных решений, которые подчас оказываются ошибочными, несправедливыми. Все это постепен-

но убеждает субъекта в ничтожности общественной морали, бессилии права. В итоге образуется временное или постоянное рассогласование личности с окружающей позитивной средой, лежащее в основе большинства форм преступного поведения.

В настоящее время не существует скольких-нибудь конкретных и полных по содержанию методологических разработок по организации в технике предупреждения утечки информации и преступлений в сфере защиты информации.

На основе данных полученных в ходе анализа отечественной и зарубежной специальной литературы и публикаций в периодической печати по вопросам теории и практики предупреждения утечки информации, можно выделить две основные группы мер предупреждения этих преступлений:

- правовые;
- организационно-технические [2].

**Цель настоящей работы** – построение моделей блоков преступного механизма, размещения преступной группы, действий преступной группы и службы безопасности объекта, а также схемы функционирования автоматизированной системы предупреждения преступлений. То есть, это относится к реализации организационно-технических мероприятий.

Предлагаемые модели дают возможность анализировать характер совершения преступлений, а также предлагать реально действующие способы реализации по борьбе с утечкой информации и предупреждения ее утечки.

### Основные положения

Рассмотрим основные блоки преступного механизма (рис. 1). Каждый из трех блоков механизма преступного поведения представляет собой сложное образование, включающие разнообразные психические состояния и процессы, влияние внешней среды, принимаемые человеком решения и обратные связи.

Планирование преступления может включать в себя: цели (основные, конечные, промежуточные, дополнительные); объекты (собственность, лич-

ность, межличностные отношения, государственный аппарат); средства (насилия, подлог, обман, подкуп, угроза, хищение, порча, нарушение).

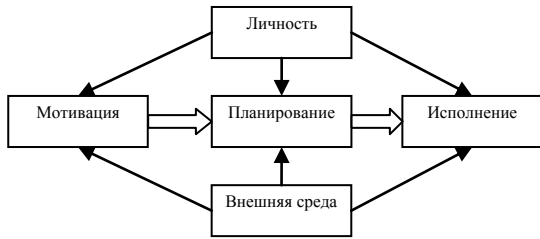


Рис. 1. Основные блоки преступного механизма

Принятие решения включает в себя: варианты поведения, ситуацию, ее прогноз, которые в зависимости от следующих элементов ценностных ориентаций, стереотипов поведения, интересов приводят к принятию решения о совершении преступления.

Исполнение или совершения преступления зависит от следующих элементов: самоконтроля (адекватного, искаженного, ослабленного); результата (достижение цели, социальный вред, ответственность); типа преступления (умышленное, неосторожное); условий (технических, организационных, психологических, способствующих, препятствующих).

Теперь рассмотрим группу, совершающую преступные действия: хищение информации или материальных ценностей. Назовем такую группу преступной группой.

Предлагаются, разработанные авторами, четыре модели размещения преступной группы (рис. 2).

В качестве модели нарушителя рассматриваются четыре варианта преступной группы, принятые на основании [3].

1. Преступная группа, не включающая в себя персонал объекта.
2. Лица из внешней среды, связанные с персоналом объекта (группа со стороны является инициатором и воздействует на персонал).
3. Персонал объекта, связанный с лицами из внешней среды (персонал сам выходит на связь).
4. Персонал объекта.

Рассмотрим более подробно каждую модель преступной группы с учетом [4].

*Преступная группа, не связанная с персоналом объекта.* Эта группа характеризуется невысокой осведомленностью о структуре объекта, барьерах защиты, информация в основном получается из отрывочных разговоров сотрудников, из каналов утечки информации, внешнего и частичного внутреннего осмотров охраняемого объекта, наблюдения за маршрутами движения машин и патрулирования. Как правило, преступление, осуществляемое этой группой, производится на объектах с очень слабой системой охраны или “случайным” знанием “слабо-

го” места в системе охраны.

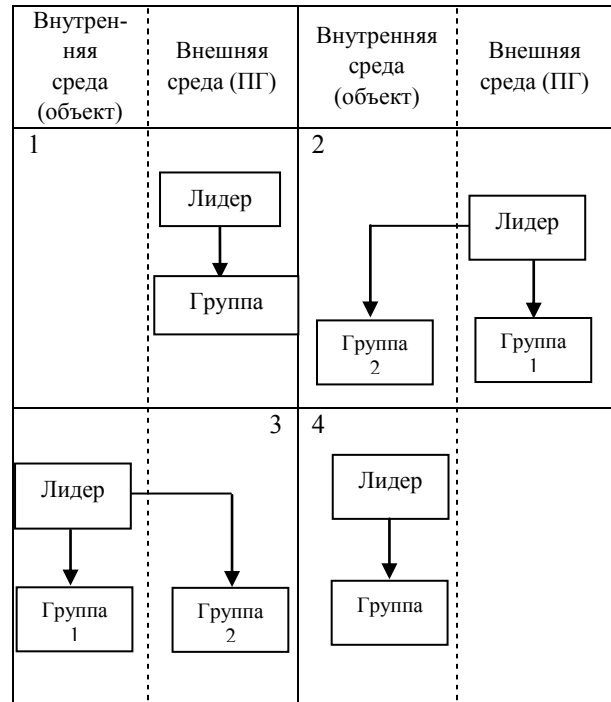


Рис. 2. Размещение преступной группировки

*Преступная группа, связанная с персоналом объекта.* Разделим персонал объекта на активно или пассивно помогающий преступной группировке.

Пассивная помощь может заключаться в сообщении сведений о передвижении спец ресурсов, размещением их на объекте, слабых местах в системе охраны, рубежах системы охраны, возможных каналах утечки информации и т.д.

Сообщение сведения делятся по возможности с точки зрения помощи преступникам в совершении преступления, объема похищенной информации, причиненному ущербу объекта.

Активная помощь может осуществляться в содействии в приеме на работу членов преступной группы и продвижение их по службе, непосредственном участии в подмене документов и носителей информации, отключении технических средств охраны, нейтрализации охраны, открытие дверей и других средств хранения носителей информации.

Такие преступления тщательно разрабатываются и осуществляются при удобном случае.

*Персонал объекта, связанный с преступной группой.* В данном случае персонал объекта является инициатором совершения хищения информации.

*Персонал объекта, не связанный с преступной группой.* В этом варианте необходимо рассмотреть схему действий преступной группы и службы безопасности объекта на основе предлагаемой модели (рис. 3).

Массовые источники информации, такие как тестирование, информаторы, проверки, руководители подразделений, представляют первичную ин-

формацию о сотрудниках, клиентах и их взаимодействие, а также о связях с внешними организациями. После обработки данных массовых источников информации выявляются потенциально опасные группы, производится доскональный и подробный анализ и осуществляется прогноз их развития.

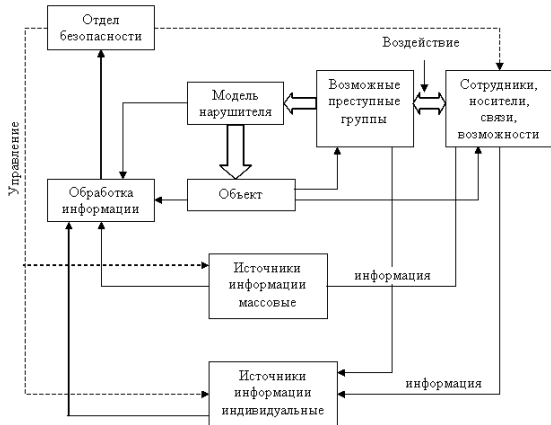


Рис. 3. Модель действий преступной группировки и службы безопасности объекта

Выявленные потенциально опасные лица и группы проверяются с использованием индивидуальных источников информации, таких как полиграф, аудит контроль, видео контроль, физическое наблюдение, внедрение агента в преступную группу, сбор информации по месту жительства. Далее снова используются массовые методы поиска.

Для реализации описанной модели действий преступной группы и службы безопасности объекта предлагается схема функционирования автоматизированной системы предупреждения преступлений, которая позволяет описать и проанализировать развитие возможных преступных групп. Причем возможно рассмотреть динамику развития группы и привлечение в нее сотрудников объекта для увеличения ее профессиональной подготовки к совершению преступления. Возможность привлечения определяется степенью взаимной связи члена преступной группы и сотрудника объекта, возможностью воздействия на него и необходимости знаний и умений данного сотрудника привлечения в группу.

На основании данной зависимости осуществляется анализ развития преступной группы (рис. 4).

### МОДЕЛЬ ПОТЕНЦІЙНО-ЗАГРОЗЛИВОЇ ГРУПИ ДЛЯ ПОПЕРЕДЖЕННЯ ВИТОКУ ІНФОРМАЦІЇ

Я.В. Невойт, Л.Н. Мазуренко, В.А. Хорошко, В.С. Чердниченко

*В даній роботі розглядаються та аналізуються моделі злочинного механізму, розміщення злочинної групи і дії злочинної групи та служби безпеки захищеного об'єкта.*

**Ключові слова:** злочинна група, служба безпеки, об'єкт, внутрішній порушник, зовнішній порушник

### THE MODEL OF POTENTIAL-DANGEROUS GROUP FOR WARNING OF LOSS OF INFORMATION

Y.V. Nevoyt, L.N. Mazurenko, V. A. Khoroshko, V.S. Cherednichenko

*In-process examined and analysed the model of criminal mechanism, placing of criminal group and action of criminal group and service safety of the protected object.*

**Keywords:** criminal group, service to safety, object, internal violator, external violator.

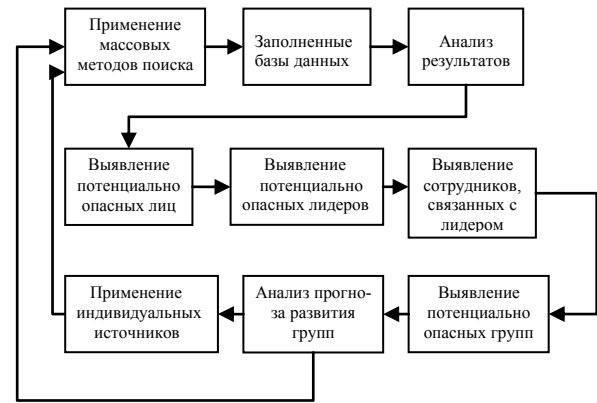


Рис. 4. Схема функционирования автоматизированной системы предупреждения преступлений

В случае привлечения в группу нового члена, который необходим группе для совершения возможного преступления, это является сигналом службе безопасности о возможном формировании преступной группы.

## Выводы

Данные подходы могут быть применены для автоматизированной обработки аналитической информации.

Показано, что предлагаемые модели позволяют выявить преступную группу, а также предупредить преступление и сохранить информацию.

## Список литературы

1. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К.: Юниор, 2003. – 504 с.
2. Кобозева А.А. Использование взвешенного графа при моделировании террористической сети / А.А. Кобозева, В.А. Хорошко // Інформаційні технології та комп'ютерна інженерія. – 2007. – № 3(10). – С. 61-67.
3. Кудрявцев Б.Н. Генезис преступления / Б.Н. Кудрявцев. – М.: Инфра – М, 1998. – 214 с.
4. Живко З.Б. Конкурентна(ділова) розвідка в системі економічної безпеки / З.Б. Живко. – Львів : АПРІОПІ, 2008. – 192 с.

Поступила в редколлегию 4.03.2009

**Рецензент:** д-р техн. наук, проф. А.А. Кузнецов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.