Scientific and Practical Cyber Security Journal (SPCSJ) 2(3): 01-07 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

MODELS OF INTERACTION OF A POTENTIALLY DANGEROUS TERRORIST GROUP AND THE SECURITY SERVICE ON A PROTECTED OBJECT

Mykola Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor Kiev, Ukraine, bk1972@ukr.net
Volodymyr Khoroshko, National Aviation University, Doctor of Engineering Science, Full Professor, Kiev, Ukraine, professor_va@ukr.net

ABSTRACT. In this paper, we analyze the models of a terrorist group (criminal mechanism), its deployment, as well as the actions of a terrorist group and security services on the protected object.

Аннотация В данной работе рассматриваются и анализируются модели террористической группы (преступного механизма), его размещение, а также действия террористической группы и службы безопасности на защищаемом объекта.

KEYWORDS: terrorist group, security service, object, internal violator, external violator.

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

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

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

В настоящее время сотрудники защищаемого объекта являются основным источником информации для террористической группы (ТГ), планирующей совершить преступление на объекте или самостоятельно совершить террористический акт.

Сотрудники были, есть и будут самой большой проблемой для организаций любой формы собственности и любого направления деятельности. Как известно, более 60% утечек информации происходят по вине внутреннего нарушителя. Тем более, когда речь идет о людях, работающих с ценной информацией или «живыми» деньгами и каждый день подверженных соблазну. Одной из задач системы управления информационной безопасностью является

создание оптимальных условий для предотвращения или эффективного расследования должностных преступлений. В таких случаях умышленные действия любого из инсайдеров должны быть однозначно установлены и доказаны.

Каждый человек адоптирован к физической, социальной и нравственно-психологической среде, в которой протекает его жизнь. Для террориста 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 для их достижения) [1].

В современных условиях как в экономике, так и в социальной и духовной жизни микросреда личности (семья, коллеги, круг общения) испытывает особую напряженность, подчас разрушая правовые и общественные нормы поведения. В значительной степени это происходит под влиянием факторов несправедливости, грубости, жестокости, нечестных поступков, нередко оказывающихся для кого-то выгодными и поощряемыми друзьями и окружением, но не одобряемыми общественной моралью. Особо значима в формировании личности роль государственных решений, которые подчас оказываются ошибочными и несправедливыми. Все это постепенно убеждает субъекта в ничтожности общественной морали, бессилия права. Кроме того, особое влияние на субъект оказывает религиозное воспитание, которое осуществляется с малолетства и широко используется в мусульманских странах. В итоге образуется временное или постоянное рассогласование личности и окружающей позитивной среды, лежащей в основе большинства форм преступного поведения.

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

На основании данных, полученных в ходе анализа отечественной и зарубежной специальной литературы, и публикаций в периодической печати по вопросам теории и практики предупреждения утечки конфиденциальной и другой информации, можно выделить две основные группы мер предупреждения этих преступлений [2]:

- правовые;
- организационно-технические.

Цель настоящей работы – построение блоков преступного механизма, размещения ТГ, действий ТГ и службы безопасности объекта, а также схемы функционирования автоматизированной системы предупреждения преступлений, как в информационном, так и киберпространстве.

Предлагаемые модели дают возможность анализировать характер совершенных преступлений и террористических актов, а также предлагать

реально действующие способы борьбы с утечкой конфиденциальной информации.

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

Планирование преступления (террористического акта) может включать в себя цели (основные, конечные, промежуточные, дополнительные); объекты (собственность, личность, межличностные отношения, государственный аппарат); средства (насилие, подлог, обман, подкуп, угроза, хищение, порча, нарушение, уничтожение).

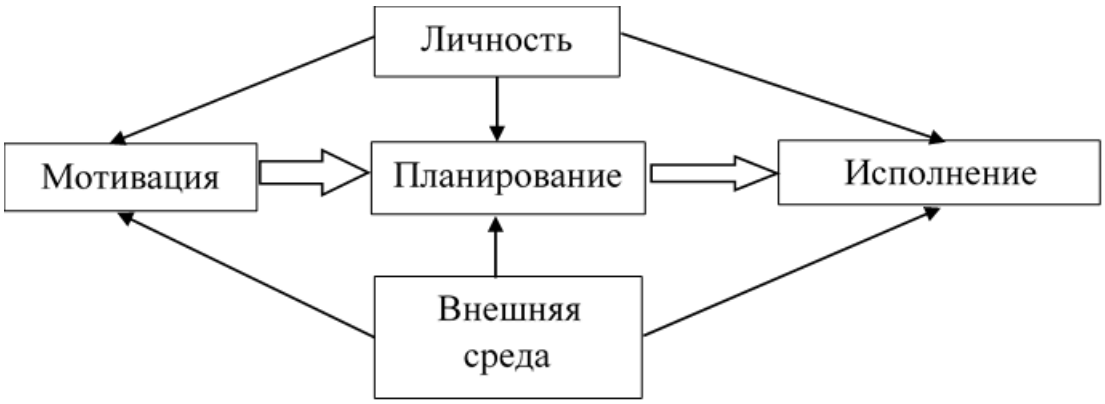


Рис. 1. Основные блоки преступного механизма.

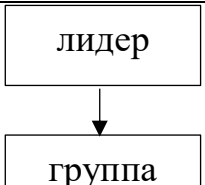
Принятие решения включает в себя: ситуацию, ее прогноз, варианты поведения, которые в зависимости от следующих элементов ценностных ориентаций, стереотипов поведения, интересов приводят к принятию решения о совершении преступления (террористического акта).

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

Теперь рассмотрим группу, совершающую преступные действия (террористический акт) против информации или материальных ценностей. Назовем такую группу ТГ или преступной группировкой.

Предлагается, разработанные авторами, четыре модели размещения ТГ (рис.2.).

Внутренняя среда (объект)	Внешняя среда (ТГ)	Внутренняя среда (объект)	Внешняя среда (ТГ)
	1	2	



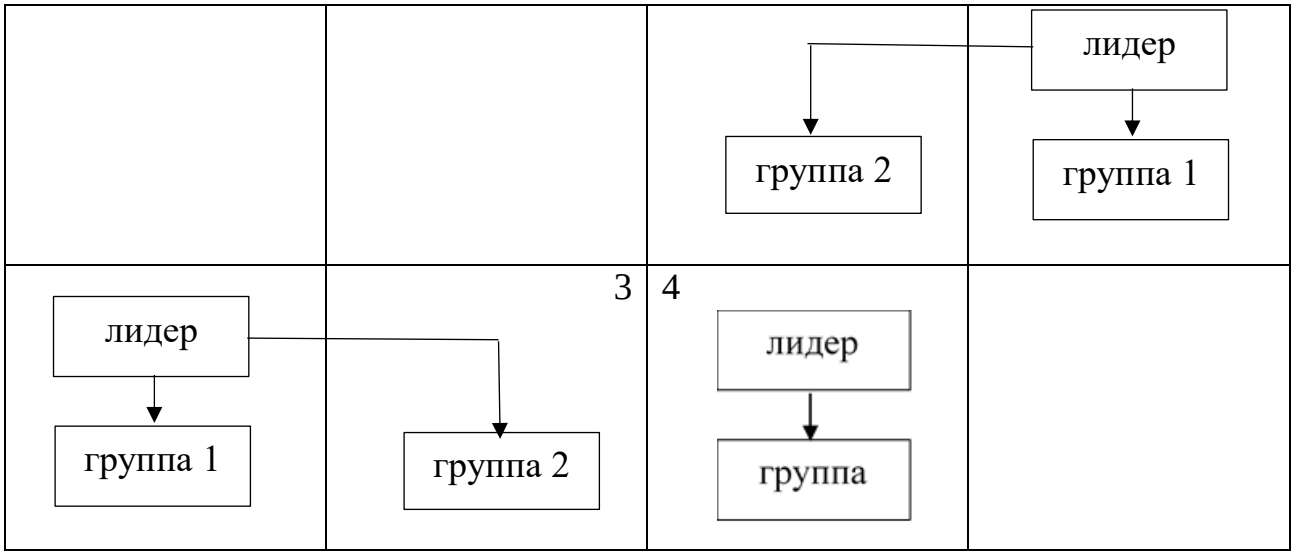


Рис.2. Размещение ТГ.

В качестве модели нарушителя рассматриваются четыре варианта ТГ, принятые на основе [3].

1. ТГ не включает 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 объекта сам выходит на связь).
4. Персонал объекта.

Рассмотрим более подробно каждую модель ТГ с учетом [4,5].

ТГ не связанное с персоналов объекта.

Эта группа характеризуется невысокой осведомленностью о структуре объекта, барьерах и рубежах защиты, информация в основном получается из отрывочных разговоров сотрудников, из каналов утечки информации, внешнего и частично внутреннего осмотров охраняемого объекта, наблюдения за маршрутами движения машин и патрулирования объекта. Как правило, преступление, осуществляемое этой группой, производится на объектах с очень слабой системой охраны или «случайным» получениям информации о «слабом» месте в системе охраны.

ТГ связанное с персоналов объекта.

Разделим персонал объекта на активно или пассивно помогающий террористической группировке.

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

Сообщение сведений делятся по возможности с точки зрения помощи преступникам в совершении преступления, объема похищенной информации или причинённому ущербу.

Активная помощь может осуществляться в содействии в приеме на работу членов ТГ и продвижении их по службе, непосредственное участие в подмене документов и носителей информации, отключении технических средств охраны и защиты, нейтрализация охраны, открытие дверей и других средств хранения носителей информации.

Такие преступления тщательно разрабатываются и осуществляются при удобном случае.

Персонал объекта, связанный с ТГ

В данном случае персонал объекта является инициатором совершения хищения или уничтожения информации.

Персонал объекта не связанный с ТГ

В этом варианте необходимо рассмотреть схему действий ТГ и службы безопасности объекта на основе предлагаемой модели (рис.3.).

Массовые источники информации, такие как тестирование, информаторы, проверки, руководители подразделений, представляют первичную информацию 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.

Выявленные потенциально опасные лица и группы проверяются с использованием индивидуальных источников информации, таких как полиграф, аудит контроль, видео контроль, физическое наблюдение, внедрение агента в ТГ, сбор информации по месту жительства. Далее снова используется массовый метод поиска.

Для реализации описанной модели действий ТГ и службы безопасности объекта предлагается схема функционирования автоматизированной системы предупреждения преступлений, которая позволяет описать и проанализировать развитие возможных ТГ. 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 ТГ и сотрудника

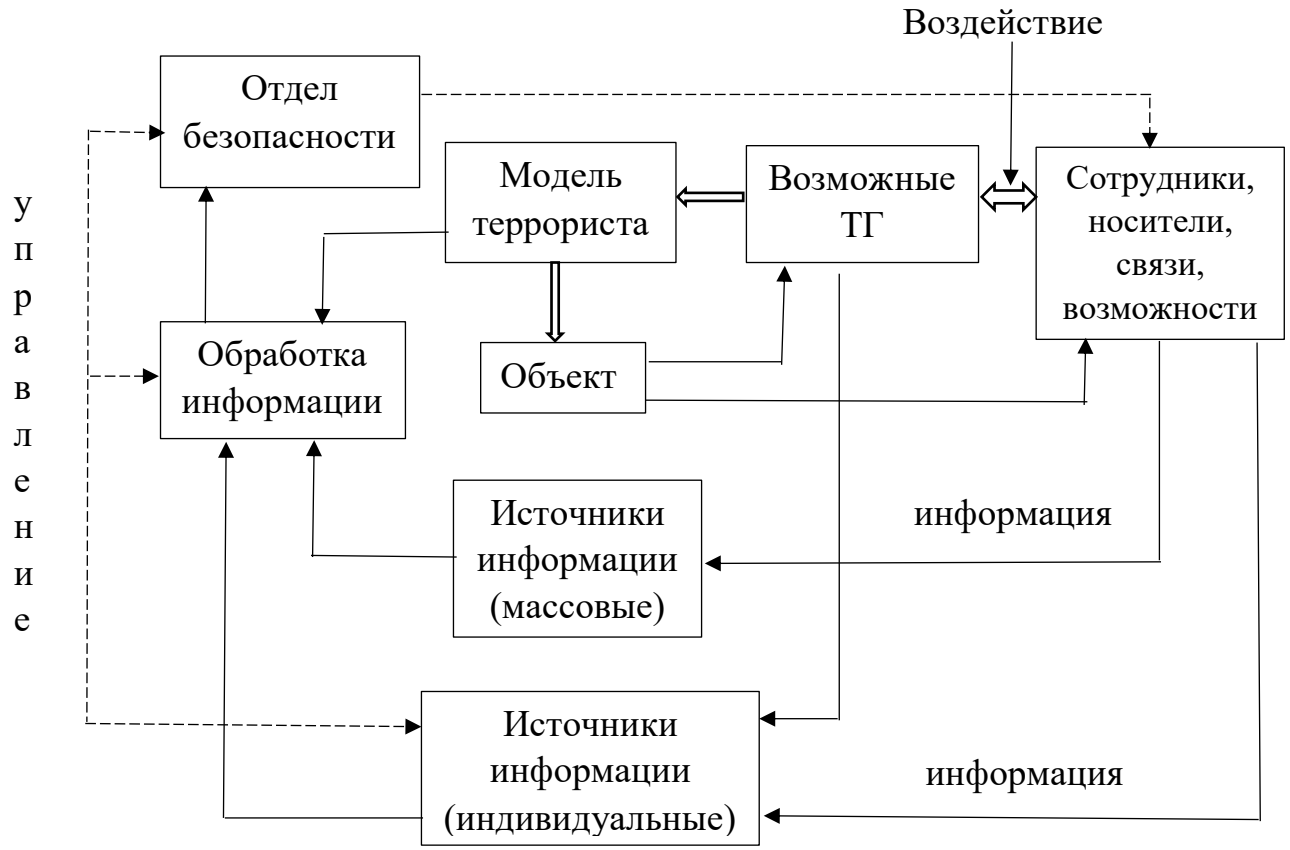


Рис. 3. Модель действия ТГ и службы безопасности объекта

объекта, возможностью воздействия на него и необходимости знаний и умений данного сотрудника привлечения в группу.

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

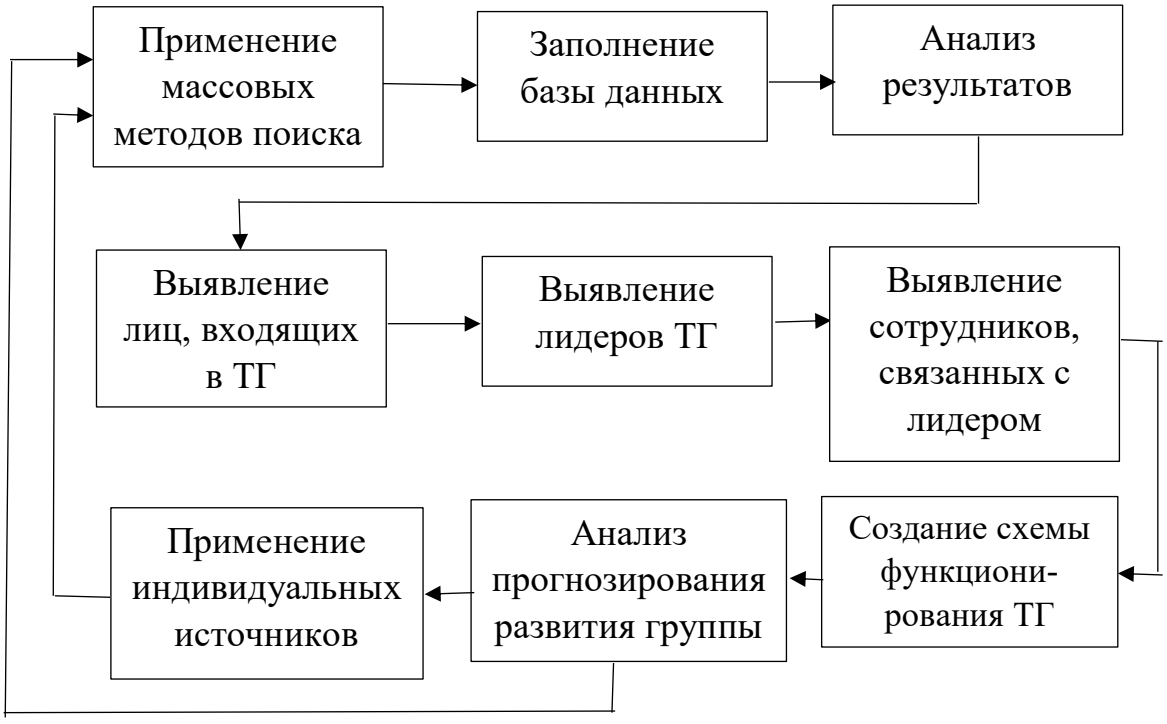


Рис.4. Схема функционирования автоматизированной системы предупреждения преступлений

В случае привлечения в группу нового члена, который необходим ТГ для совершения возможного преступления (террористического акта), это является сигналом службе безопасности о возможном формировании ТГ.

Выводы

Данные подходы могут быть применены для автоматизированной обработки аналитической информации.

Показано, что предлагаемые модели позволяют выявить террористическую группу на раннем этапе, что позволит предупредить преступление и сохранить информацию.

Литература

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. В 2-х томах. – К.: Арий, 2008.
2. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности. –Л.: Изд. ГУИКТ, 2009. -251 с.
3. Голубев В.О., Гавловський В.Д., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп’ютерних технологій – Запоріжжя: ГУ «ЗІДМУ» 2002. – 292 с.
4. Живко З.Б. Конкурента (ділова) розвідка в системі економічної безпеки – Львів: АПРІОРІ, 2008. – 192 с.
5. Хорошко В.А., Шелест М.Е. Информационно-аналитическое обеспечение безопасности. – К.: ВПВ «Задруга», 2016. – 183 с.