Формирование модели нарушителя при нападении на важный государственный объект

А.С. Олейник

Академия управления МВД России, Москва

Аннотация: В статье рассмотрены вопросы формирование модели нарушителя при нападении на важный государственный объект. Описана классификация нарушителей по типам.
В статье предложена простейшая модель оценки эффективности сговоров нарушителей.
Ключевые слова: комплексная безопасность, методы, модели, силы охраны, нарушители, важные государственные объекты, столкновения сил охраны и нападения, модели нарушителя.

Под моделью нарушителя понимается логическое и математическое его описание, направленное на исследование определенных свойств и характеристик нарушителя, влияющих на выбор и значение показателя эффективности системы физической защиты (далее – СФЗ).

Таким образом, под формированием модели понимается определение перечня характеристик нарушителя, влияющих на эффективность СФЗ. Эти характеристики в последующем используются при моделировании функционирования СФЗ с целью определения ее эффективности. Задача формирования модели нарушителя - одна из главных задач анализа уязвимости, поскольку нарушитель является важнейшей объективной причиной необходимости охраны объекта. Если нет нарушителей, то и СФЗ становится практически ненужной.

Перечень свойств нарушителя, которые необходимо учитывать в модели, во многом определяется характеристиками важного государственного объекта (далее – ВГО) и внешними условиями. Он может изменяться во времени и служит, наряду с угрозами и другими факторами, одним из своеобразных фильтров, определяющих возможность достижения тех или иных целей несанкционированных действий на объекте.

К любым моделям обычно предъявляются следующие требования:

- корректность и достаточная точность;
- чувствительность;
- относительная простота;
- обеспеченность известным аппаратом исследования.

Необходимо отметить, что требования в практических задачах могут вступать в противоречие. Примером такого противоречия может служить точность и простота. Как правило, чем выше точность модели, тем она сложнее. Поэтому при формировании модели задачей эксперта является отыскание разумного компромисса в выполнении требований к ней.

Классификация нарушителей по типам может быть осуществлена по нескольким признакам. Это определяется множественностью описания нарушителя. Если в качестве признака взять отношение к объекту, то нарушители могут быть внешними, внутренними и образовавшими группу в результате сговора. Если в качестве признака взять причинность совершения противоправных действий, то к основным типам нарушителей относятся:

- члены террористических организаций, осуществляющие несанкционированный доступ (далее – НСД);
- члены экстремистских групп (объединений), пытающиеся реализовать свои цели через проведение противоправных акций на объекте;
- лица, имеющие преступные наклонности;
- сотрудники объекта, принуждаемые к преступным действиям другими типами нарушителей путем подкупа, шантажа или угрозы применения силы;
- сотрудники объекта, недовольные условиями работы и пытающиеся решить свои вопросы путем проведения противоправных акций;
- психически неуравновешенные люди.

Мотивами, которые могут побудить потенциальных нарушителей к совершению преступных действий, могут являться:

- политические (идеологические);
- экономические;
- экологические;
- личные.

Идеологические мотивы обычно связаны с политической философской системой взглядов определенных групп людей могут руководствоваться террористы, экстремисты и радикальные группы религиозных фанатиков.

Экономические мотивы связаны с желанием получения финансовых выгод. При этом ценности, имеющиеся на ВГО, становятся предметом хищений с целью продажи. Экологические мотивы связаны с выдвижением требований о прекращении деятельности объекта по причине загрязнения окружающей среды. Эти мотивы наиболее часто проявляются по отношению к ядерно-опасным объектам, крупным химическим комбинатам, предприятиям деревообработки и ряда других. Личностные мотивы связаны со специфическими обстоятельствами, характерными для определенных лиц, и могут быть вызваны отношениями в коллективе, социальными и другими причинами.

К общим целям, которые могут преследовать нарушители, можно отнести:

- диверсию в отношении объекта;
- захват заложников на объекте с целью выдвижения требований путем угроз совершения диверсии;
- нарушение нормального функционирования предприятия за счет воздействия на технологический процесс или другим путем;
- хищение материальных ценностей;
- хищение конфиденциальной информации об объекте.

К тактикам, которые используются нарушителями на ВГО, и особенно часто рассматриваются при анализе уязвимости, относятся:

- насильственная (силовая) - допускает применение насилия к людям и разрушение (повреждение) инженерно-технических средств;

- обманная - с использованием поддельных документов, ключей, идентификаторов личности и т. п.;

- скрытная - когда нарушитель при совершении своей акции стремится остаться незамеченным;

- комбинированная - различные сочетания тактик, упомянутых тактик упомянутых выше.

При решении реальных задач на конкретных объектах число анализируемых тактик может увеличиваться, причем дополнительно включенные в перечень тактики при ранжировании могут оказаться главными. Так, для ВГО высоких категорий с весьма эффективными СФЗ в качестве дополнительных элементов общей тактики можно рассмотреть:

- сговор внешнего и внутреннего нарушителей с последующими совместными действиями по достижению цели;

- принуждение внешними нарушителями сотрудников объекта к НСД;

- внедрение внешними нарушителями на объект сообщников, которые в последующем должны облегчить достижение целей нарушителей;

- использование нарушителями в своих целях персонала, временно работающего на объекте;

- непрогнозируемые, специфичные действия, определяемые особенностями функционирования объекта.

Значительное влияние на выбор тактики нарушителя оказывают остальные его характеристики: уровень подготовленности к проведению акции, финансовый, временной и технический ресурсы.

Все рассмотренные характеристики определяют выбор и возможность достижения целей несанкционированного доступа на конкретном объекте. Еще раз необходимо отметить, что характеристики нарушителей связаны

между собой, и эти связи должны быть выявлены при формировании его модели. Кроме того, при формировании модели должны быть использованы имеющиеся данные о возможностях преодоления рассматриваемыми типами нарушителей технических средств охраны и физических барьеров. В концентрированном виде такая информация накапливается в базах данных компьютерных программ по оценке эффективности СФЗ.

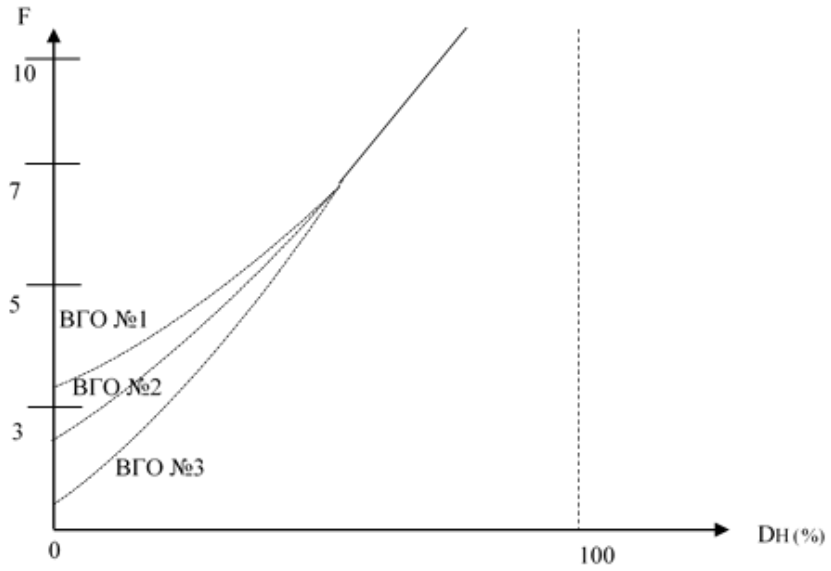

Рис. 1. Характер зависимости изменения необходимого превышения сил охраны над нарушителями от допустимого уровня потерь нарушителей

Необходимо сделать отдельное пояснение понятия допустимого для нарушителя уровня собственных людских потерь при проведении противоправной акции. Очевидно, что чем выше этот уровень, тем большее число сил охраны потребуется для нейтрализации нарушителей. Допустимый уровень потерь Dн может колебаться от ноля (нарушители планируют проведение акции без собственных жертв), до 100% (акцию проводят нарушители смертники). Возможный вид графиков зависимости необходимо

для нейтрализации нарушителей соотношения сил охраны для трех условных типов ВГО представлен на рис. 1 Коэффициент F определяется как необходимое для нейтрализации нарушителей соотношение сил охраны и нарушителей в условиях примерно одинакового их вооружения и боевой подготовки.

Аналогичная по смыслу зависимость существует и между допустимым уровнем потерь сил охраны (антитеррористической группы) D_0 и требуемым для достижения успеха соотношением сил сторон. Характер кривых, отражающих эту зависимость, представлен на рис. 2.

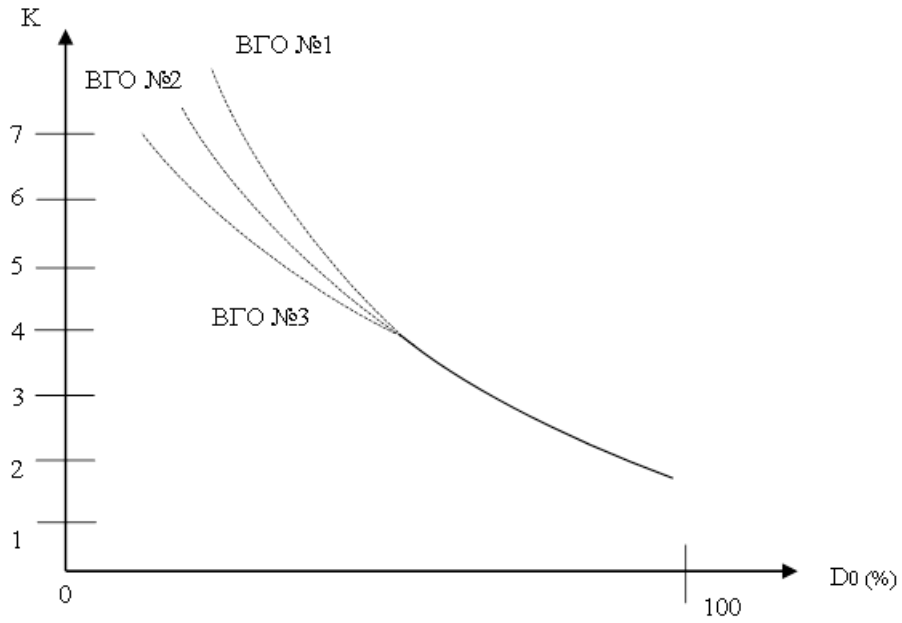

Рис. 2. Характер зависимости изменения необходимого превышения сил охраны над нарушителями от допустимого уровня потерь сил охраны

На сегодняшний день, по имеющейся информации, вопросы о допустимых уровнях потерь ни в научном, ни в правовом плане не только не решались, но даже и не ставились. Однако угрозы терроризма сейчас таковы, что эти вопросы требуют проработки во всех направлениях, а по ряду аспектов необходимо иметь правовое решение. В практических задачах,

решаемых в настоящее время, в качестве исходного соотношения сил охраны и нарушителей может быть принято F = 3. Это соотношение необходимое для уничтожения террористов без учета допустимого уровня потерь сил охраны.

Необходимо сделать одно весьма важное замечание. Рассматривая формирование модели нарушителя в рамках анализа уязвимости ВГО, мы говорим о тех характеристиках нарушителя, которые влияют на показатель эффективности СФЗ, т.е. влияют на вероятности обнаружения, задержки и нейтрализации. При этом в общем плане мы говорили о низшем уровне иерархии нарушителей - исполнителях несанкционированных действий. В целом же для всех типов нарушителей существует определенная иерархия их уровней. Наиболее она развита для диверсантов (террористов). В частном случае иерархия для террористов может быть представлена в - следующем виде:

- «заказчики террористической напряженности». Эти люди, как правило, в настоящее время не рассматриваются как имеющие отношение к терроризму. К этой группе относятся крупные политики или бизнесмены, политические или финансовые интересы которых в той или иной степени зависят от активности террористического движения в общемировом, государственном или региональном масштабе. Цели этих групп могут достигаться, например, через смену власти в государствах или серьезные финансово-экономические изменения на мировых рынках;

- руководители террористических движений или объединений (второй уровень). Эти люди на сегодняшний день, как правило, рассматриваются общественным мнением как высший уровень террористов, как организаторы и заказчики крупных терактов или их серий;

- террористы-аналитики (третий уровень). Эти люди разрабатывают общую концепцию диверсионно-террористической деятельности в мире, регионе или государстве;

- главари террористических групп или объединений (четвертый уровень);
- исполнители диверсионно-террористических актов (пятый уровень).

Очевидно, что приведенная иерархия является только примером и может быть расширена за счет большей детализации или сужена за счет того, что некоторые уровни на практике могут сливаться между собой. Важность примера состоит в том, чтобы показать, что каждый уровень должен иметь соответствующее противодействие. Основными в борьбе с первым уровнем должны быть международные организации и объединения политических лидеров государств, со вторым - вооруженные силы и разведывательные ведомства одного или нескольких государств, с третьим и четвертым специализированные штабы контртеррористической борьбы, только с пятым - системы физической защиты объекта. Правильное распределение функций между контртеррористическими организациями является одним из важнейших факторов в борьбе с терроризмом в целом.

В настоящее время оценка сговоров нарушителей изучена явно недостаточно. В [1] предложена простейшая модель оценки эффективности сговоров, которая сводится к тому, что внутренний нарушитель помогает внешнему осуществить вынос с объекта какого-либо предмета (материала). Такой подход, безусловно, не охватывает всех возможных вариантов сговора, а главное, не предлагает математического подхода к оценке их эффективности.

В общем случае под сговором понимается объединение усилий (в том числе и полномочий) различных типов нарушителей для совершения совместной противоправной акции на объекте [2-4].

Столь широкая формулировка сговора предполагает, что он может осуществляться не только между внешним и внутренним нарушителем, но и

любыми типами нарушителей с самым широки трактованием понятия «усилий». Сговоры могут возникать на любых типах ВГО, но особенно они опасны на объектах высоких категорий (с высокими потенциальными потерями). Именно на этих объектах сговор позволяет преодолевать достаточно эффективные СФЗ. В свою очередь, весьма дорогостоящие и эффективные СФЗ созданные без учета сговоров, могут оказаться против них фактически бесполезными [5-7].

Специфика ВГО различных типов и, прежде всего, их производственных процессов и предметов физической защиты, делают создание единой математической модели сговоров весьма сложной [5-7]. Целесообразно рассмотреть лишь общий подход к оценке эффективности сговоров, а математическую модель разрабатывав в каждом конкретном случае, фиксируя при этом целый ряд параметров, допущений и ограничений. Разрабатываемая модель должна позволять рассчитывать значение основного показателя эффективности Рпр в условиях сговора. Формально (с точки зрения расчета Рпр) сговор представляет собой устранение или снижение эффективности части организационно-технических барьеров СФЗ за счет использования полномочий нарушителей, вступающих в сговор. Полномочия могут быть делегированы одним из нарушителей другому или объединены при совместных действиях нарушителей [8-10].

При оценке сговоров необходимо иметь в виду несколько факторов.

Поскольку полномочия сотрудников объекта, рассматриваемых «качестве потенциальных внутренних нарушителей, весьма разнообразны, то весь персонал необходимо разделить по полномочиям преодоления барьеров СФЗ законным порядком на несколько групп, исходя из соображения обеспечить простоту использования модели, целесообразно, чтобы число групп не превышало пяти-шести. С этой же целью всем объединенным в

группу потенциальным нарушителям присваиваются высшие полномочия сотрудников объекта, включенных в группу.

Под барьерами в модели сговоров понимается более широкий круг организационно-технических факторов, препятствующих достижению цели нарушителей, чем только физические барьеры. Так, в качестве барьера может быть рассмотрена необходимость иметь полномочие на использование погрузочных средств объекта или права на другие действия, которые при нарушениях становятся противоправными.

Сговоры должны рассматриваться относительно фиксированных целей нарушителей (предметов физической защиты). Именно относительно этих целей и осуществляется построение модели оценки сговора. Число целей для упрощения модели целесообразно по возможности сократить, оставив только наиболее опасные по потенциальным потерям.

Если не учесть влияния важных дополнительных возникающих при сговоре, то может сложиться впечатление (по данным таблицы), что сговор с первой группой внутренних нарушителей однозначно приводит к достижению нарушителем инициатором своей цели. В качестве примеров дополнительных факторов, которые необходимо учитывать в модели, можно привести:

- отказ внутреннего нарушителя от сговора с доведением информации о нем до компетентных органов;

- наличие на объекте скрытых источников информации, которые противодействуют заключению сговоров.

Учет этих и других факторов, определяемых спецификой ВГО, приводит к увеличению значения Рпр.

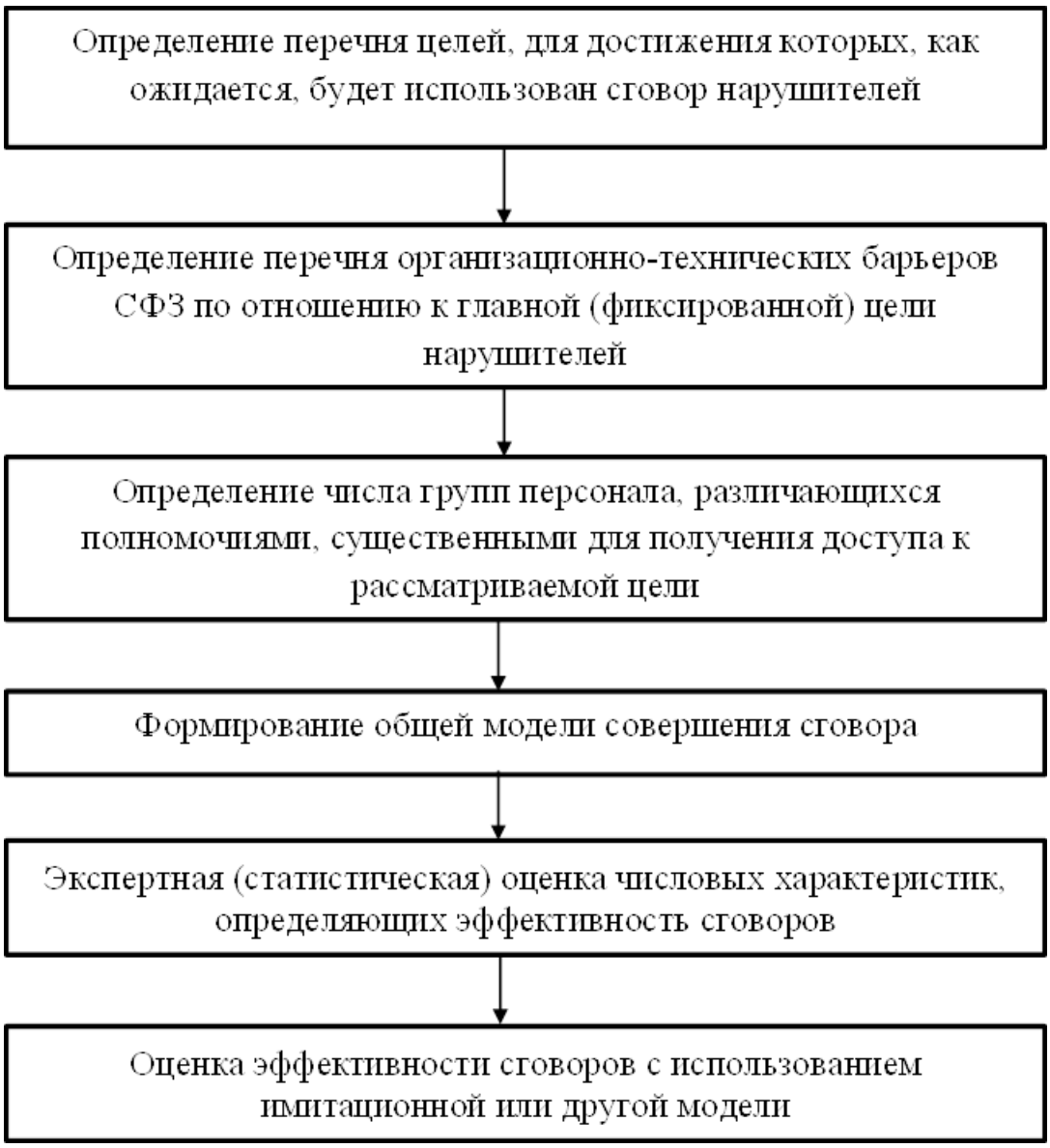

Рис. 3. Вариант алгоритма оценки эффективности сговоров

На основании сказанного может быть предложен один из вариантов обобщенного алгоритма оценки эффективности сговора нарушителей, приведенный на рис.3.

Литература

1. Олейник А.С. Методы и модели принятия решений по охране и обороне важных государственных объектов: монография. – М.: Академия управления МВД России, 2017. С. 91.

2. Цыгичко В.Н., Черешкин Д.С., Смолян Г.Л. Безопасность критических инфраструктур: монография - Изд. 2, стереотип, 2021. С. 200.

3. Цыгичко В.Н. Руководителю о принятии решения: монография, М.: Издательство Красанд, 2010. С. 95.

4. Цыгичко В.Н. Теория и практические методы принятия решений в иерархических организационных системах: монография. - Изд. 2, стереотип, 2020. С. 350.

5. Баленко С.В. Модели и методы управления операциями специального назначения. - М.: Издательство Раритет, 2002. С. 288.

6. Качанов С.А. Технологии повышения безопасности объектов повышенного риска, Технологии гражданской безопасности, 2013. №4. С. 12-15

7. Козьминых С.И. Математическое моделирование информационной безопасности органа внутренних дел. Сборник: Актуальные вопросы управления в социально-экономических системах. Сборник научных трудов Всероссийского научного семинара, 2018. С. 41-51.

8. Акимов В.А. Приложение общей теории безопасности к исследованию чрезвычайных ситуаций природного, техногенного и биолого-социального характера. Технологии гражданской безопасности. 2021. №5. С. 13-28.

9. Oleynik A.S. Blockchain technologies in the management of socio-economic systems: a study of legal practice / Revista inclusiones. 2020. volume 7, number: S4-5 - P. 10.

10. Oleynik A.S. Models of the loss of work of socio-economic systems. Revista inclusiones. 2020. volume 7, number: S3-3 - P. 17.

References

1. Oleynik A.S. Metody i modeli prinyatiya reshenij po oxrane i oborone vazhnyx gosudarstvennyx obektov: monografiya [Methods and models of decision-making on the protection and defense of important state facilities]. M.: Akademiya upravleniya MVD Rossii, 2017. P. 91.

2. Cygichko V.N., Chereshkin D.S., Smolyan G.L. Bezopasnost kriticheskix infrastruktur: monografiya [Security of Critical Infrastructures]. Izd. 2, stereotip, 2021. P. 200.

3. Cygichko V.N. Rukovoditelyu o prinyatii resheniya: monografiya [To the leader about making a decision]. M.: Izdatelstvo Krasand, 2010. P. 95.

4. Cygichko V.N. Teoriya i prakticheskie metody prinyatiya reshenij v ierarxicheskix organizacionnyx sistemax: monografiya [Theory and practical methods of decision making in hierarchical organizational systems]. Izd. 2, stereotip, 2020. P. 350.

5. Balenko S.V. Modeli i metody upravleniya operaciyami specialnogo naznacheniya [Models and methods of managing operations for special purposes]. M.: Izdatelstvo Raritet, 2002. P. 288.

6. Kachanov S.A. Texnologii povysheniya bezopasnosti obektov povyshennogo riska, Texnologii grazhdanskoj bezopasnosti, 2013. №4. pp. 12-15.

7. Kozminyx S.I. Matematicheskoe modelirovanie informacionnoj bezopasnosti organa vnutrennix del, sbornik: Aktualnye voprosy upravleniya v socialno-ekonomicheskix sistemax. Sbornik nauchnyx trudov Vserossijskogo nauchnogo seminara, 2018. pp. 41-51.

8. Akimov V.A. Texnologii grazhdanskoj bezopasnosti. 2021. №5. pp. 13-28.

9. Oleynik A.S. Revista inclusiones. 2020. volume 7, number: S4-5. P. 10.

10. Oleynik A.S. Revista inclusiones. 2020. volume 7, number: S3-3. P. 17.