Анализ угроз при проектировании систем технических средств охраны

Алексей Омельянчук. Нач. КБ Рубикон ООО «СИГМА-ИС».

Анализ угроз на особо важных государственных объектах Этот вариант самый известный и самый проработанный. Целые лаборатории в нескольких научных центрах занимаются разработкой программных средств моделирования угроз. Специальные отделы в правоохранительных органах собирают статистику и пытаются предсказывать возможные пути нападения террористов. Спецподразделения службы безопасности стараются выявить планы международных террористов. Проектировщики технических систем безопасности обязаны включать в проект раздел про анализ угроз. Как всегда, больше половины бумаг заполнены бюрократической или псевдонаучной писаниной. Тем не менее, массовый напор по всему фронту дает свои результаты.
Какие же полезные выводы могут сделать для себя простые смертные, занятые охраной небольших магазинчиков, офисов, коттеджных поселков?
Главный положительный результат, которому способствует формальное требование анализа угроз, – это отсутствие очевидных дыр в системе защиты. Даже если вы пишете анализ ради отписки, относитесь к нему как к пустой формальности – вы все равно напишете, например, какими средствами будет отражено нападение со всех четырех сторон света (и как результат не забудете запроектировать равнопрочную оборону со всех сторон). Вы не забудете рассмотреть пеших, колесных и плавающих нарушителей и потому не допустите существенных перекосов вроде железобетонного забора, обрывающегося на берегу озера на глубине по колено. Вы не забудете упомянуть как внешних, так и внутренних пособников преступников и будете вынуждены рассмотреть средства, препятствующие не только открыванию главных ворот снаружи, но и несанкционированному открыванию их изнутри.

Анализ угроз в рекомендациях британского МВД Почему именно британского? Это одни из самых проработанных рекомендаций, положенные в основу серии европейских стандартов. В целом неудивительно – Британия одна из немногих стран, живущих последние 30 лет в состоянии гражданской войны (в Ирландии). Сравнимое внимание системам безопасности оказывается только в Израиле, но там традиционно более закрытое общество, да и даже то, что публикуется открыто, увы, недоступно большинству наших соотечественников без переводчика.
Итак, британские рекомендации. В основном разрабатываются в специальном подразделении под названием «Научно-исследовательский отдел МВД» (прямой аналог нашего НИЦ «Охрана»). Кроме того, в большинстве графств шеф полиции издает свои рекомендации (как правило, буквально переписанные с рекомендаций научного отдела МВД). Строго говоря, именно рекомендации шефа полиции обязательны на территории графства, например, для получения лицензии на торговлю алкоголем, оружием или лекарствами. Впрочем, косвенно они обязательны для всех. Страховые компании имеют собственные рекомендации для категорирования клиентов по степени риска. Эти

рекомендации не публикуются открыто, но все они в первых строках включают обязательность выполнения требований шефа полиции, если, конечно, клиент хочет платить страховые взносы по минимальной ставке. Вот так и получается, что никоим образом необязательные исследовательские отчеты научного отдела становятся обязательными в реальной жизни.

Все, хватит рассуждений, опишу суть самих рекомендаций. Суть – аналогична проведению анализа угроз. Главное требование – провести анализ, от каких преступников предполагается защищать объект, в каких условиях и какие, собственно, помещения (предметы) на охраняемом объекте представляют интерес для преступников.

В зависимости от предполагаемой квалификации преступников и от общественной важности охраняемого объекта, опасности для общества преступного деяния (да-да! Это термин вовсе не изобретение социалистической законности – опасность деяния для общества во всех обществах считается важным критерием – оружейные магазины, склады наркотических веществ – обязательно охраняются значительно строже, чем следует просто из стоимости хранящихся там предметов).

Классификация предлагается достаточно простая.

Класс 1 – низкий риск. Для объектов, на которых вероятный преступник мало знаком с охранными системами. В частности, такое предположение характерно для объектов с незначительной стоимостью хранящегося там товара, без ценных в глазах преступников товаров (наркотики или алкоголь), и не несущие угрозы безопасности окружающих людей.

Класс 2 – риск средний низкий. Для объектов, на которых вероятный преступник предполагается с некоторым знанием охранных систем, но лишь с обычными инструментами широкого применения. Такое предположение характерно для объектов со средним объемом ценностей или незначительным объемом алкоголя. Класс 3 – риск средний высокий. Для объектов со значительным объемом ценностей, наркотическими веществами или объектов, представляющих угрозу для окружающих людей. Предполагаемый преступник оснащен всеми необходимыми инструментами и портативным электронным оборудованием.

Класс 4 – риск высокий. Для объектов с особо высоким объемом ценностей или с особо высоким уровнем риска для окружающего населения. Предполагаемый преступник считается тщательно подготовившимся, имеющим знания об охранной системе на этом объекте и имеющим образцы оборудования, аналогичного установленному на объекте.

Так вот в зависимости от важности объекта и предполагаемой подготовки преступника предъявляются особые требования к охранной сигнализации. Это вовсе не требования применять тот или иной датчик и даже не вполне требования к самим датчикам – в конце концов, какая разница, сколько метров дальность действия датчика, если охраняемая комната 2 х 2 м. Требования предъявляются в основном к системе реагирования на тревоги (для винных магазинов, например, обязательно выводить сигнализацию на круглосуточный пульт службы охраны). Кроме того, предъявляются требования по минимизации ложных тревог (ни одна служба охраны не будет всерьез охранять объект, на котором ложные тревоги три раза за ночь). Описываются способы снижения количества ложных тревог. Наконец, предъявляются требования к системе самодиагностики и информативности сообщений на пульт наблюдения. В этой части это и некоторые особые требования к датчикам. Например, для соответствия классу 3 датчики должны иметь не только выходы «тревога», «вскрытие» и «маскирован», но и выходной сигнал «неисправность».

С формальной точки зрения британские рекомендации сводятся к многочисленным «чеклистам», которые необходимо проконтролировать для соответствия объекта требованиям. Кроме того, для упрощения работы проектировщиков осуществляется сертификация всего оборудования на соответствие требованиям соответствующих классов, и на объекте класса 3, например, может использоваться только оборудование класса 3 или класса 4 – оборудование класса 2 заведомо не позволит выполнить

требования к системе по классу 3.
Тем не менее, по умолчанию предполагается, что после классификации объекта возможные угрозы для него «очевидны» и не стоят явного анализа.
Исключение – анализ задач для систем видеонаблюдения. Поскольку эти системы относительно дороги и не могут быть спроектированы на основе стандартного алгоритма (требуется творческий подход), для систем телевизионных предписывается провести анализ всех охраняемых зон и ясно указать, какова цель видеосистемы в той или иной зоне, какие действия какого нарушителя должны быть обнаружены и как и кто будет наблюдать изображение, чтобы этого достичь.

Анализ угроз в РД-78
Аналогом британских рекомендаций в нашей стране являются ведомственные Р (рекомендации) и РД (руководящие документы), выпускаемые НИЦ «Охрана» и другими организациями. Они также формально не являются обязательными даже для вневедомственной охраны. Тем не менее, за отсутствием иных документов (в некоторых крупных компаниях вроде «Газпрома» есть аналогичные внутренние документы) эти РД фактически обязательны для выполнения всеми создателями технических систем безопасности.
Что же они говорят о необходимости анализа угроз? На удивление мало. Например, один из основных документов – РД РД 78. 36.003-2002 «Технические средства охраны. требования и нормы проектирования по защите объектов от преступных посягательств». Во-первых, в нем вводится аналогичная классификация объектов на 4 группы – А1 (особо важные объекты высокой ценности или высокой опасности), А2 (собственно наиболее опасные помещения на этих объектах), Б1 (объекты розничной торговли и т. д.), Б2 (объекты категории Б, содержащие алкогольную продукцию или наиболее компактные легкосбываемые товары – электронику, товары повседневного спроса).
Для объектов группы Б1 (а фактически и для остальных) допускается создавать системы на основании акта обследования (а не полного проекта). Акт должен включать в себя классификацию объекта, перечисление защищаемых ценностей, их расположения на объекте, перечень уязвимых мест проникновения, однако подразумевается, что собственно угрозы для объекта автоматически вытекают из его классификации и их анализ может не проводиться. Следует отметить, что аналогично британским коллегам Р 78.36.002-99 «Выбор и применение телевизионных систем видеоконтроля» добавляет специфики. В частности, в нем вводится собственная классификация объектов на три группы: А (особо важные), Б (существенный ущерб) и В (прочие). Однако на классификации объекта анализ угроз заканчивается. Дальнейшее построение системы рекомендуется проводить на основе анализа архитектурно-планировочных решений, но необходимость собственно анализа возможных угроз уже явно не упоминается.

Проект техрегламента о противокриминальной безопасности
Как вы, наверное, знаете, уже несколько лет мы живем по новому закону о техрегулировании, согласно которому ГОСТы, как и любые стандарты предприятий или общественных организаций, сами по себе не являются обязательными. Обязательными являются лишь техрегламенты, которые принимаются только по основным вопросам безопасности. Например, экологической безопасности, безопасности дорожного движения и т. д. В области противокриминальной защиты также предполагается технический

регламент, в первую очередь описывающий классификацию объектов в зависимости от предполагаемых угроз, а затем уже рекомендующий разные уровни защиты в зависимости от уровня угрозы. Процитирую основные положения:
«В зависимости от степени потенциальной опасности, а также возможных последствий в случае реализации криминальных угроз объекты, их помещения и территории подразделяются на три основные группы:
– критически важные и потенциально опасные объекты;
– социально значимые объекты;
– объекты сосредоточения материальных ценностей.
Кроме того, в зависимости от вида и размеров ущерба, который может быть нанесен объекту, находящимся на нём людям и имуществу в случае реализации криминальных угроз все объекты подразделяются на следующие классы:
Класс I (высокая значимость) – ущерб в результате реализации криминальных угроз приобретет федеральный или межрегиональный масштаб;
Класс II (средняя значимость) – ущерб в результате реализации криминальных угроз приобретет региональный или межмуниципальный масштаб;
Класс III (низкая значимость) – ущерб в результате реализации криминальных угроз приобретет муниципальный или локальный масштаб; В зависимости от класса объекта и вида находящегося (хранящегося) на нем имущества устанавливают классы защиты объектов».
Далее в техрегламенте предлагается провести анализ потенциальных угроз и уязвимых мест объекта, и с учетом принципов адекватности потенциальным угрозам, зональности (многорубежности) и равнопрочности необходимо проектировать систему охраны. Звучит очень серьезно, в жизни, несомненно, в большинстве случаев проектировщик решит, что классификация объекта – это и есть анализ угроз. А после установления класса значимости и группы опасности объекта дальше надо лишь использовать рекомендованные для данного класса защиты виды оборудования.

Здравый смысл
Большинство систем среднего размера делаются не на основе РД и регламентов, а на основе здравого смысла. В ходе проектирования нередко здравый смысл отходит в сторону, и обсуждаются мелкие детали, но на начальном этапе, когда заказчик впервые задумался об установке системы охраны, он, конечно, задает себе вопрос: что и от кого должна охранять эта система и как, собственно, у нее получится охранять? Это и есть анализ угроз. К сожалению, как уже сказано, вскоре исполнитель начинает задавать конкретные вопросы: «где поставим датчики», «куда повесить сирену», а если еще и про видеокамеры заговорит, тогда уж вопросов так много, что главные, с которых все начиналось, как-то забываются и отходят на второй план. Чтобы этого не произошло, полезно перечислить на бумаге ответы на главные вопросы:
– что мы защищаем,
– от какого нападения защищаем (случайный хулиган, рецидивист-алкоголик или организованная группа),
– что должна сделать охранная система, чтобы помочь предотвратить (или хотя бы уменьшить) ущерб.
И в дальнейшем, обсуждая конкретные вопросы типа «где поставить датчик», надо просто регулярно возвращаться и проверять этот датчик: от какой угрозы он будет защищать, когда и как он должен сработать, почему такой, соответствует ли он вероятному противнику (преступнику). Регламенты, РД и ГОСТы пишутся весьма бюрократическим языком, но, если вникнуть в суть, она вполне соответствует здравому смыслу: отдавайте себе отчет, от чего вы намерены защитить объект, и применяйте адекватные угрозам средства. И применяйте их равнопрочно со всех сторон объекта (без явных дыр в защите). И постарайтесь защитить несколькими средствами (многими рубежами) самые важные помещения. И опять не забудьте про равнопрочность, – что толку в решетках на окнах,

если помещение отделено гипсокартонной перегородкой от соседней неохраняемой подсобки.
А описанные выше способы классификации объектов пусть помогут вам правильно оценить степень опасности и послужат отправной точкой для анализа.

Методика персонажей
При разработке сложных систем, особенно программного обеспечения, в последнее время популярна следующая методика, призванная наглядно представить себе, что требуется от системы: вы придумываете несколько конкретных персонажей-пользователей (например, для известного MicrosoftWord что-то типа «секретарша Леночка», «журналист Сергей», «завсектором учета бродячих собак Марья Ивановна»). И далее наглядно представляете себе, когда, зачем и как они будут пользоваться разрабатываемым вами программным продуктом.
При разработке системы безопасности вполне уместно применять тот же метод. Чтобы не шокировать апологетов ЕСКД персонажей, можно назвать условные модели преступников и обозначить легко запоминающимися словами, например, «Бомж», «плохой менеджер» (внутренний вор), «банда», «шпион (конкурентов)». И все разделы проекта системы безопасности сверять (хотя бы мысленно, чтобы не плодить бесконечные бумаги) с действиями предполагаемых основных персонажей. Главное – представить себе противника достаточно наглядно, вжиться в его роль, смоделировать его действия в конкретных ситуациях.
Только не забудьте вернуть вещи, украденные вами, пока вы вживались в роль преступника.