ПРИМЕНЕНИЕ РИСК-ИНФОРМИРОВАННОГО ПОДХОДА В РАБОТЕ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ

ESTIMATE OF THE EFFICIENCY OF PHYSICAL PROTECTION SYSTEMS. FINDING OF THE MOST DANGEROUS SCENARIOS OF THE ATTACK ON PPS

A. Oboymov

Summary. The article considers the possibility of using of the paradigm of risk-informed analysis of the vulnerabilities of potentially dangerous objects to criminal-terrorist threats in the work of the physical protection system. The possibility of using the results of risk-informed analysis of vulnerabilities to assist personnel in detecting and preventing attacks on PPS is considered. The developed prototype of the software demonstrating the principle of operation of the risk-informed physical protection system in the example of one room is described.

Keywords: physical security system, risk-informed approach, probabilistic safety analysis, performance analysis, vulnerability analysis, modeling of attacks' scenarios.

Обоймов Антон Сергеевич
Аспирант, Московский Физико-Технический Институт (государственный университет), Московская область, г. Долгопрудный
anton.oboimov@gmail.com

Аннотация. В статье рассматривается возможность использования парадигмы риск-информированного анализа уязвимостей потенциально-опасных объектов к криминально-террористическим угрозам в работе системы физической защиты объекта. Рассматривается возможность использования результатов риск-информированного анализа уязвимостей для помощи персоналу в обнаружении и предотвращении атак на СФЗ. Описывается разработанный прототип программного обеспечения, демонстрирующий принцип работы риск-информированной системы физической защиты на примере одного помещения.

Ключевые слова: система физической защиты, риск-информированный подход, вероятностный анализ безопасности, анализ эффективности, анализ уязвимостей, моделирование сценариев атак.

Риск-информированный подход

В концептуальной модели (парадигме) риск-информированного анализа уязвимостей потенциально-опасных объектов к криминально-террористическим угрозам ключевые понятия — риск (R), угрозы (T), последствия (C) и уязвимости (V) — соотносятся между собой следующим образом (рис. 1).

Как указано на Рис., риск (ожидаемый ущерб) от диверсионного акта на данный потенциально-опасных объект определяется логическим пересечением последствий диверсии, вероятности угрозы и уязвимостями рассматриваемого объекта к угрозам.

$$R = C \times V \times T \quad (1)$$

На данной схеме показано, что риск возникает только в области пересечения трех факторов — угрозы, уязвимости и последствий — и не существует без них. Другими словами, риск отсутствует (равен нулю) если

1) при существующей угрозе для неуязвимого объекта ($V \to 0$),

2) для уязвимого объекта при отсутствии угрозы ($T \to 0$),

3) для незначительных последствий ($C \to 0$) при существующей угрозе уязвимого объекта.

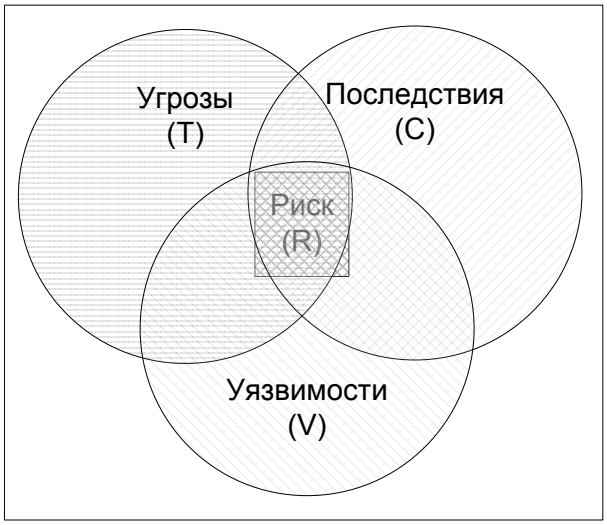

Рис. 1. Связь между понятиями риск, угрозы, последствия, уязвимости

Анализ рисков как один из основных методологических инструментов обеспечения безопасности ядерно-опасных объектов (ЯОО) применяется в атомной отрасли с конца 1970-х годов [1].

Основной результат анализа рисков — это ответ на три основных практических вопроса:

- «Что может происходить неправильно?» — анализ репрезентативных сценариев;
- «Какова вероятность сценария?» — анализ вероятности;
- «Каковы последствия сценария?» — анализ последствий

(определение так называемого «триплета риска» [2]).

Ответ на первый вопрос обычно имеет форму «сценария» (комбинации событий и/или условий при которых реализуются неблагоприятные последствия) или семейства «сценариев».

Ответ на второй вопрос, обычно, получают, используя имеющиеся доказательства, способные помочь количественно описать вероятность неблагоприятных последствий и неопределенности, связанные с ней. В некоторых ситуациях, могут быть эмпирические данные о частоте сходных событий в прошлом (например, о переоблучении персонала или числе криминальных инцидентов). В ситуациях, когда данных мало или они отсутствуют (например, частота повреждения первого контура АЭС) для оценки вероятности и неопределенностей используют предсказательное моделирование.

Ответ на третий вопрос получают для каждого из выбранных (на первом шаге) сценариев путем оценки диапазона ущерба при заданных неопределенностях данных и моделей. Результатом являются «конечными» точками анализа.

Таким образом, в риск-информированной парадигме, основанной на «вероятностном» подходе (в виде ВАБ или других методов оценки риска) рассматривается риск (т.е. все три вопроса триплета) в согласованной, явной и количественной форме.

Подробно методика анализа СФЗ с использованием риск-информированного подхода изложена в работе [3].

Риск-информированная СФЗ

В рамках данной работы был разработан прототип риск-информированной системы безопасности, работающий по принципам, описанным выше.

В качестве основной системы, поставляющей информацию для обработки, была выбрана система видеонаблюдения. Современная видеоаналитика обладает возможностями, включающими распознание людей, трекинг (слежение) за людьми, в том числе и в многокамерных системах, распознание выделяющегося, подозрительного поведения, например, бег, праздношатание и многое другое [4].

Однако, эти возможности во многом используются вхолостую, максимум, включая запись по обнаружению движущихся объектов и сигнализируя об этом оператору. Вся тяжесть дальнейшего анализа и принятия решений ложится исключительно на оператора. Однако, эффективность работы оператора сильно зависит от времени суток, общей нагрузки, и многих других факторов и является недостаточной для многих случаев. А во-вторых, как показывает практика, часто операторы игнорируют происходящее на видеокамерах по привычке, например, после нескольких ложных срабатываний или после длительного периода отсутствия каких-либо попыток нарушить безопасность охраняемого объекта [5].

Значительно облегчить работу персонала СФЗ, а также повысить эффективность всей системы безопасности возможно, если использовать результаты риск-информированного анализа уязвимости и эффективности СФЗ непосредственно в работе системы. На этапе проведения анализа эффективности СФЗ объекта, с использованием инструментов риск-информированного подхода, были описаны принципиально возможные нарушители, тактики и сценарии их действий, смоделированы как сценарии вторжения, так и сценарии контрдействий по нейтрализации нарушителя.

Задача удержания в памяти всех инструкций на все случаи действий нападающих, и, что важнее — задача своевременного обнаружения и распознания несанкционированных, враждебных действий — эти задачи очень сложны для операторов и дежурных службы безопасности любого крупного объекта. Эту задачу можно существенно упростить, если обеспечить информационное сопровождение оператору, выдачей точных данных о текущем состоянии дел, помощью в обнаружении возможных нападений на ранней стадии, выдачей четких инструкций, что делать в том или ином случае.

Разработан прототип, показывающий принцип работы всей системы на примере одного помещения в здании.

Для демонстрации принципа работы всей системы рассматривается одно помещение — коридор, на рисунках 2–4 показаны скриншоты работающей программы. Вход в помещение охраняется сотрудником службы безопасности объекта, кроме того, вход помещение блокируется замком, например кодовым. В помещении предполагается наличие некой «запретной» зоны, в которой находится какой-либо предмет физической защиты — цель нарушителя. Камера отслеживает происходящее в помещении в автоматическом режиме, без участия оператора. Данные с видеокамеры обрабатываются программой. В случае появления кого-либо в помещении, программа начинает трекинг обнаруженных людей,

Рис. 2. Окно программы. Помещение (картинка с видеокамеры в реальном времени), «запретная» зона в помещении, дерево событий (сверху) и дерево отказов (снизу)

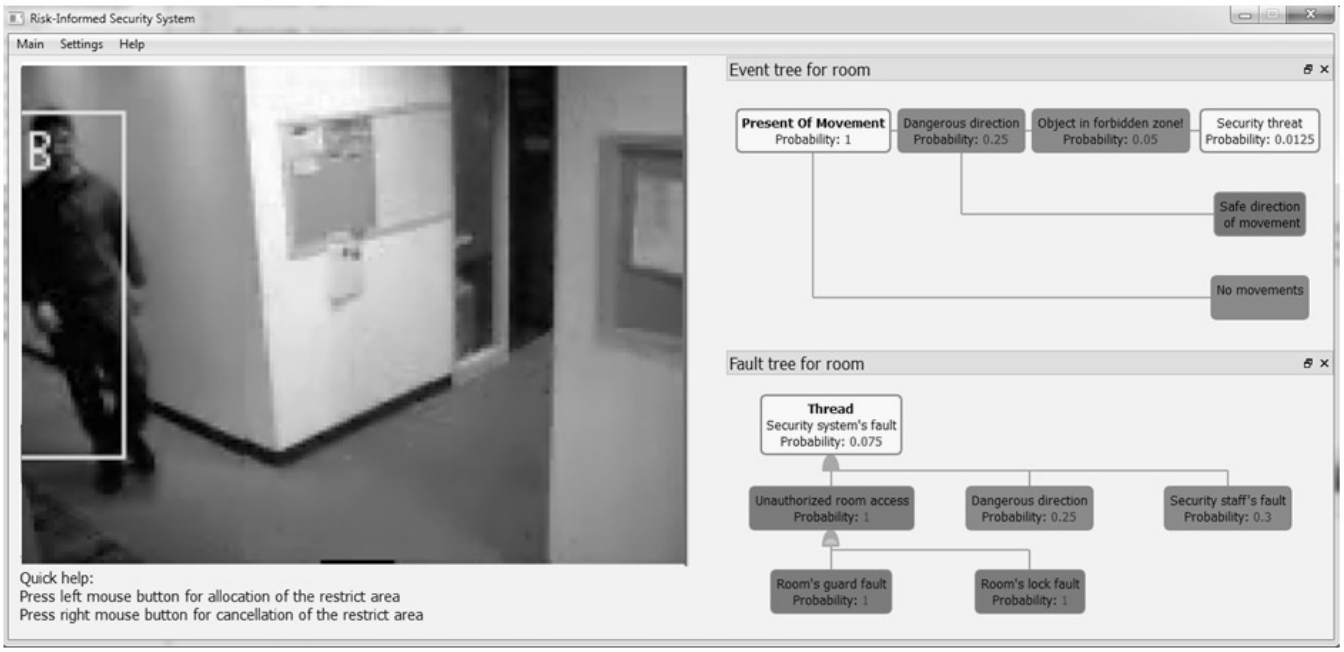

Рис. 3. Обнаружен нарушитель, движущийся в направлении к запретной зоне

отслеживая все их действия и перемещения, одновременно анализируя их.

Для помещения построены дерево событий и дерево отказов, соответствующие проникновению нарушителя в запретную зону. Заданы начальные вероятности событий и отказов. Вероятности возможных итоговых событий и отказов вычисляются в соответствии с логическими операциями, гейтам дерева.

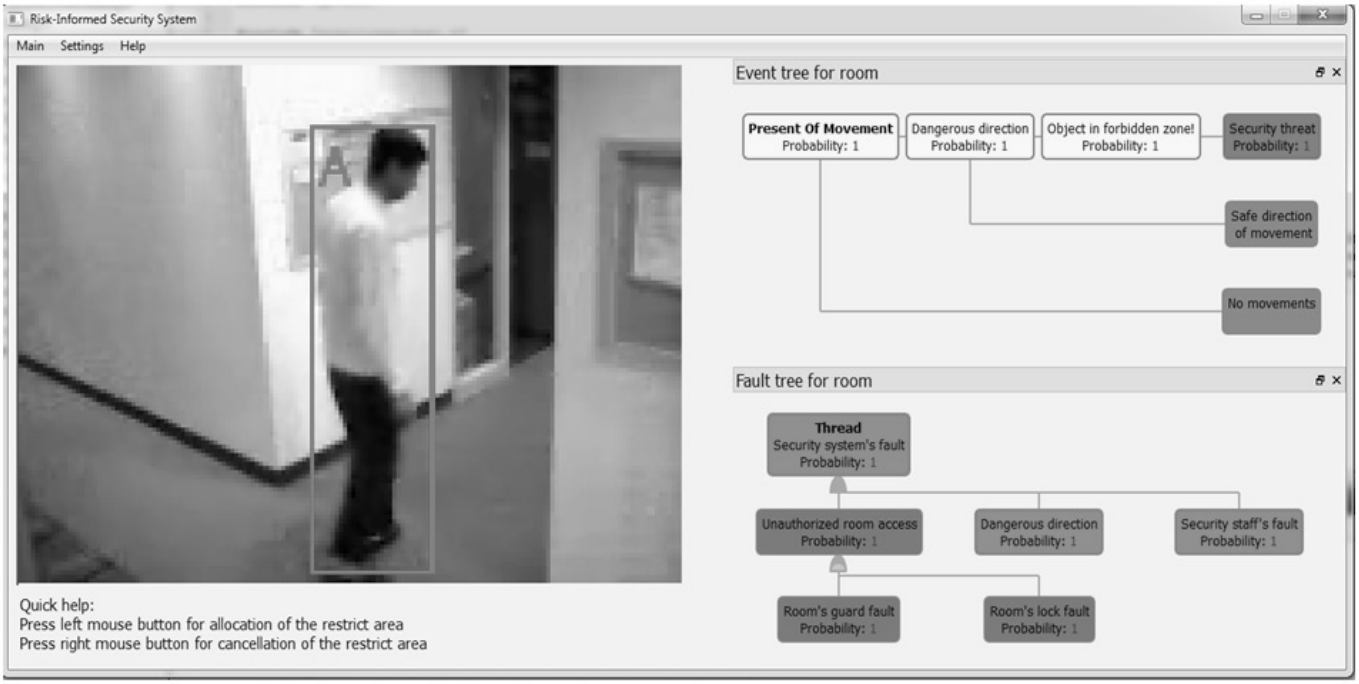

Рис. 4. Нарушитель проник в запретную зону. Отказ СФЗ

Если обнаруживается какое-либо из событий, внесенное в дерево событий, программа автоматически отмечает событие как произошедшее (его вероятность становится равной единице), пересчитывает всё дерево и сигнализирует о повышении уровня риска (а значит, и повышение уровня угрозы безопасности), если таковое обнаруживается.

Все обнаруженные события, а также соответствующие им отказы регистрируются в системе, что позволит впоследствии, при необходимости, проследить развитие событий, проанализировать действия нарушителя и персонала СФЗ, выработать предложения по улучшению СФЗ и повышению эффективности.

Дерево событий в данной программе отображает следующие ключевые события:

- Наличие движения. Камера зафиксировала наличие движения в помещении. В первую очередь, это означает, что обнаруженный злоумышленник каким-то образом попал в помещение, а значит, произошел отказ замка на двери или отказ охранника на входе в помещение (либо охранник нейтрализован, либо он в сговоре с нарушителем).
- Движение к запретной зоне. Наличие движущегося к опасной зоне человека ещё не означает автоматически, что он движется именно в сторону «запретной зоны», однако, если движение направлено именно в эту сторону — это ещё больше повышает риск.

Проникновение в запретную зону. Пока потенциальный нарушитель ещё не проник в зону, есть вероятность, что он туда и не проникнет: не успеет и его задержит группа реагирования, или он вообще пройдет мимо, или вдруг развернется и уйдет, например, если поймет, что его сейчас поймают и надо уходить. Однако, если он проник в эту зону, это автоматически означает провал группы реагирования, которая не успела или не смогла по каким-либо причинам задержать злоумышленника, отказ замка или какой-либо системы контроля доступа в «запретную» зону, если такая имеется, ну а также отказ всей системы защиты, которая допустила проникновение нарушителя в запретную зону.

Дерево событий выполняет функции:

- Показывает текущие распознанные события, так или иначе влияющие на уровень безопасности и риска и способные привести к негативному исходу;
- Показывает дальнейшие возможные пути и сценарии развития событий в явном виде на мониторе оператора;
- Выдает численную оценку вероятности исхода тех или иных событий.

Дерево отказов в данном случае выполняет следующие функции:

- показывает, отказ каких именно элементов привёл к тому, что нарушитель оказался в том или ином месте, преодолел тот или иной рубеж безопасности;

- показывает влияние произошедшего отказа на всю систему в целом, в явном виде показывает последствия, как возможные, так и произошедшие. Дело в том, что современные системы защиты строились на принципе единичного отказа — предполагалось, что при отказе одного из компонентов системы вся система способна обеспечить требуемый уровень защищенности. Однако, это далеко не всегда так, в сложных системах отказ одних элементов может явно или неявно влиять на работу других, повышая вероятность их отказа, а значит, и текущий уровень риска. Данная программа явно это показывает на мониторе оператора, выдавая звуковое оповещение;
- при наличии соответствующих инструкций, выдает предупреждение о необходимости включить резервные элементы СФЗ, отправить группу реагирования для проверки ситуации и, при необходимости, задержания нарушителя, предсказывает возможные отказы элементов, зависящих как либо от уже отказавших и т.д.

Работа с видеопотоком реализована с помощью открытой библиотеки компьютерного зрения OpenCV. Программа выделяет на неподвижном фоне движущиеся объекты, и осуществляет их трекинг (слежение за объектом). Кроме того, программа работает как детектор движения, на случай, если объект как-то маскируется, и явно его выделить не получается. В этом случае, осуществляется слежение за движущимися частями.

Дальнейшая разработка данного программного продукта и его интеграция в существующие системы физической защиты предполагает подключение к программе, как минимум, следующих функций:

- подключение к системе обработки информации с других элементов КТСФЗ: датчиков движения, инфракрасных датчиков, других сигнальных элементов.
- интеграция с системой контроля и управления доступом — в том числе, для отслеживания действий персонала объекта и выявления внутреннего нарушителя, использующего свои полномочия для нарушения работы объекта;

Данная программа также позволяет с высокой степенью надежности (выше, чем у оператора-человека) оценивать масштаб вторжения.

ЛИТЕРАТУРА

1. Rasmussen, N. Reactor safety study. An assessment of accident risks in U. S. commercial nuclear power plants, WASH-1400 (NUREG-75/014). Rockville, MD, USA: Federal Government of the United States, U. S. Nuclear Regulatory Commission. Retrieved 2009–10–31.
2. Kaplan S., Garrick, B. J. On the Quantitative Definition of Risk, Risk Analysis, 1981, v.1, n.1, 11–27
3. Обоймов, А. С. Риск-информированный анализ уязвимостей ядерно-опасных объектов // MEDIAS-2012: труды Международной научной конференции.— Протвино-Москва: Изд. ИФТИ, 2012, С. 43–56.
4. Птицын Н. Тенденции применения видеоанализа при создании систем защиты периметра. Анализ наиболее востребованных функций. // Алгоритм безопасности № 1, 2012 г.
5. Обоймов А. С. Анализ эффективности систем физической защиты: моделирование сценариев, влияющих на целостность СФЗ / А. С. Обоймов // СРТ2013: труды Международной научной конференции.— Протвино-Москва: Изд. ИФТИ, 2013 — С. 203–220.

© Обоймов Антон Сергеевич (anton.oboimov@gmail.com). Журнал «Современная наука: актуальные проблемы теории и практики»

Московский Физико-Технический Институт