ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ МОДЕЛИРОВАНИЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ

Дашкевич А. А., Кузьмицкий А. М.
Кафедра специальных и инженерно-технических дисциплин учреждения образования «Военная академия Республики Беларусь»
Минск, Республика Беларусь
E-mail: AndreiDashkevich@gmail.com

В статье излагаются аспекты моделирования эффективности системы физической защиты объектов использования атомной энергии, проводится обзор программномного обеспечения которое может быть применено на Белорусской АЭС.

Автоматизация процесса оценки эффективности системы физической защиты (СФЗ), как проекта, так и существующей системы позволяет уменьшить объемы работы аналитика и свести к минимуму вероятность возможных ошибок. Конечным результатом анализа должна являться количественная характеристика эффективности имеющая, вероятностную природу – это уязвимость. Такой анализ в случае его проведения должен не только дать количественную оценку уязвимости, но помочь выявить в случае необходимости все слабые места системы защиты. В сущности, простейшая задача оценки уязвимости является задачей вероятностного анализа и может быть решена известными способами [1]. Общее время задержки *Tmin.* рассчитывается по формуле:

$$T_{min} = \sum_{i=k}^{m} Ti > Tg \qquad (1)$$

где m – общее число элементов системы защиты по маршруту нарушителя; k – точка, где $Tmin$ начинает превышать Tg; Tg – время выдвижения резервной группы караула. Суммарная вероятность обнаружения определяется следующим образом:

$$P_I = \prod_{i=k}^{k-1} (1 - P_i) \qquad (2)$$

где k – точка, где $Tmin$ начинает превышать Tg; i – элемент обнаружения; Pi – вероятность обнаружения датчика обнаружения; $(1 - Pi)$ – вероятность необнаружения.

Старейшим программным продуктом, применяемым для этих целей является EASI *(Estimate of Adversary Sequence Interruption)* – простой и удобный в использовании метод оценки эффективности СФЗ на заданном маршруте при определенных угрозах и состояниях самой СФЗ. В модели используются значения параметров обнаружения, задержки, развертывания сил реагирования и установления связи, с помощью которых рассчитывается результат – вероятность перехвата на данном маршруте. Исходные данные модели EASI: значение Pi для каждого датчика на маршруте; вероятности установления связи с охраной; значение времени задержки для каждого Ti и среднее квадратическое отклонение для каждого из этих значений; значение времени развертывания сил реагирования Tg и среднее квадратическое отклонение для этого значения. Результатами расчета по заданным исходным данным и схеме, являются значения вероятности перехвата или вероятности прерывания последовательности действий диверсантов до совершения ими несанкционированных действий. Другой инструмент – расчет времени задержки, а затем выставление вероятностей. Модель EASI может использоваться для анализа уязвимость объекта, но она не позволяет анализировать вероятность нейтрализации нарушителей.

В России ГУП «Элерон», разработана компьютерная модель «Вега», позволяющая оценивать уязвимость СФЗ объекта используя методику цепей Маркова. В основу модели положен анализ по принципу «событие-время».При оценке рассматриваются все возможные сценарии действий нарушителя. Под сценарием действий рассматривается последовательность преодоления правонарушителем физических барьеров (далее – ФБ), а также способ их преодоления. Каждый способ характеризуется вероятностью обнаружения во время преодоления и после преодоления. Комплекс предназначен для оценки эффективности СФЗ стационарных объектов [2]. Программный комплекс, объединяет в себе ряд программ-модулей: модуль описания объекта; расчетный модуль; модуль формирования отчета; автоматизированные базы данных по средствам обнаружения, физическим барьерам, моделям нарушителей. Файл описания объекта программы «Вега» описывает все цели нарушителя, находящиеся на объекте. Описание структуры и состава СФЗ объекта осуществляется при помощи «зон», «секций» и «переходов». Программа имеет базы данных по физическим барьерам и средствам обнаружения (далее – СО), при необходимости есть возможность удалять и добавлять новые ФБ и СО. Также пользователь имеет возможность самостоятельно изменять па-

раметры, заложенные в базу данных. После завершения описания объекта хотя бы одной цели проводится оценка эффективности СФЗ с использованием опции«расчетный модуль». После задания модели нарушителя проводятсяк расчеты. Модуль рассчитывает оценку СФЗ для конкретной цели нарушителя, группы целей, объекта в целом.

Результатом оценки эффективности является вероятность пресечения нарушителя силами реагирования, рассчитанная для наихудшей, с точки зрения охраны, ситуации. При этом, расчетный модуль отражает критический маршрут нарушителя, которому соответствует оценка. Отличительной особенностью программы является оценка эффективности при внутренней угрозе, где оценивается: вероятность обнаружения внутреннего нарушителя при попытке вноса им запрещенных предметов, используя каналы легального прохода; вероятность пресечения силовых действий внутреннего нарушителя, в зависимости от его оснащения; итоговый показатель эффективности при внутренней угрозе для каждого типа нарушителя с учетом комбинации скрытных и силовых действий.

Программный комплекс «Полигон» предназначен для моделирования локальных боевых столкновений в системе «охрана-нарушитель» при перевозках специальных грузов. Она позволяет моделировать боестолкновения малых подразделений и групп с учетом видов и характеристик транспортных средств, численности, вооружения и тактики действий противоборствующих сторон, природных условий (рельеф местности, растительность и т.п.). При проведении моделирования каждая из сторон имеет свой компьютер, на экране отображается только та информация, которая доступна данной стороне. Имеется также компьютер администратора (посредника). Компьютеры объединены в локальную сеть. Все рутинные операции автоматизированы. Моделирование проводится в пошаговом режиме. Сторона, которой предоставлен ход, в течение отведенного времени принимает решение о своих действиях (движение транспортных средств, личного состава, ведение огня). Сеанс моделирования оканчивается победой одной из сторон. Сеансы проводятся многократно, что позволяет выявить тенденцию в победе той или иной стороны. Если преимущественно побеждают нападающие, то далее определяется важный параметр – время боя, к которому затем добавляется время преодоления нарушителем ФБ и время других действий нарушителя, необходимых для захвата ядерных материалов. Сравнение этого суммарного времени со временем прибытия сил реагирования позволяет сделать вывод об эффективности физической защиты. В программе используются достоверные исходные данные по стрелковому оружию и ФБ. Особенности ПО «Полигон»: применение вероятностной модели ведения огня из различных типов стрелкового оружия с учетом характеристик стрелка, цели местности; полная автоматизация процессов определения взаимной видимости и возможностей перемещения боевых единиц (автотранспорта, людей); ведение протоколов моделирования, позволяющих производить ретроспективный просмотр боестолкновения; наличие 3D - редактора местности; открытая архитектура ПО «Полигон», позволяющая вносить в программу необходимые изменения.

Выводы:

1. Представленный обзор предопределяет два возможных направления деятельности специалистов, участвующими в обеспечении комплексной безопасности функционирования Белорусской АЭС.

Во-первых – изучение, выбор и использование наиболее оптимального из представленных программных продуктов в практической деятельности по оценке уязвимости СФЗ.

Во-вторых – разработка отечественных алгоритмов и программ системного анализа и оценки эффективности системы физической защиты.

2. Наиболее приемлемыми программные продуктыдля использования в служебно-боевой деятельности внутренних войск МВД Республики Беларусь являются компьютерная модель анализа уязвимости «Вега», программные комплексы «Спрут», «Полигон».

1. СТБ 34.101.30-2007. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация. Нац. Интернет-портал Респ. Беларусь [Электронный ресурс] / Нац. фонд технических нормативных актов Респ. Беларусь. – Минск, 2015. – Режим доступа: http://www.tnpa.by/KartochkaDoc.php. – Дата доступа: 25.05.2017.
2. Рук. документ Гостехкомиссии Российской Федерации «Защита от несанкционированного доступа к информации. Термины и определения». Режим доступа: http://www.iso27000.ru/zakonodatelstvo/normativnye-dokumenty-fstek-rossii/rukovodyaschii-dokument. – Дата доступа: 25.05.2017
3. Голиков, В.Ф. Безопасность информации и надежность компьютерных систем: пособ. для студентов специальностей 1-40-1 01 01 и 1-53 01 02 в 2 ч / В.Ф.Голиков. – Минск, БНТУ, 2010. ч.1. – 86с.
4. Погожин, Н.С. Физическая защита ядерных объектов. Учебник для высших учебных заведений / П.В.Бондарев, А.В.Измайлов, А.И.Толстой; под ред. Н.С.Погожина. – М.: МИФИ, 2004. – 459 с.
5. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Национальный Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. фонд технических нормативных актов Респ. Беларусь. – Минск, 2015. Режим доступа: http://www.tnpa.by/KartochkaDoc.php. – Дата доступа: 25.05.2017.