

УДК 623.094

Метод оценки защищенности критически важных объектов информационной инфраструктуры

Казаков Геннадий Викторович

kgv.64@mail.ru

Котяшев Николай Николаевич

knn1941@gmail.com

Мочалов Виктор Васильевич^(*)

mvvd@mail.ru

ФГБУ «4 ЦНИИ» Минобороны России, Королев, Московская обл., Россия

Аннотация. При рассмотрении безопасности объектов факторы риска необходимо перевести в сферу угроз, что позволит получить их описание, определяющее наиболее эффективный способ реализации механизмов защиты в соответствии с требованиями безопасности. С этой целью разработаны модели угроз и защиты, а также подход, связанный с комплексным описанием угрозы и средств защиты от ее воздействия. Рассмотрен метод расчета показателя безопасности критически важных объектов информационной инфраструктуры с использованием метода анализа иерархий.

Ключевые слова: защищаемый актив, конкатенация, логическая композиция, логическое объединение, модель защиты, модель угроз, средство защиты

Введение. При рассмотрении безопасности критически важных объектов информационной инфраструктуры (КВО ИИ) необходимо перевести некоторые факторы риска в сферу угроз безопасности КВО ИИ. В этом случае получается более конструктивное их описание, позволяющее определить наиболее эффективный способ реализации механизмов защиты в соответствии с требованиями безопасности КВО ИИ. С этой целью разрабатывается модель угроз и связанная с ней модель защиты.

Материалы и методы; результаты. При разработке этих моделей необходимо руководствоваться определенными принципами, которые позволяли бы охватывать все основные процедуры реализации угрозы и были бы присущи всем угрозам, независимо от их конкретного вида. С формальной точки зрения совокупность моделей угроз и защиты описывается в виде плоского графа [1].

Для формального описания общей модели «угроза-защита» необходимо использовать некоторые действия над графами [2, 3]. При формальном описании модели «угроза-защита» необходимо руководствоваться новыми понятиями операций над графами: логическая композиция ($\oplus$), конкатенация ($\mapsto$) и логическое объединение графов ($\perp$).

Задача проектирования КВО ИИ заключается в построении такой системы, которая обеспечивала бы требуемое качество КВО ИИ в условиях воздействия факторов риска. При этом комплекс средств защиты должен проектироваться в соответствии с моделью защиты для установленного актуального состава преднамеренных угроз и установленных видов характеристик безопасности.

Модель защиты, также как и модель угроз, позволяет получить определенные исходные данные для оценки остаточного риска для КВО ИИ, как комплексного показателя, определяющего эффективность применяемых мер и средств обеспечения безопасности КВО ИИ.

Для определения структуры свойства безопасности КВО ИИ целесообразно применять метод анализа иерархий [4]. Суть метода заключается в разработке такой иерархии, которая определяла бы атомарные свойства, входящие в состав комплексного свойства безопасности КВО ИИ. Полученная таким образом иерархия позволит получить замкнутые алгоритмы расчета показателя безопасности КВО ИИ.

Если такая иерархия построена, то из опыта эксплуатации КВО ИИ можно установить числовые значения простейших свойств безопасности и, используя метод анализа иерархий, получить числовое значение показателя безопасности КВО ИИ.

Заключение. Таким образом, разработаны модель угроз и модель защиты, а также приведен алгоритм расчета числовой оценки показателя безопасности КВО ИИ.

Список источников

- [1] Скопенков А.Б. Вокруг критерия Куратовского планарности графов. *Математическое просвещение*, 2005, сер. 3, вып. 9, с. 116–128.
- [2] Харари Ф. *Теория графов*. Москва, Ленанд, 2018, 304 с.
- [3] Лодкин А.А., Манаев И.Е., Минабутдинов А.Р. Реализация автоморфизма Паскаля в графе конкатенаций и функция $s_2(n)$. *Зап. научн. сем. ПОМИ*, 2012, т. 403, с. 95–102.
- [4] Саати Т.Л. *Принятие решений. Метод анализа иерархий*. Москва, Радио и связь, 1993, 312 с.