Классификатор угроз на основе синергетического подход

УДК 04.056:004.738.5

Сергей Евсеев[1], Ольга Король[2]

Харьковский национальный экономический университет им. С. Кузнеца,
[1]Serhii.Yevseiev@hneu.net, [2]Olha.Korol@hneu.net

Основной задачей исследований в области безопасности автоматизированных банковских систем (АБС) является разработка новых и усовершенствование имеющихся методов оценки уязвимости (рисков), нанесения ущерба АБС в целом или отдельным ее составляющим компонентам. Одной из задач мероприятий по защите банковской информации (БИн) является построение системы защиты, направленной на противодействие угрозам безопасности. Как правило система защиты строится с учетом моделей нарушителя и модели угроз.

Целью данной работы является разработка классификатора для моделей нарушителя и угроз на основе синергетического подхода оценки рисков.

Для построения метрик угроз на основе синергетического подхода воспользуемся подходом построения классификатора угроз на основе информационно-аналитической модели метода двойных троек, впервые предложенного Юдиным А.К. В отличие от известного при построении классификатора содержательная часть каждой из четырех платформ включает в себя соответственно:

первая платформа – классификация угроз по отношению к составным обеспечения безопасности БИн в АБС ОБС: информационная безопасность (ИБ) (01), безопасность информации (БИ) (02), кибербезопасность (КБр) (03). При этом введем следующие определения:

Безопасность банковской информации (Б БИн) – состояние защищенности банковской информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность аутентичность и доступность БИн при ее обработке в АБС.

Информационная безопасность банковской информации (ИБ БИн) – состояние защищенности информационной среды ОБС, обеспечивающее ее формирование, использование и развитие в интересах граждан и ОБС.

Кибербезопасность банковской информации (КБрБ БИн) – набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды АБС, ресурсов и пользователей ОБС;

вторая платформа – классификация угроз по характеру направлений: нормативно-правовое (01), организационное (02), инженерно-техническое (03);

третья платформа – классификация угроз в соответствии с основными особенностями информации: конфиденциальность (01), целостность (02), доступность (03), аутентичность (04);

четвертая платформа – классификация угроз по уровням иерархии инфраструктуры АБС: FL – физический уровень (01), NL – сетевой уровень (02), OSL – уровень операционных систем (ОС) (03), DBL – уровень систем

управления базами данных (04), BL – уровень банковских технологических приложений и сервисов (05).

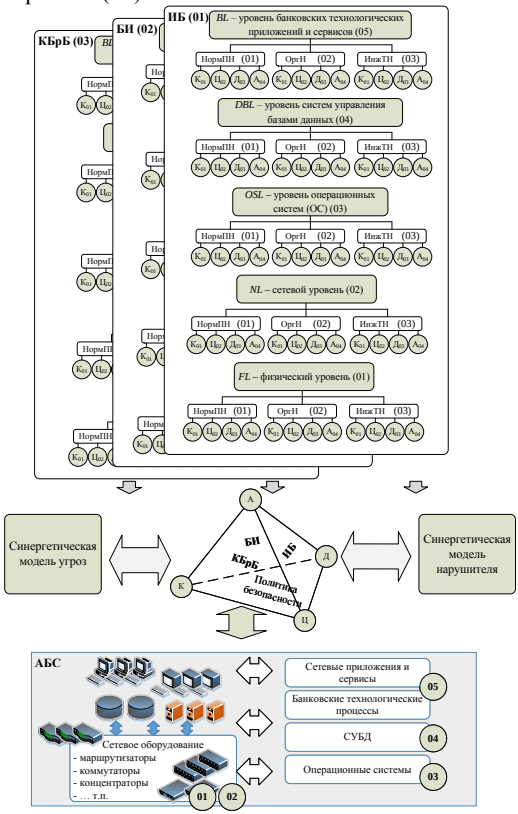

Рис.1. Взаимосвязь структурной схемы классификатора угроз с АБС ОБС

Описание модифицированного классификатора угроз состоит из четырех числовых величин: – составная обеспечения безопасности БИн в АБС ОБС: информационная безопасность (ИБ) (01), безопасность информации (БИ) (02), кибербезопасность (КБр) (03); – характер направлений: нормативно-правовое (01), организационное (02), инженерно-техническое (03); – основные особенности информации: конфиденциальность (01), целостность (02), доступность (03), аутентичность (04); – уровни иерархии инфраструктуры АБС: FL – физический уровень (01), NL – сетевой уровень (02), OSL – уровень операционных систем (ОС) (03), DBL – уровень систем управления базами данных (04), BL – уровень банковских технологических приложений и сервисов (05). Представленная классификация позволяет сформировать соответствующие метрики угроз и превентивных защитных мер.