ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

А.А. Бабенко

ЭКСПЕРТНЫЙ МЕТОД ОПРЕДЕЛЕНИЯ СОСТАВА СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

(Волгоградский государственный университет)

Государственные информационные системы (ГИС) используются в Федеральных органах исполнительной власти, Министерствах РФ и иных структурах. В результате анализа существующих ГИС установлено, что они имеют сложный состав, включающий информационные системы персональных данных и системы общего пользования. Выделяют следующие классы ГИС:

1) по масштабу (федеральные, региональные, объектовые);

2) по степени конфиденциальности обрабатываемой информации;

3) по отношению к сетям международного информационного обмена (без доступа к сетям международного информационного обмена и взаимодействующие с сетями международного информационного обмена).

ГИС позволяют решать задачи: автоматизированного управления; осуществление непрерывного обмена информацией; сбор, анализ и визуализация оперативных данных; мониторинг различных отраслей.

Требования нормативно правовых актов обязывают операторов ГИС обеспечить: предотвращение хищения и утечки информации, снижение ущербов, прогнозирование рисков информационной безопасности, отказоустойчивое функционирование программно-технического обеспечения ГИС [1, 2].

Согласно Приказу ФСТЭК России от 11 февраля 2013 г. N 17 к объекту защиты в ГИС относятся содержащаяся в них информация, технические средства, программное обеспечение, информационные технологии и средства защиты информации.

Анализ угроз безопасности информации ГИС позволил выявить наиболее актуальные:

1. Перехват ценных сведений по используемым линиям связи;
2. Кража данных;
3. Искажение и подмена данных;
4. Уничтожение данных и программного обеспечения.

Злоумышленников интересуют персональные данные, государственная тайна, конфиденциальная и платёжная информация. Следовательно, проектируемая система защиты информации (СЗИ) должна быть направлена на предотвращение хищения и утечки информации, обрабатываемой в ГИС [3, 4].

Так как к внедрению в СЗИ ГИС регуляторами разрешены сертифицированные средства защиты, обеспечивающие защиту от угроз ГИС, разработана процедура анализа средств технической защиты информации, состоящая из шагов:

1. Выявление требований к классу средств защиты информации в результате анализа нормативно-правовых актов;

2. Определение класса и области применения средств защиты информации;

3. Определение соответствия класса защиты ГИС и средств защиты информации.

Разработанная процедура анализа средств технической защиты (СТЗ) информации в ГИС позволяет определить соответствие классов защищенности ГИС и классов защиты используемых средств защиты ГИС.

Состав СЗИ в ГИС зависит от эффективности используемых средств защиты. Критерий оценки технических средств защиты информации в ГИС представлены в таблице 1.

Таблица 1. Критерии оценки технических средств защиты информации в ГИС.

Название	Возможные значения критерия
Продолжительность действия сертификата регуляторов	Большой, средний и маленький
Многофункциональность	Да, нет
Уровень контроля на отсутствие недекларированных возможностей	Да, нет
Цена средства защиты информации	Высокая, низкая
Количество перекрываемых угроз	N
Величина предотвращенного риска	N

В результате анализа методов определения состава системы технической защиты ГИС выявлены:

1. Метод точечных решений, предполагающий решение возникающих проблем;

2. Метод на основе обработки статистических данных, требующий точные статистические данные об угрозах и, как правило, привлечения для их получения сторонних организаций;

3. Экспертный методы, предполагающий создание экспертной группы из сотрудников ГИС без привлечения сторонних специалистов.

В результате их сравнения установлено, что особую роль в определении состава СТЗ информации в ГИС приобретают экспертные методы (таблица 2).

Таблица № 2. Анализ методов определения состава СТЗ информации в ГИС

Метод	Критерии		
	Прогнозирование угроз	Стоимость	Эффективность решения задач ИБ
Точечных решений	Нет	Высокая	Низкая
На основе обработки статистических данных	Да	Высокая	Средняя
Экспертный	Да	Средняя	Высокая

Определение состава СТЗ информации в ГИС состоит из этапов, представленных на рисунке 1

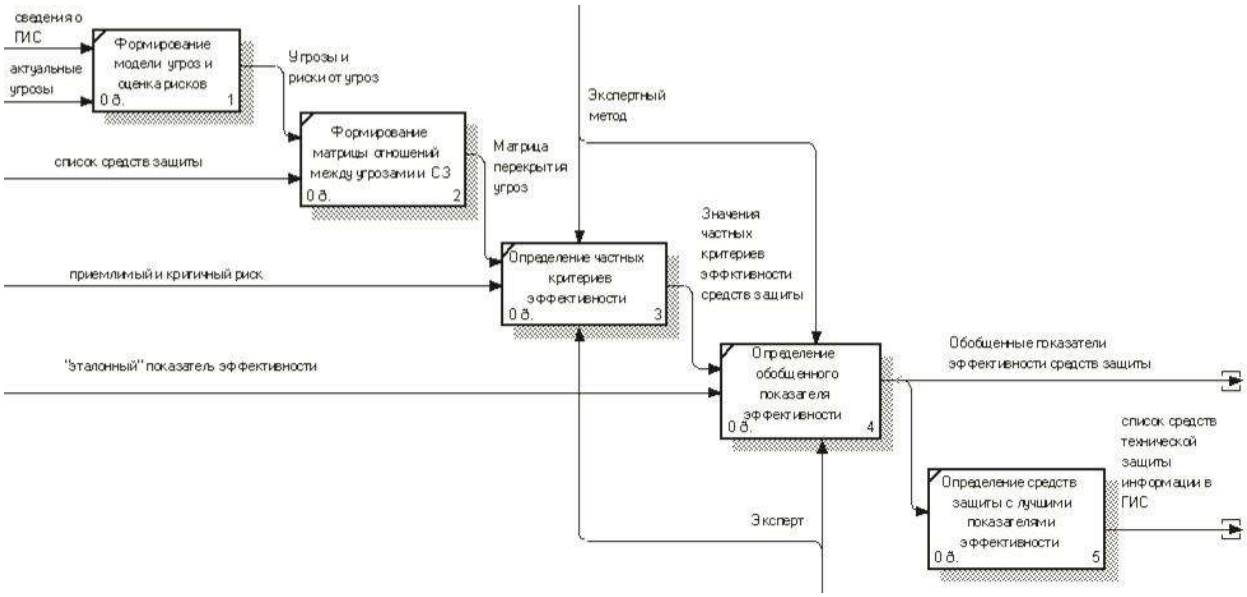

Рисунок 1 – Декомпозиция функциональной модели определения состава СТЗ информации в ГИС (экранная копия)

Для автоматизации разработанного метода определения состава СТЗ информации в ГИС разработан программный комплекс, имеющий следующий интерфейс (рисунок 2).

Разработанный программный комплекс, реализующий экспертный метод определения состава СТЗ информации в ГИС, позволяет эксперту оценить ценность активов ГИС, выявить угрозы этим активам, основываясь на банке данных угроз безопасности информации ФСТЭК России, осуществить оценку рисков ИБ, определить контрмеры и состав системы технической защиты информации в государственных информационных системах, минимизирующий вероятность реализации существующих угроз ИБ [5].

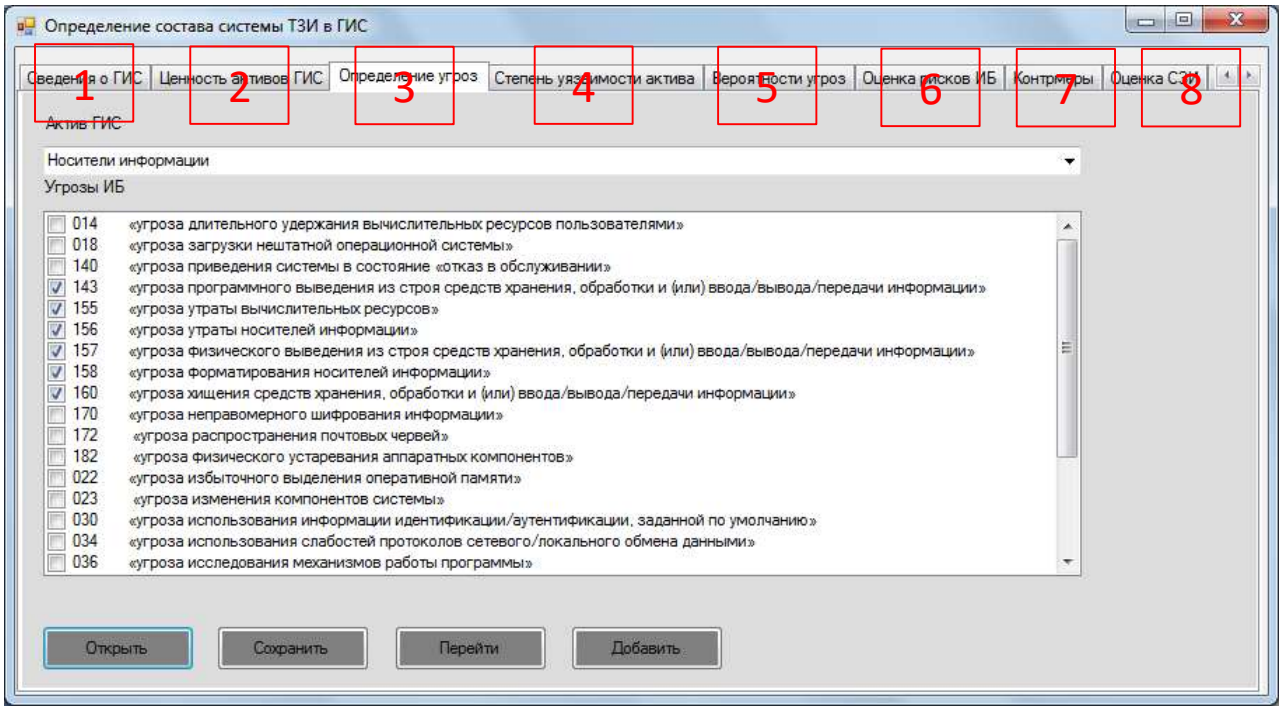

Рисунок 2 - Графический пользовательский интерфейс программного комплекса определения состава СЗИ в ГИС (экранная копия): 1) ввод сведений о ГИС; 2) ввод сведений об активах ГИС и определение их ценности; 3) определение угроз ИБ для активов ГИС; 4) оценка уязвимости активов ГИС; 5) оценка вероятности угрозы; 6) уровень риска ИБ для активов ГИС; 7) ввод контрмер для перечня угроз ценным активам ГИС; 8) оценка по критериям технических СЗИ, реализующих контрмеры; 9) список технических средств для защиты информации в ГИС

Литература

1. Бабенко А.А. Козунова С.С. Модель управления защитой информации в государственных информационных системах. – НБИ технологии, 2018. – Т.12. – № 4. – С. 16-22.

2. Жаринова С.С., Бабенко А.А. Оптимизация инвестиций в информационную безопасность предприятия. – Информационные системы и технологии, 2014. – № 3(83). – С. 114-123.

3. Козунова С.С., Бабенко А.А. Модель безопасности информации в сегменте корпоративной информационной системы. – Информационные системы и технологии, 2017. – № 1(99). – С.87-91.

4. Y.M. Gushchina, A.A. Babenko and Y.S. Bakhracheva AIP Conf. Proc. 2313, 070025 (2020)

5. Бабенко А.А. Жарков Г.В. Программа определение состава системы технической защиты информации в государственных системах: св-во о гос. рег. прогр. для ЭВМ 2020615502 Российская Федерация. Зарегист. 25.05.2020.