СЕКЦИЯ IX
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МОДЕЛИРОВАНИЕ

РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ВЫЯВЛЕНИЯ НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТЕ

В. В. Аниканов

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Брянский государственный технический университет», Россия

Научный руководитель В. И. Аверченков

В процессе построения систем информационной безопасности одним из ключевых аспектов является разработка модели нарушителя. Данная модель позволяет систематизировать информацию о типах и возможностях субъектов, целях их воздействия и подготовки необходимых средств организационной и технической защиты. Правильно разработанная модель нарушителя является гарантией построения грамотной системы информационной безопасности.

Актуальность работы обусловлена тем, что большое количество конфиденциальной информации обрабатывается с использованием средств автоматизации, доступ к которым случайно или преднамеренно может получить нарушитель. Система комплексного анализа всех возможных нарушителей и методов противодействия угрозам позволит снизить стоимость системы информационной безопасности, определить величину ущерба от несанкционированного доступа к защищаемой информации, а также рационально использовать средства защиты информации.

Важным аспектом является отсутствие автоматизированных систем, позволяющих рекомендовать службе безопасности способы и средства противодействия отдельным категориям нарушителей информационной безопасности. В связи с этим система безопасности выстраивается обобщенная и не учитывает специфику работы организации и уровень подготовки работников.

Главной целью работы является разработка автоматизированной системы на базе собственной методики выявления нарушителей информационной безопасности.

В основные задачи работы входят:

1) разработка методики классификации объектов защиты;

2) разработка методики классификации способов несанкционированного и непреднамеренного воздействия;

3) категорирование нарушителей информационной безопасности с выработкой наиболее оптимальных способов противодействия;

4) оценка предрасположенности к несанкционированному доступу отдельных категорий нарушителей;

5) оценка вероятности нарушения и величины ущерба.

Анализ возможностей нарушителя показывает, что для построения эффективной системы безопасности недостаточно определить категории нарушителей. Необходимо сформировать индивидуальную картину относительно каждого сотрудника организации в соответствии с профессиональными обязанностями, уровнем доступа

к ресурсам организации, имеющимся навыкам и интересам, после чего классифицировать потенциальные объекты защиты, а также способы воздействия на них.

Рассмотрим концептуальную модель работы автоматизированной системы (рис. 1).

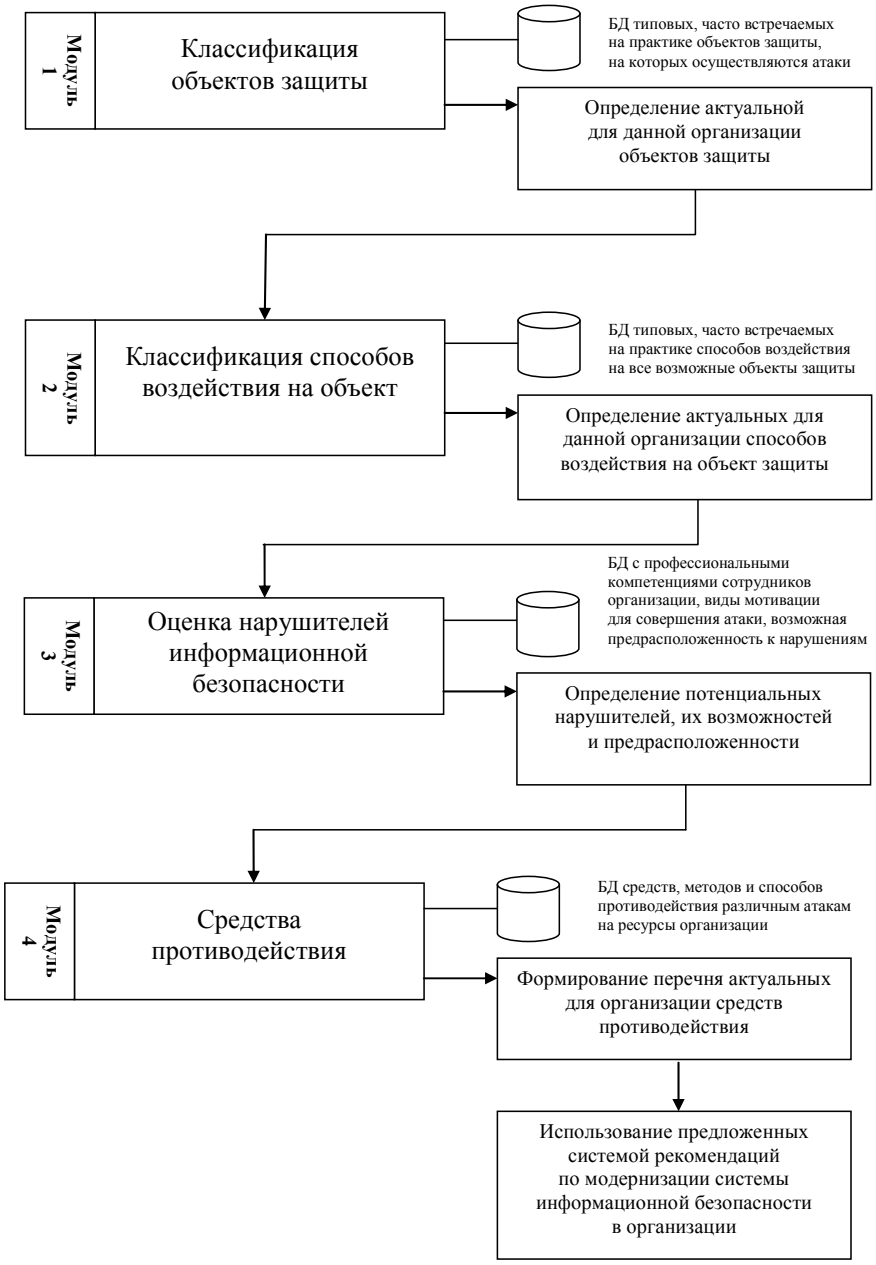

Рис. 1. Концептуальная модель работы системы

Рассмотрев основные виды атак, можно выделить следующие виды объектов, на которые нарушители наиболее часто оказывают воздействие:

1) информационные системы;

2) базы данных;

3) средства защиты информации.

Любой из данных объектов имеет определенные параметры, используя которые нарушитель может реализовать атаку. Для того чтобы учитывать различные сцена-

рии атак на систему, конкретному типу нарушителей можно присвоить определенный уровень технической и организационной подготовки для реализации тех или иных угроз в соответствии с уровнями.

В рамках реализации проекта предполагается разработать совокупность основных модулей, представленных в концептуальной модели, и дополнительных:

1. Модуль классификации объектов защиты.
2. Модуль классификации способов воздействия на объект.
3. Модуль классификации нарушителей информационной безопасности.
4. Модуль тестирования потенциальных нарушителей на предрасположенность к реализации атак.
5. Модуль оценки вероятности нарушения.
6. Модуль оценки величины ущерба в случае реализации угрозы.

Каждый модуль будет разрабатываться на основе авторской методики, которая будет учитывать уровень информационной безопасности в организации и требования нормативно-правовых документов.

Акцент в разработке методики для данной автоматизированной системы будет сделан на анализ возможностей потенциального нарушителя (организационные и технические) с учетом профессиональных компетенций, а также на анализ совокупности положительной и отрицательной мотивации, которая может подтолкнуть потенциального нарушителя информационной безопасности к атаке на ресурсы организации.

Потенциальными покупателями данной системы являются коммерческие фирмы, федеральные органы власти, органы муниципального управления, которые заинтересованы в безопасности информации, которая хранится и обрабатывается в информационных системах и базах данных, а также в санкционированном доступе к средствам защиты информации.

ИНФОРМАЦИОННО-СПРАВОЧНОЕ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ «УЛИЦЫ ГЕРОЕВ»

Г. В. Беломутов, П. Ю. Дроздов, А. С. Куранцов, И. Д. Шинкоренко

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Беларусь

Научный руководитель Т. В. Тихоненко

Именами Героев Великой Отечественной войны названо большое количество улиц. Не исключением является Гомель – город с богатым историческим прошлым. В нем насчитывается более 60 улиц, названных в честь Героев Великой Отечественной войны. Иногда, прогуливаясь по такой именной улице, возникает вопрос: почему она так называется? Можно долго искать в Интернете ответы, но, на наш взгляд, проще, когда под рукой есть специальное приложение, содержащее всю достоверную информацию по необходимым улицам.

Разработанное мобильное приложение «Улицы Героев» – это своеобразный путеводитель по улицам города Гомеля, названным в честь Героев Великой Отечественной войны. Это приложение разрабатывалось к годовщине освобождения города Гомеля от немецко-фашистских захватчиков. Приложение дает возможность ознакомить жителей и гостей города Гомеля с его историей, путем предоставления интересной информации через специализированное приложение для мобильных телефонов и планшетов (рис. 1).