DOI: 10.58168/CISMP2024_366-370
УДК 004.94

АВТОМАТИЗИРОВАННАЯ СИСТЕМА НА ОСНОВЕ МОДЕЛИ «ПОЛНОГО ПЕРЕКРЫТИЯ» ДЛЯ АНАЛИЗА ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

И.В. Луценко

Приднестровский Государственный Университет им Т.Г. Шевченко

Аннотация. В статье рассматривается процесс построения защиты информации в информационной системе предприятия с использованием модели “полного перекрытия”, благодаря которой можно найти оптимальный состав средства для построение системы защиты информации в информационной системе предприятия или организации.

Ключевые слова: защита информации, информационная система, угрозы, автоматизирования система.

AN AUTOMATED SYSTEM BASED ON THE “FULL OVERLAP” MODEL FOR ANALYZING THE PROTECTION OF AN ENTERPRISE INFORMATION SYSTEM

I.V. Lutsenko

T.G. Shevchenko Pridnestrovian State University

Abstract. The article discusses the process of building information protection in the information system of an enterprise using the “complete overlap” model, thanks to which it is possible to find the optimal composition of the means for building an information protection system in the information system of an enterprise or organization.

Keywords: information protection, information system, threats, automation system.

Развитие информационных технологий упростило задачи по защите данных, внедрив автоматизированные системы для обеспечения информационной безопасности. Такие системы позволяют не только собирать и хранить данные, но и оперативно оценивать их уязвимости, а также принимать меры для защиты этих данных. В условиях, когда предприятие обрабатывает не только товары и сырье, но и ключевую информацию о покупках, отчетах и других данных, от которых зависят дальнейшие бизнес-решения, автоматизация защиты становится необходимой.

Автоматизированные системы защиты информации помогают владельцам определять ценность данных и выбирать оптимальные меры безопасности. Благодаря анализу угроз и различным методам из теории информации, система способна быстро оценить риски и предложить эффективные стратегии для

предотвращения утечек или несанкционированного доступа. Собственник информации принимает решение о степени конфиденциальности и ресурсах, которые следует инвестировать в защиту, на основе рекомендаций системы, что снижает трудоемкость и упрощает процесс принятия решений в условиях повышенных рисков.

Для упрощения реализации выбора средств защиты информации используют различные системы, которые позволяют моделировать защиту данных информационной системы.

Данные системы используют различные модели для моделирования процесса. Моделирование процесса защиты информации представляет собой сложную задачу, для решения которой применяются методы декомпозиции и приведения сложной задачи к формальному описанию и решению данной задачи формальными методами.

Наиболее подходящей моделью при проектированиии системы защиты информации является модель системы с полным перекрытием (модель Клементса-Хофмана) (рис. 1). Модель позволяет оценить защищенность системы, рассчитать затраты для проектирования системы защиты информации, а также определить оптимальный вариант построения системы безопасности. Для реализации модели используется теория графов, теория нечетких множеств и теория вероятности.

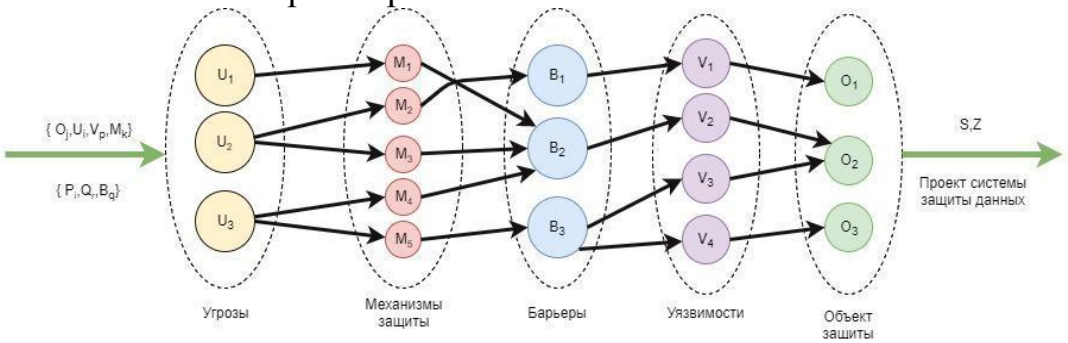

Рисунок 1 – Модель системы полного перекрытия
(модель Клементса – Хофмана)

Для построения модели с полным перекрытием необходимо определить три множества:

- множество угроз $U = \{u_i\}, i = \overline{1,m}$;
- множество объектов барьеров $O = \{o_j\}, j = \overline{1,n}$;
- множество механизмов защиты $M = \{m_k\}, k = \overline{1,r}$.

Элементы множества U и O находятся между собой в определенных отношениях «угроза – объект», определяемых двудольных графом $G(X,E)$, где X - множество вершин графа $X = \{x_{i+j}\}, i = \overline{1,m}, j = \overline{1,n}$, а E - множество дуг графа. Дуга $< U_i, O_j >$ существует только тогда, когда U_i является средством получения доступа к объекту O_j.

Цель защиты модели состоит в том, чтобы «перекрыть» каждую дугу графа и создать барьер для доступа по этому пути.

Используя множество средств защиты информации M, 2-х дольный граф преобразуется в 3-х дольный.

В защищенной системе данных все рёбра представляются в виде:

$$< U_i, M_k > \text{ и } < M_k, O_j >$$

Предлагается ввести еще два элемента:

V - набор уязвимых мест в защите данных, с помощью которых можно осуществлять угрозы u_i в отношение объектов o_j.

B - набор барьеров в системе защиты информации, который представляют собой пути осуществления угроз безопасности, перекрытые средствами защиты.

Таким образом, процесс защиты информации представляет собой кортеж:

$$S = \{O, U, M, V, B\}, \quad (1)$$

Где O - множество защищаемых объектов;

U - множество возможных угроз;

M - множество средств защиты;

V - множество уязвимых мест в системе защиты информации;

B - множество барьеров.

Но, если рассматривать данную модель в информационной системе, то при получении доступа к защищаемому объекту, можно получить и доступ другим защищаемым объектам. Например, при получении доступа к информационной базе, злоумышленник может получить таблицы пользователей с их логинами и паролями, что позволит злоумышленнику авторизоваться, как администратор и иметь полный доступ к всей информационной системе.

Была реализована система автоматизированного проектирования на основе данной модели.

Для ввода данных используется модуль исходных данных об объекте. В данный модуль вводиться объекты, которые нужно защищать. Также сделана база знаний по средства предотвращения объектов (барьеры). Каждый объект имеет поля для ввода стоимости данного барьера. С помощью экспертной оценки проставляется коэффициент стойкости барьера от угрозы.

После выбора защищаемых объектов, система моделирует различные варианты угроз, которые есть в базе данных с барьерами, то находится оптимальный вариант, где процент стойкости барьеров от угроз на информационную систему и сумму стоимости затраченных на барьер.

Данная система реализована в виде веб-сайта, что позволяет без установки и использования веб-браузера заходить и обновлять информационную базу, а также производить анализ угроз. Скриншот работы системы представлен на рис. 2.

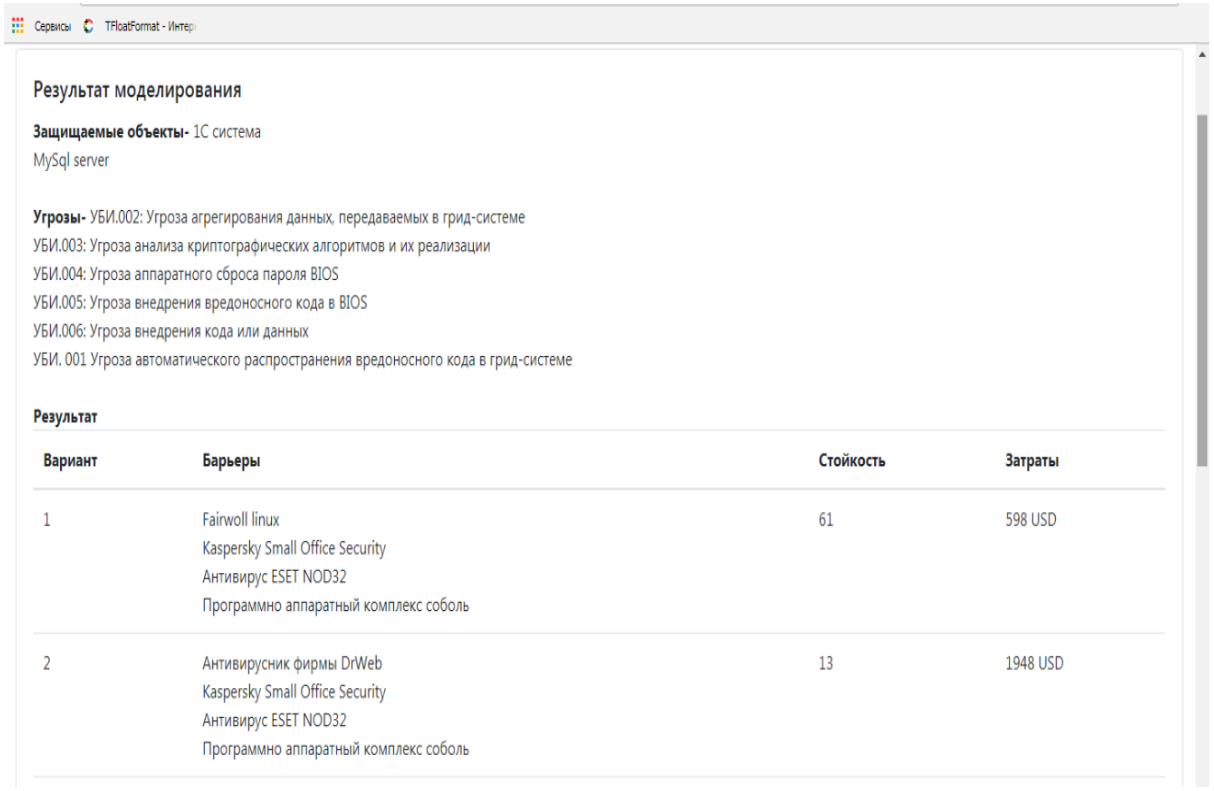

Рисунок 2 - Результат работы автоматизированной системы

Данная автоматизированная система моделирования угроз на информационную систему автоматически обновляет базу угроз и средств защиты информации, что позволяет держать построенную систему защиты актуальной для противодействия современным угрозам.

Применение автоматизированной системы, в основе работы которой лежит модель Клеменса-Хофмана для нахождения оптимального набора средств защиты информации на информационную систему предприятия, значительно снижает трудоемкость процессов, связанных с защитой информации, и повышает эффективность проектных решений.

Модель Клеменса-Хофмана учитывает множество факторов, таких как динамика угроз, оценка уязвимостей и рисков, что позволяет более точно прогнозировать возможные угрозы и оптимизировать меры по их предотвращению. Благодаря такому подходу, владельцы данных могут принимать обоснованные решения о том, какие меры безопасности внедрить, с учетом актуальной оценки рисков, что, в свою очередь, снижает затраты на избыточные меры и усилия. Автоматизация процессов анализа и защиты информации, основанная на данной модели, способствует ускорению проектирования и внедрения необходимых решений, повышает их адаптивность и обеспечивает более точное распределение ресурсов на защиту наиболее критичных данных.

Список литературы

1. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум : учеб. пособие. – 2-е изд., перераб. и доп. – М.: РИОР: ИНФРА-М, 2016. – 224 с.

2. Луценко И.В. Моделирование процесса защиты информации на промышленном предприятие // Приоритетные направления инновационной деятельности в промышленности. – 2024. – С. 143-145.

3. Рытов М.Ю. Использование специализированной САПР для проектирования комплексных систем защиты информации / М.Ю. Рытов, И.В. Луценко, М.А. Луценко // Инновационные, информационные и коммуникационные технологии. – 2018. – № 1. – С. 100-104.

References

1. Baranova Ye.K., Babash A.V. Modelirovaniye sistemy zashchity informatsii. Praktikum : ucheb. posobiye. – 2nd ed., revis. and add. – M.: RIOR: INFRA-M, 2016. – 224 p.

2. Lutsenko I.V. Modelirovaniye protsessa zashchity informatsii na promyshlennom predpriyatiye // Prioritetnyye napravleniya innovatsionnoy deyatel'nosti v promyshlennosti. – 2024. – P. 143-145.

3. Rytov M.Yu. Ispol'zovaniye spetsializirovannoy SAPR dlya proyektirovaniya kompleksnykh sistem zashchity informatsii / M.Yu. Rytov, I.V. Lutsenko, M.A. Lutsenko // Innovatsionnyye, informatsionnyye i kommunikatsionnyye tekhnologii. – 2018. – № 1. – S. 100-104.