УДК: 004.056
DOI: 10.30987/article_5d8d113d6e9f18.01574772

М.Ю. Рытов, И.В. Луценко, П.С. Цвинкайло

РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ НА МАЛОМ ПРЕДПРИЯТИИ С ПОМОЩЬЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

В статье рассматривает поиск оптимальной политики безопасности информационной системы малого предприятия с помощью модели полного перекрытия. С помощью реализованной автоматизированной модели можно быстро и качественно найти нужный набор барьеров защиты за определенные затраты.

Ключевые слова: *оптимальный набор, комплексная защита информации, малое предприятия, моделирование.*

M. Yu. Rytov, I. V. Lutsenko, P. S. Svincolo

SECURITY POLICY DEVELOPMENT FOR SMALL BUSINESS USING AN AUTOMATED SYSTEM

The article considers the search for the optimal security policy of the information system of a small enterprise using the model of complete overlap. With the help of the implemented automated model, you can quickly and efficiently find the right set of protection barriers at a certain cost.

Keywords: *optimal set, complex information protection, small enterprise, modeling.*

Введение

С развитием новых информационных технологий и появление доступных мощных компьютеров позволило малому бизнесу их использовать в безнес-процессе. Также появилась необходимость в повышение уровня защиты в связи с развитием хранения и обработки информации. Так постепенно защита экономической информации становится обязательной: разрабатываются возможные документы по защите информации, формируются рекомендации по защите информации, даже проводиться федеральный закон о защите информации, который рассматривает проблемы защиты информации и задачи защиты информации, а также решают некоторые уникальные вопросы защиты информации.

Следует, что угрозы защиты информации сделала средства обеспечением информационной безопасности одной из обязательных элементов информационной системы.

Под информационной безопасностью Российской Федерации(информационной системы) подразумевается техника защита информации от преднамеренного или случайного несанкционированного доступа и нанесения тем, самым вред нормальному процессу документооборорота и обмена данными в системе, а также хищения, модификации и уничтожения информации [1*].

Вопрос защиты информации на малом предприятии решаются для того, чтобы изолировать нормально работоспособную информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Успешная реализованная угроза на информационную система малого предприятии может привести временной остановки и финансовым потерям. Процесс реализации угрозы за последние года усовершенствовался. Для реализации уже не нужно специализированные знания, а требуется приобрести специализированное обеспечение которое по нажатию кнопки может обойди все барьеры защиты информации. Можно выделить распространенные меры защиты информации на малом предприятии: антивирусная защита, регулярное

обновление программного обеспечения и также тонкая настройка политики безопасности в информационной системы.

Процесс проектирование системы защиты информации трудоемкий. Для того чтобы спроектировать нужно нанимать в штат специалиста. Выход из такой сложной ситуации приходиться находить специалистам, которые смогут выполнять ряд задач других сотрудников. Для того, чтобы настроить всю информационную систему предприятия, необходимо иметь в штате инженера-программиста, который сможет проанализировать информационные потоки, и на основе анализа построить систему и внедрить на предприятие, а также в дальнейшем ее сопровождать при возникновении проблем.

1. Описание модели

Автоматизированные системы используют различные модели. Наиболее подходящей моделью для проектировании автоматизированной системы можно использовать модель “Клементса - Хофмана”. Данная модель позволяет найти оптимальный набор средств защиты информации (рис.1).

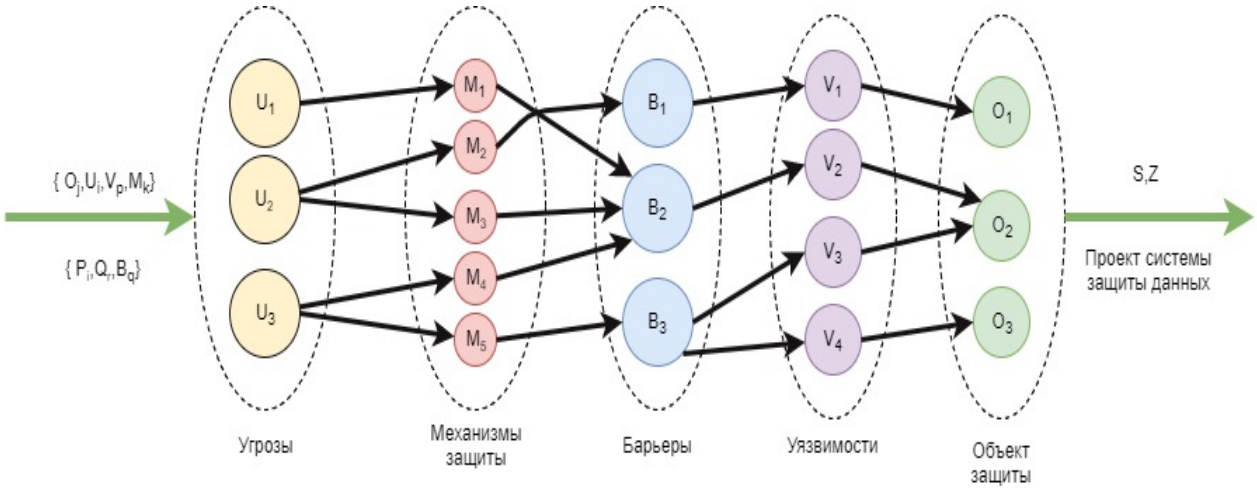

Рис. 1. Модель системы полного перекрытия (модель Клементса – Хофмана)

Модель проста в использовании, можно рассчитать защищённость барьеров системы, рассчитать экономические затраты при проектировании системы защиты информации, а самое главное определить оптимальный вариант построения системы безопасности.

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.

Чтобы получить доступ, злоумышленнику необходимо выполнить ряд этапов и процессов, которые можно свести к трем условиям разведывательного контакта злоумышленника с источником информации:

- поиск ценной информации ($P_{пр}$ - пространственный фактор);
- размещение программно-аппаратных средств для получения информации на удалении от источника, при котором гарантируется приемлемое отношение сигнал/шум на входе средства ($P_{эн}$ - энергетический фактор);
- совпадение времени проявления демаскирующих признаков объекта защиты

или передачи информации и работы средства добывания ($P_{вр}$ - временный фактор).

Угрозы выполняются одновременно при трех условиях, а общая вероятность равна произведению:

$$P = P_{пр} \cdot P_{эн} \cdot P_{вр}, \tag{2}$$

Аппарат нечетких множеств позволяет производить простейшие операции непосредственно со значениями лингвистических переменных без промежуточного перевода их в числовые значения.

Принцип обобщения Заде может найти функцию принадлежности нечеткого числа, советующего значению четкой функции от нечетких аргументов

$$\mu\overline{y} = f(x_1, x_2, ..., x_n) \to (\mu\overline{x}(x_i))$$
$$x_i \in \sup(\overline{x_i}), i = \overline{1,n} \tag{3}$$

Требуется в таких условиях найти нечеткое число

$$\tilde{p} = \tilde{p}_{пр} \cdot \tilde{p}_{эн} \cdot \tilde{p}_{вр} \tag{4}$$

Дефазификация вероятности проявления угрозы определяем по формуле:

$$p = \frac{\sum_{i=1}^{k} U_i \cdot \mu_A(U_i)}{\sum_{i=1}^{k} \mu_A(U_i)}. \tag{5}$$

Прочность барьера системы защиты информации характеризуется величиной остаточного риска $Risk_i$, связанного с возможностью осуществления угрозы u_i в отношении объекта o_j, при использовании барьера b_q. Определяется по формуле :

$$Risk_i = P_i \cdot Q_j \cdot (1 - B_q), i = \overline{1,m}, j = \overline{1,n}, q = \overline{1, m \times n};, \tag{6}$$

Где P_i - вероятность появления угрозы u_i,

Q_i - величина ущерба при удачном осуществлении угрозы u_i в отношении защищаемого объекта o_j. Величина ущерба рассчитывается в условных единицах,

B_q- степень сопротивления барьера, величина характеризует вероятность его преодоления.

По формуле можно определить величину защищенности всей системы:

$$S = \frac{1}{\sum_{(\forall b_q \in B)} (P_i \cdot Q_j \cdot (1 - B_q))},$$
$$P_i \in (0,1), B_q \in [0,1). \tag{7}$$

2. Структура автоматизированной системы, составные модули

Созданы универсальные алгоритмы в виде модулей, входящие в состав системы. Структурно-функциональная модель проектирования системы защиты информации представлена на рис. 2.

Задача моделирования защиты информации состоит в объективном описании объектов защиты, с помощью которых будет происходить процесс защиты. Защищаемый объект в модели (данные, сервер базы данных и т.д.) должен быть представлен на схеме системы защиты информации в виде некоторой структуры.

Свойствами этой структуры являются наиболее важные характеристики объекта, такие как перебор пароля, открытые порты в сервисе, установление антивирусного ПО и т.д. В моделирование объектов защиты так же входит: источник угрозы, описание основных моментов, где возможно произвести атаку для несанкционированного получения данных, описание с указанием характеристик существующих барьеров на путях проникновения за пределы защиты. На основе полученных данных происходит иерархическое построение модели объекта защиты.

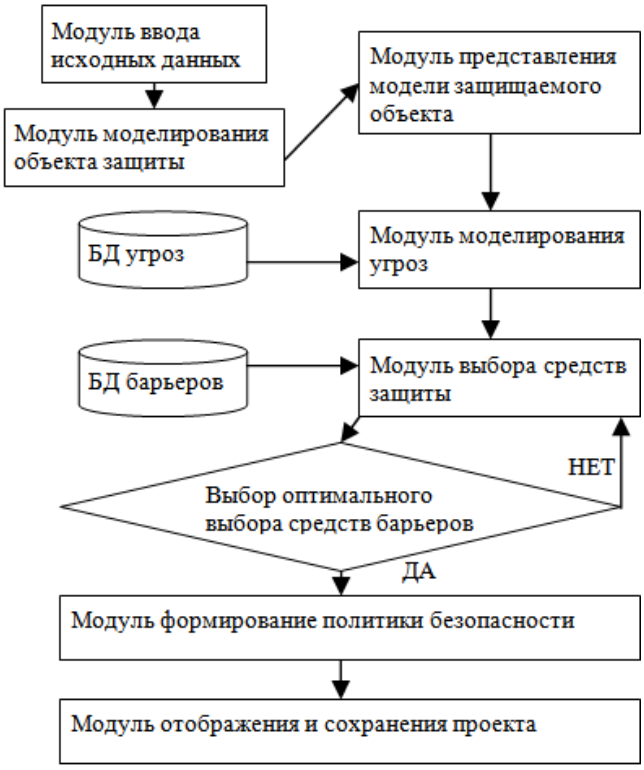

Рис. 2. Структурная схема системы защиты информации

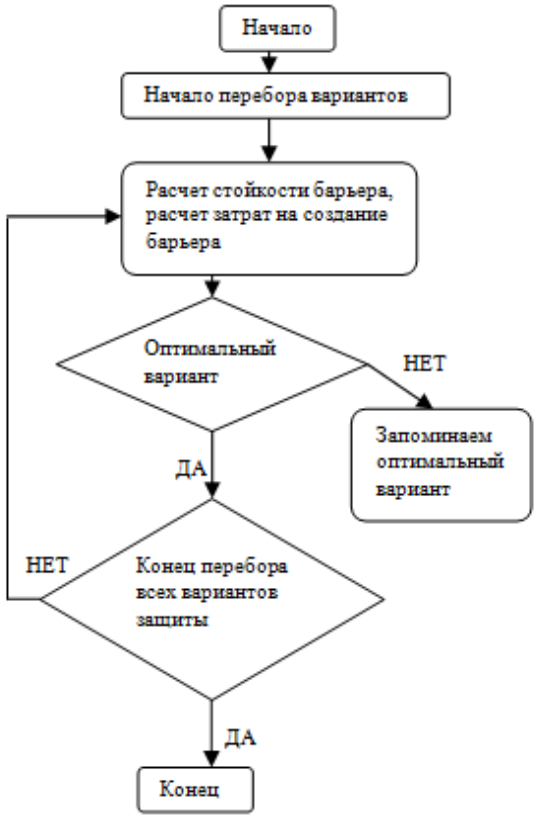

Рис. 3. Модуль перебора вариантов защиты

После создания модели защищаемого объекта происходит построение системы его защиты. Согласно принципам системного подхода, каждый элемент в программном

комплексе строится отдельным модулем, что позволяет динамически расширять возможности системы [2, с. 28].

В системе защиты информации основополагающим является программно-аппаратные средства защиты. Разработанные модули (рис. 3), позволяющие оценить и категорировать данные в соответствии в них определенных условий (в качестве таких условий выступают стойкость барьера, его цена и т.д.). Оценка основных элементов барьеров защиты таких как: персональный межсетевой экран, антивирусная программа, электронная цифровая подпись позволяют оценить их устойчивость к взломам, в случае нехватки стойкости предложить варианты по их замене или модернизации. Данные меры позволяют защитить максимально данные и увеличить время необходимое для злоумышленника, чтобы реализовать несанкционированный доступ. Данный запас позволяет системе проинформировать администратора, что был реализован несанкционированный доступ, и отреагировать, вычислив место нахождения, для задержания злоумышленника [1, с. 45].

3. Процесс проектирования

В ходе разработки *web*-сайта реализованы следующие списки:

1. Список угроз в БД.
2. Список источников угроз.
3. Список защищаемых объектов.
4. Список барьеров защиты в БД.
5. Список последствий от реализации угроз.

Открыв список угроз в БД (рис. 4) открывается окно, в котором представлены названия угроз и список действий, таких как: изменить, удалить и добавить запись. Все эти кнопки говорят сами за себя. Кнопка «Удалить» вызывает функцию, которая удалит тот элемент, напротив которого будет располагаться данная кнопка.

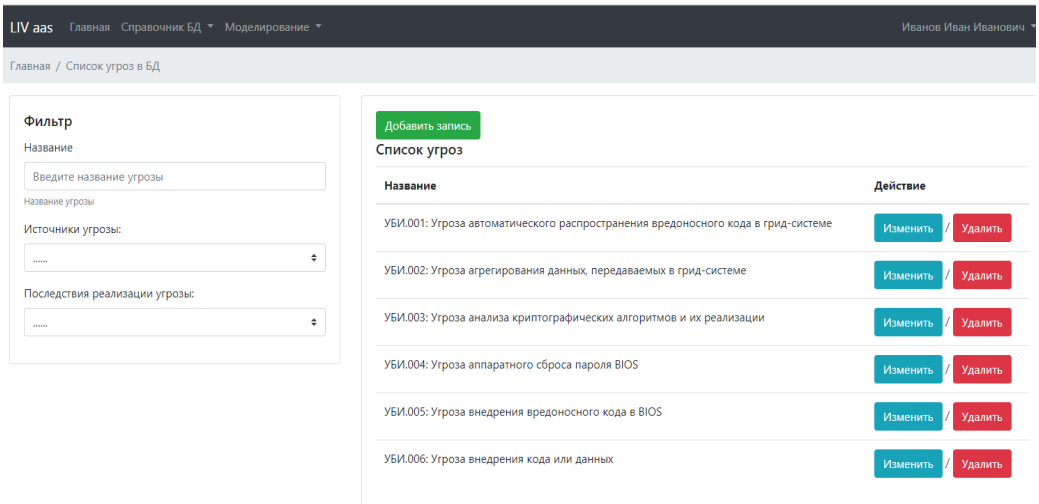

Рис.4. Список угроз в БД

При нажатии на кнопку «Изменить» открывается окно управления данными (рис. 5), где можно увидеть *ID* угрозы, описание угрозы, ее источники, и последствия, а также можно изменить эти поля, введя другое название или описание, также выбрав один или несколько пунктов в полях: «Источники угроз» и «Последствия реализации угрозы», затем нажать кнопку «Сохранить».

В окне «Список защищаемых объектов» (рис. 6) представлены названия объектов и список действий над этими объектами: «Добавить запись», «Изменить» и «Удалить».

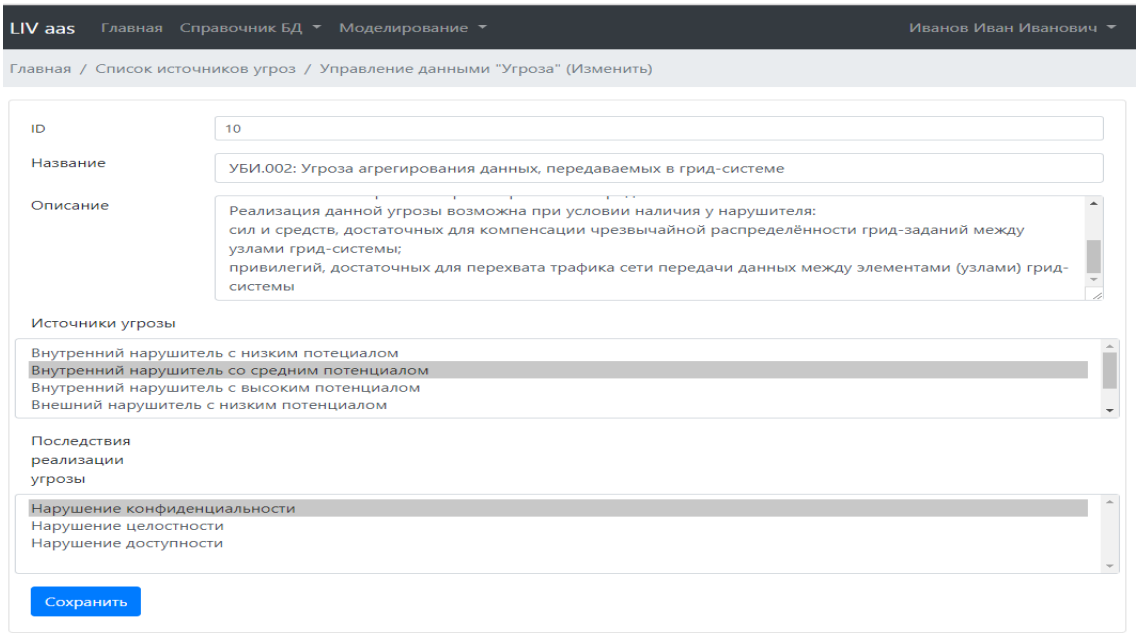

Рис. 5. Управление данными «Угроза»

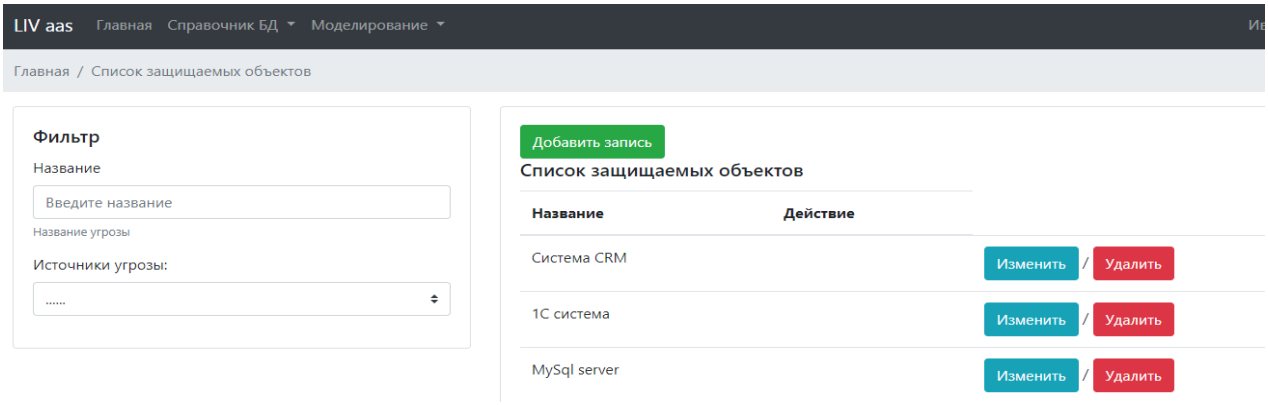

Рис. 6. Список защищаемых объектов

На странице списков барьеров защиты базы данных (рис. 7), также приведены названия барьеров и список действий, среди которых есть кнопка «Стойкость», которая позволяет просмотреть стойкость каждого барьера и внести изменения в случаях, когда данные неверны, либо потеряли свою актуальность.

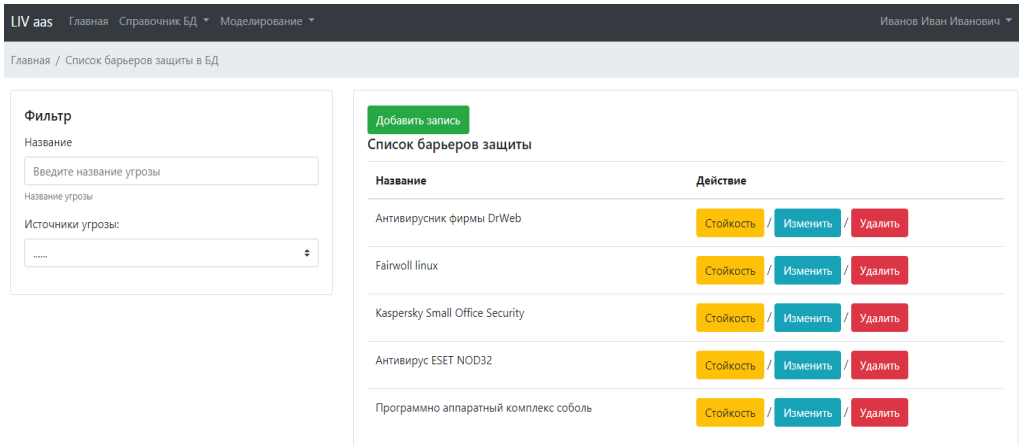

Рис. 7. Список барьеров защиты в БД

Нажав на кнопку «Стойкость» переходим в окно «Стойкость угрозам» (рис. 8), где указано:

1. Название барьера.
2. Название угрозы.
3. Стойкость барьера против данной угрозы.

Где также можно изменить поля в случаях, когда данные неверны, либо потеряли свою актуальность.

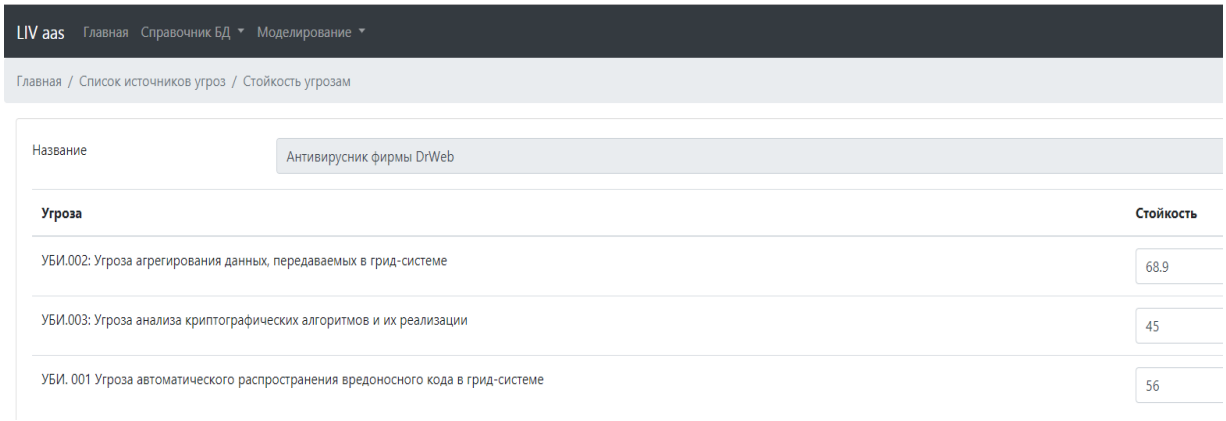

Рис. 8. Стойкость угрозам

Выбрав пункт «Моделирование» пользователю необходимо выбрать объекты, которые необходимо защитить, как показано ниже (рис. 9).

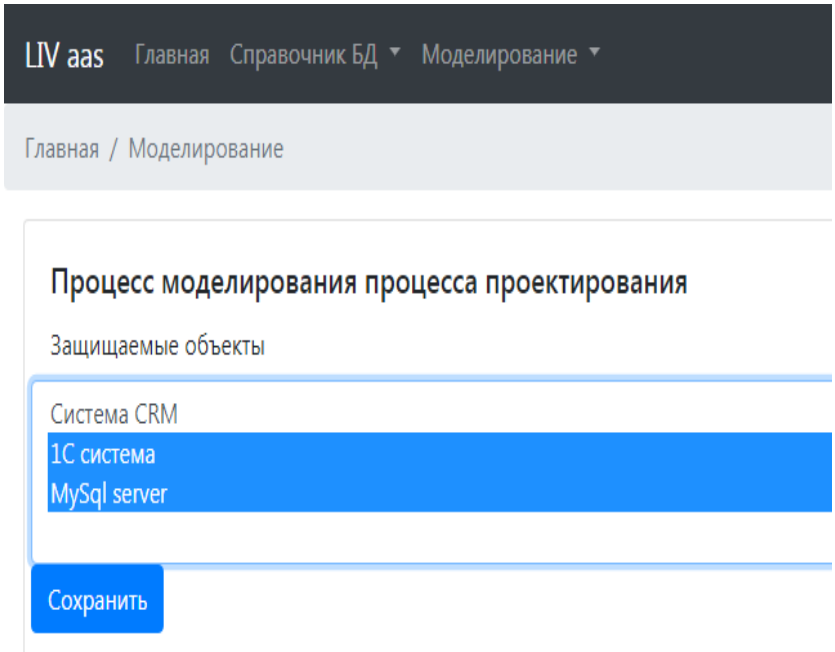

Рис. 9. Моделирование

После чего, обработав данные, пользователю предоставляется результат (рис. 10), в котором описаны: наименования защищаемых объектов, наименования угроз, которым подвержены объекты и варианты барьеров, которые можно противопоставить данным угрозам с описанием затрат и стойкости.

Результат моделирования

Защищаемые объекты- 1С система
MySql server

Угрозы- УБИ.002: Угроза агрегирования данных, передаваемых в грид-системе
УБИ.003: Угроза анализа криптографических алгоритмов и их реализации
УБИ.004: Угроза аппаратного сброса пароля BIOS
УБИ.005: Угроза внедрения вредоносного кода в BIOS
УБИ.006: Угроза внедрения кода или данных
УБИ. 001 Угроза автоматического распространения вредоносного кода в грид-системе

Результат

Вариант	Барьеры	Стойкость	Затраты
1	Fairwoll linux Kaspersky Small Office Security Антивирус ESET NOD32 Программно аппаратный комплекс соболь	61	598 USD
2	Антивирусник фирмы DrWeb Kaspersky Small Office Security Антивирус ESET NOD32 Программно аппаратный комплекс соболь	13	1948 USD
3	Антивирусник фирмы DrWeb Fairwoll linux Антивирус ESET NOD32 Программно аппаратный комплекс соболь	77	1579 USD

Рис. 10. Полученный результат моделирования

Заключение

Автоматизированная система позволила ускорить и увеличить качество защиты информации на малом предприятии в несколько раз, а (рис.11) также позволила сократить расходы на закупку только нужного перечня оборудования и его настройки для защиты информации. Благодаря нахождению оптимального варианта, автоматически время на проектирование комплексной системы защиты сократилось в 5 раз, уменьшилось появление ошибок при проектировании, а также закупка оборудование сократилась на 30 процентов.

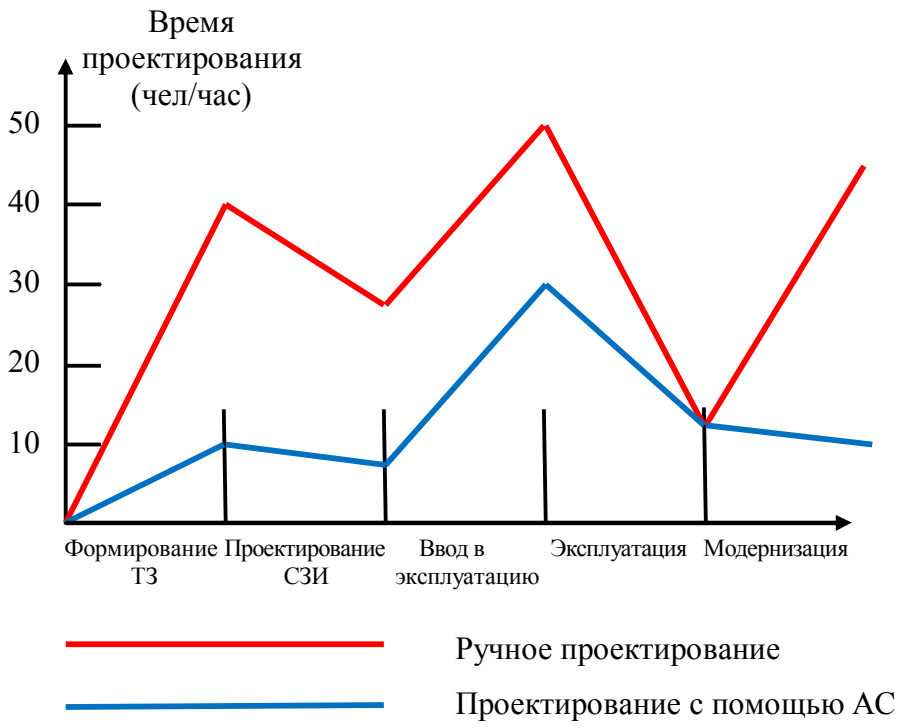

Рис. 11. Сравнительный анализ время проектирования с помощью системы или ручным методом

В результате работы для проектирования программного обеспечения была выбрана модель полного перекрытия, которая позволяет находить оптимальный вариант средств защиты информации. В конечном результате выдается перечень различных политик безопасности с общей стойкостью угроз и затрат на реализацию. Предложенные политики безопасности позволяют существенно сэкономить время на выборе необходимой. С помощью данного сайта малым предприятиям не нужно обращаться к дорогостоящим специалистам, ведь поиск оптимальной политики безопасности станет быстрым и удобным.

Разработанный программный продукт способен эффективно производить вычисления по нахождению оптимальной стоимости и стойкости барьеров. В перспективе планируется расширить функционал сайта для работы с более сложными информационными системами.

Список литературы:

1. Алаухов С.Ф. Вопросы создания систем информационной безопасности для крупных промышленных объектов / С.Ф. Алаухов, В.Я. Коцеруба // Системы безопасности. – 2011. – № 41. – С. 93.
2. Аверченков В.И. Организационная защита информации / В.И. Аверченков, М.Ю. Рытов. – Брянск: Изд-во БГТУ, 2015. – 184 с. – (Серия «Организация и технология защиты информации»).
3. Алаухов С.Ф. Вопросы создания систем информационной безопасности для крупных промышленных объектов / С.Ф. Алаухов, В.Я. Коцеруба // Системы безопасности. – 2011. – № 41. – С. 93.
4 Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. – СПб.: БХВ-Петербург, 2010.
5. Баранова Е.К. Моделирование системы защиты информации. Практикум: учеб. пособие / Е.К. Баранова, А.В. Бабаш. – М.: РИОР: ИНФРА-М, 2016. – 224 с.
6. Драгунова Е. В., Митев П. К. Моделирование бизнес-процесса выбора инвестиционного поведения предприятия // Молодой ученый. — 2010. — №10. — С. 35-38. — URL https://moluch.ru/archive/21/2103/ (дата обращения: 10.01.2019).
7. Луценко И.В. Способы и приемы оценки защищенности данных малого предприятия / И.В. Луценко, М.Ю. Рытов // Информационные системы и технологии. – 2018. - №3(107). – с. 125.
8. Мельников, В.П. Информационная безопасность и защита информации. / В.П.Мельников, С.А.Клейменов, А.М.Петраков // 3-е изд., стер. - М.: Академия, 2008. — 336 с.
9. 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. – Москва. Ассоциация выпускников и сотрудников ВВИА им проф. Жуковского, 2018. – 652 с.

References:

1. Alukov S. F. the creation of information security systems for large industrial facilities / S. F. Alahov, V. J. Kotseruba // security System. - 2011. - №41. - P. 93.
2. Averchenkov V. I. Organizational information security / V. I. Averchenkov, M. Yu. Rytov. - Bryansk: Publishing house of BSTU, 2015. - 184 p. - (Series "Organization and technology of information security").
3. Alukov S. F. the creation of information security systems for large industrial facilities / S. F. Alahov, V. J. Kotseruba // security System. - 2011. - №41. - P. 93.
4. Anin B.Y. Protection of computer information systems / B. Y. Anin. – SPb.: BHV-Petersburg, 2010.
5. Baranova E. K. Modeling of information security system. Workshop: studies. posobie / E. K. Baranova, A. V. Babash. – M.: RIOR: INFRA-M, 2016. - 224 p.
6. Dragunova E. V., Mitev p. K. Modeling of business process of the choice of investment behavior of the enterprise. Young scientist. - 2010. - №10. - P. 35-38. URL https://moluch.ru/archive/21/2103/ (accessed: 10.01.2019).
7. Lutsenko I. V. Methods and techniques for assessing the data security of a small enterprise / I. V. Lutsenko, M. Yu. Rytov / / Information systems and technologies. - 2018. - №3 (107). - p. 125.
8. Melnikov, V. P. Information security and information protection. / V. P. Melnikov, S. A. Kleimenov, A. M. Petrakov // 3rd ed., erased. - Moscow: Academy, 2008. - 336 p.
9. Rytov M. Yu. The use of specialized CAD for the design of complex information security systems / M. Yu. Rytov, I. V. Lutsenko, M. A. Lutsenko / / Innovative, information and communication technologies. – Moscow. The alumni Association staff and vvia Zhukovsky them prof, 2018. - 652 p.

Статья поступила в редколлегию 03.04.19.
Рецензент: д.т.н., доцент,
Брянский государственный технический университет
Аверченков А.В.
Статья принята к публикации 30.04.19.

Сведения об авторах:

Рытов Михаил Юрьевич
кандидат технических наук, доцент,
заведующий кафедрой «Системы информационной безопасности» Брянского государственного технического университета.
Тел.: +79103300237
E-mail: rmy@tu-bryansk.ru

Луценко Игорь Владимирович
аспирант кафедры «Системы информационной безопасности» Брянского государственного технического университета.
Тел.: +79206025080
E-mail: EROPA@LIVE.RU

Цвинкайло Петр Станиславович
Старший преподаватель кафедры «АТПиП» в Рыбницком Филиале ПГУ им Т.Г.Шевченко
Тел.: +79206025080
E-mail: human033@gmail.com

Information about authors:

Rytov Mikhail Yurevich
Candidate of Technical Sciences, Associate Professor,
Head of the department
«Information security systems»,
Bryansk state technical university
Phone: +79103300237
E-mail: rmy@tu-bryansk.ru

Lutsenko Igor Vladimirovich
Post-graduate student of the department «Information security systems», Bryansk state technical university
Phone: +79206025080
E-mail: eropa@live.ru

Ciencia Peter Stanislavovich
Senior lecturer of the department "ATEP" in Rybnitsa Branch of PSU of T. G. Shevchenko
Phone: +79206025080
E-mail: human033@gmail.com