**BCM-Analyser**

**v.2.0**

**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**

020313-2.0-33

2014 г.

**Аннотация**

Настоящий документ содержит принципы функционирования, описание правил использования и порядка эксплуатации программного продукта «BCM-Analyser v.2.0».

Последовательность установки программного продукта «BCM-Analyser» представлена в «Руководстве по установке BCM-Analyser v.1.2» (020313-2.0-34).

Руководство пользователя описывает:

* принципы функционирования комплекса;
* процедуры ввода исходных данных в программный продукт;
* проведение расчетов;
* процедуры получения и экспорта результатов расчетов.

**Содержание**

[Перечень сокращений 4](#_Toc406593646)

[1. Общие положения 4](#_Toc406593647)

[1.1. Цели использования 4](#_Toc406593648)

[1.2. Решаемые задачи 4](#_Toc406593649)

[2. Принципы функционирования комплекса 5](#_Toc406593650)

[2.1. Общие принципы 5](#_Toc406593651)

[2.2. Объекты безопасности, типы объектов 5](#_Toc406593652)

[2.3. Свойства объектов и ущерб 7](#_Toc406593653)

[2.4. Угрозы 10](#_Toc406593654)

[2.5. Контрмеры 12](#_Toc406593655)

[2.6. Проекты 17](#_Toc406593656)

[3. Порядок работы с программным комплексом 19](#_Toc406593657)

[3.1. Общий порядок 19](#_Toc406593658)

[3.2. Определение всех возможных свойств объектов 19](#_Toc406593659)

[3.3. Определение всех возможных угроз 20](#_Toc406593660)

[3.4. Определение всех возможных контрмер 22](#_Toc406593661)

[3.5. Определение всех возможных типов объектов безопасности 26](#_Toc406593662)

[3.6. Управление проектом 29](#_Toc406593663)

[3.7. Расчет проекта, получение результатов 32](#_Toc406593664)

[3.8. Экспорт результатов 34](#_Toc406593665)

[Термины и определения 35](#_Toc406593666)

[Приложение – Пример формы сбора данных об ущербе 36](#_Toc406593667)

Перечень сокращений

|  |  |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| ПО | Программное обеспечение |

1. Общие положения
   1. Цели использования

Целью использования программного комплекса является:

* определение оптимальной стратегии управления рисками (принятие, уменьшение, избежание или перенос рисков);
* оценка необходимости внедрения контрмер, обеспечивающих непрерывность бизнес-процессов;
* формирование множества экономически обоснованных требований к контрмерам, обеспечивающим непрерывность бизнес-процессов.
  1. Решаемые задачи

В процессе использования комплекса решаются следующие задачи:

* сбор информации о бизнес-процессах и ресурсах, участвующих в этих бизнес-процессах;
* определение пользователем ожидаемого ущерба бизнес процессам при реализации различных рисков;
* при необходимости, дополнение параметров внесенных в базовую конфигурацию комплекса, либо изменение существующих;
* автоматизированный выбор оптимальной стратегии управления операционными рисками – принятие, уменьшение, перенос или избежание риска;
* автоматизированный выбор оптимальных контрмер реализующих выбранную стратегию управления рисками.

1. Принципы функционирования комплекса
   1. Общие принципы

Общие принципы работы программного комплекса:

* «Единая мера эффективности». Используемые в программном комплексе исходные данные, параметры, характеристики позволяют получить оценку эффективности различных способов снижения затрат возникающих при ведении бизнеса. Мерой эффективности служат денежные единицы.
* «Открытость для редактирования». Учитывая все многообразие возможных бизнес-процессов, различных ресурсов, средств и систем, используемых в их составе, работа с программным комплексом подразумевает возможность дополнения параметров внесенных в базовую конфигурацию комплекса и их обработку на базе единых алгоритмов заложенных в комплекс.
* Рекомендуется не удалять свойства, угрозы, контрмеры, которые уже заданы в программном комплексе. В противном случае, при получении обновления базы контрмер, некоторые контрмеры могут быть установлены некорректно и не учитываться при проведении анализа.
  1. Объекты безопасности, типы объектов

Основой для анализа непрерывности бизнес-процессов является выявление бизнес-процессов и объектов безопасности или активов (помещений, машин, оборудования, вычислительной техники, конкретных файлов, каталогов, баз данных, персонала и других ресурсов), обеспечивающих функционирование этих бизнес-процессов. В программном комплексе возможно задание любых объектов.

Объекты могут обладать вложенностью. Вложенность объектов описывает зависимость некоторых свойств объектов от других объектов.

*Примером вложенности объектов является файловый сервер с хранящейся на нем информацией или помещение с установленным в нем оборудованием.*

При реализации некоторых угроз в отношении объекта, в который вложены другие объекты, ущерб наносится и всем вложенным объектам.

*Примером является угроза пожара в помещении, в результате которого наносится ущерб и всем объектам находящимся в данном помещении. Другим примером является сбой в работе аппаратной части сервера, в результате которого нарушается доступ к информации.*

Наследование ущерба в отношении вложенных объектов происходит не всегда.

*К примеру, повреждение грузовой машины вследствие поломки, в общем случае, не ведет к повреждению груза.*

Так как в реальности существуют однотипные объекты – объекты, обладающие одинаковыми свойствами, одинаковой степенью использования в бизнес-процессах, в программном комплексе возможна типизация объектов. При этом типизация производится по следующим направлениям:

1. Если на некоторую группу объектов действуют одинаковые угрозы и применимы одинаковые контрмеры, то в программном комплексе задается «Тип объекта безопасности», который используется при описании таких объектов.

*Примером объектов, которые могут являться однотипными являются:*

* *помещения;*
* *АРМ пользователей;*
* *автомобили и т.п.*

1. Если некоторая группа объектов имеет не только одинаковые угрозы и контрмеры, но и одинаковые свойства, ущерб по этим свойствам, то при задании таких объектов можно задать такой объект один раз и указать общее количество таких объектов.

Сводные параметры объектов и типов объектов, которые необходимо определить в программном комплексе, представлены в таблице 2.1.

Таблица 2.1 – Сводные параметры объектов и типов объектов

| **Параметр** | **Диапазон значений** **(ед. измерения)** | **Характеристика параметра** |
| --- | --- | --- |
| **Параметры объектов** |  |  |
| Тип объекта безопасности | Все предопределенные типы | Параметр определяет принадлежность объекта к какому-либо типу |
| Свойства | Все предопределенные свойства | Характеристики объекта, нарушение которых приведет к ущербу, например, конфиденциальность информации, целостность оборудования.  Подробнее см. раздел 2.3 |
| Ущерб по каждому свойству |  | см. раздел 2.3 |
| Объем защищаемых ресурсов объекта | Целое, положительное число (для информации в измеряется в Мбайт) | Параметр позволяет определять контрмеры, которые обеспечивают восстановление ресурсов после их повреждения (например, эффективность стримера зависит от объема ресурсов, которые он позволяет восстановить в единицу времени).  В стандартной конфигурации комплекса параметр используется для определения объема информационных массивов входящих в объект, указывается в Мбайтах. Однако, возможно, использовать данный параметр и для других объектов, при этом единица измерения в объекте и соответствующей контрмере восстановления должны быть одинаковыми. |
| Количество объектов в проекте[[1]](#footnote-1) | Целое, положительное число (штук) | Значение определяет количество идентичных объектов, у которых совпадают все параметры, определенные в данной таблице |
| **Параметры типов объектов** |  |  |
| Действующие угрозы | Все предопределенные угрозы | Параметр определяет угрозы, действующие на данный тип объектов |
| Применимые контрмеры | Все предопределенные контрмеры | Параметр определяет контрмеры, которые могут быть применены к данному типу объектов |

* 1. Свойства объектов и ущерб

Каждый объект имеет ряд свойств от характеристик, которых зависит корректное использование этих объектов в рамках бизнес-процесса. Примером свойства является, например, целостность оборудования.

Свойства объектов основываются на следующих состояниях компонентов обеспечивающих функционирование бизнес-процессов:

* наличие или отсутствие объекта,
* возможность использования объекта в нужное время и в нужном месте или отсутствие такой возможности,
* соответствие состава и структуры объекта требованиям бизнес-процесса или несоответствие;
* объект используется по назначению или нет.

Нарушение свойств ведет к негативным последствиям для бизнес-процессов (денежному ущербу), в частности:

* нарушение целостности может привести к ошибочному, некорректному функционированию бизнес-процесса;
* нарушение доступности ресурсов может привести к полной или частичной остановке бизнес-процесса;
* нарушение конфиденциальности информации может привести к потере выгоды от функционирования бизнес-процесса;
* нарушение владения может привести к полной или частичной остановке бизнес-процесса.

Ущерб в результате нарушения свойств может быть выражен в виде дополнительных затрат, снижения величины получаемой прибыли и т.п. При анализе могут быть использованы следующие наиболее явные последствия ущерба:

* недополученный доход;
* потеря средств размещенных на счетах;
* увеличение затрат на сотрудников (больший объем работ, простой) и связанные с этим дополнительные выплаты заработной платы;
* увеличение выплат на социальные нужды;
* дополнительные затраты на материалы, энергию, сырье и т.п.;
* судебные издержки;
* дополнительные командировочные и представительские расходы;
* пени, неустойки, штрафы и т.п.
* При анализе объектов необходимо учитывать возможность их вложенности и, соответственно, суммировать возможный ущерб по наследуемым свойствам для объектов, в которые вложены другие объекты.

*Например, если при нарушении целостности базы данных ущерб будет 100 рублей, то нарушение целостности жесткого диска сервера вызовет ущерб равный сумме ущербу, появляющемуся при нарушении целостности базы данных, и стоимости самого устройства.*

В базовой конфигурации комплекса выделены свойства, представленные в таблице 2.2.

Таблица 2.2 – Свойства объектов

| **Свойство** | **Описание свойства** |
| --- | --- |
| Целостность | Целостность подразумевает соответствие состава и структуры используемого объекта требованиям выдвигаемым бизнес-процессами |
| Доступность | Доступность подразумевает наличие объекта в нужное время и в нужном месте |
| Конфиденциальность информации | Свойство конфиденциальности относится к информации и подразумевает некоторую ценность информации в силу неизвестности ее третьим лицам |
| Используемость по назначению | Данное свойство предполагает, что объект не используются для целей не определенных в бизнес-процессе |
| Владение | Владение подразумевает, что объект находится в распоряжении владельца, не потерян, не украден и т.п. |

* При анализе ущерба от объектов необходимо **не** **учитывать** возможное снижение ущерба за счет использования уже имеющихся контрмер. Все имеющиеся контрмеры должны быть внесены в программный комплекс и будут учтены при анализе.

Учитывая, что после нарушения свойств величина ущерба изменяется с течением времени и в общем случае эта зависимость не линейная, то величину ущерба необходимо определять в различные временные интервалы. В базовой конфигурации программного комплекса для каждого свойства величина ущерба должна заноситься:

* После часа.
* После одного дня.
* После трех дней.
* После десяти дней.
* После месяца.
* После полугода.
* После года.

Однако, возможно внесение дополнительных временных интервалов, что может потребоваться для повышения точности вычисления промежуточных значений.

*Пример формы, по которой возможно проведение сбора данных об ущербе, представлен в Приложении.*

*Пример результирующей функции ущерба представлен на рисунке* *2.1.*

Рисунок 2.1 – Пример функции ущерба для некоторого свойства некоторого объекта

Сводные параметры свойств представлены в таблице 2.3.

Таблица 2.3 – Сводные параметры свойств объектов

| **Параметр** | **Диапазон значений (ед. измерения)** | **Характеристика параметра** |
| --- | --- | --- |
| Необходимость восстановления ресурсов объектов  после нарушения свойства | «Да», «Нет» | После нарушения некоторых свойств требуется произвести восстановление объекта до штатной конфигурации. При нарушении таких свойств должны применяться контрмеры обеспечивающие восстановление.  В базовой конфигурации комплекса к таким свойствам отнесено свойство «целостности информации». |
| Величина ущерба | Положительное число (тыс. рублей) | Значения ущерба бизнесу в случае нарушения данного свойства объекта через заданные интервалы времени |

* 1. Угрозы

Причиной нарушения свойств является реализация угроз.

Угрозы, в общем случае:

* определяют свойства, к нарушению которых они ведут;
* зависят от типов объектов, на которые эти угрозы могут влиять.

Графическое отображение данных зависимостей показано на рисунке 2.2.

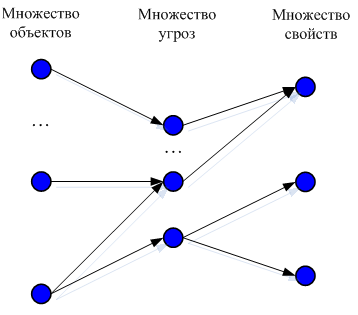


Рисунок 2.2 –Зависимости между угрозами, свойствами и объектами

Основной характеристикой угрозы является вероятность ее возникновения в отношении каждого объекта, а также степень влияния на ущерб свойствам объектов.

В базовой конфигурации комплекса внесены наиболее вероятные угрозы для некоторых типов объектов.

Сводные параметры угроз представлены в таблице 2.4.

Таблица 2.4 – Сводные параметры угроз

| **Параметр** | **Диапазон значений (ед. измерения)** | **Характеристика параметра** |
| --- | --- | --- |
| Вероятность реализации угрозы | от 0 до 1 (вероятность в год) | Вероятность реализации угроз определяет вероятность того, что угроза проявится в отношении объекта, с которым она связана, в течение года |
| Степень влияния на свойства объекта | от 0 до 1 (процент от ущерба за год) | Степень влияния на свойства объекта определяет процент от ущерба, который произойдет, в случае если угроза будет реализована в год |
| Свойства, на которые влияет | Все предопределенные свойства | Данный параметр определяет те свойства, к нарушению которых приводит реализация угрозы |

* При задании угроз необходимо соблюдать следующее правило – характеристики объекта угрозы должны соответствовать характеристикам угрозы

*Например, если рассматривается угроза кражи конкретного устройства, то вероятность реализации этой угрозы, тоже должна определяться в отношении данного устройства. Т.е. если вероятность кражи любого устройства в организации будет 0,1 (т.е. в организации в течение 10 лет произошла 1 кража), то, учитывая наличие в организации большого количества устройств, вероятность кражи конкретного устройства может быть в тысячи раз меньше.*

* 1. Контрмеры

Контрмеры, заданные в программном комплексе, обеспечивают:

* снижение уровня риска (например, задание в качестве контрмеры системы автоматического пожаротушения снижает вероятность возникновения пожара);
* уход от риска (например, задание в качестве контрмеры возможности отказа от использования сервиса удаленного доступа позволяет уйти от угроз, реализуемых мобильными пользователями);
* перенос риска (посредством, например, задания в качестве контрмеры мер по страхованию каких-либо рисков).

Все возможные контрмеры разделены на два типа:

* групповые – контрмеры, которые могут обеспечивать защиту сразу нескольких объектов (например, межсетевые экраны, системы обнаружения атак, обеспечивающие защиту групп АРМ и/или серверов);
* индивидуальные – контрмеры, которые применяются для защиты отдельных компонент (например, электронные замки, персональные антивирусные средства и т.п.).

Для каждой контрмеры определяют функции, которые эта контрмера выполняет для нейтрализации каждой из угроз, на которые действуют. Возможны следующие функции:

* обнаружение;
* нейтрализация;
* предотвращение;
* восстановление.

Для успешного воздействия на угрозу должен быть выполнен один из следующих сценариев:

* угроза должна быть предотвращена контрмерой реализующей функцию «предотвращение»;
* если угрозу не удалось предотвратить и нарушенное свойство объекта **требует** восстановления, угроза должна быть обнаружена (контрмерой реализующей функцию «обнаружение»), нейтрализована (контрмерой реализующей функцию «нейтрализация»), а объект должен быть восстановлен (контрмерой реализующей функцию «восстановление»);
* если угрозу не удалось предотвратить и нарушенное свойство объекта **не требует** восстановления, угроза должна быть обнаружена (контрмерой реализующей функцию «обнаружение»), нейтрализована (контрмерой реализующей функцию «нейтрализация»).

*Например, использование специальных жаропрочных конструкций снижает риск возникновения угрозы, т.е. данная контрмера реализует функцию «предотвращение».*

*Другой случай: при возникновении пожара сработала пожарная сигнализация, затем пожар был потушен пожарной командой, после чего потерянные данные были восстановлены с помощью резервных копий. В данном случае присутствуют три контрмеры реализующие функции «обнаружения», «нейтрализации», «восстановления».*

Функции, которые реализуют контрмеры, и зависимости между ними могут быть представлены в виде ориентированного графа, в котором дуги есть функции, узлы результат выполнения типовых функций.

*Пример такого графа представлен на рисунке* 2*.3.*

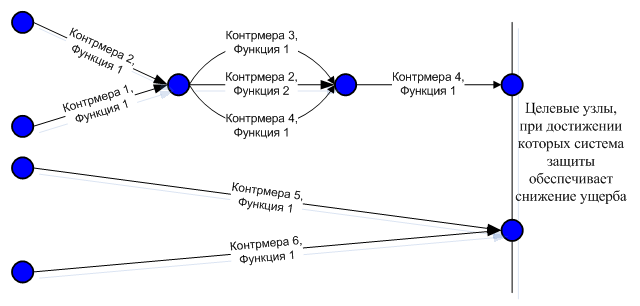


Рисунок 2.3 – Пример графа функций

В программном комплексе, возможно, определение зависимостей между контрмерами, реализующими функции «обнаружение» и «нейтрализация». Т.е. можно связать, например, следующие контрмеры – срабатывание пожарной сигнализации и тушение пожара пожарной командой. Дополнительно связывать контрмеры реализующие функцию «восстановление» не является необходимым.

Множество контрмер, которое можно задать в программном комплексе, не ограничено. К контрмерам могут быть отнесены любые организационные, правовые, организационно-технические, технические меры и средства, в том числе:

* организация круглосуточной охраны помещений, зданий, транспортируемых грузов;
* организация защищенного документооборота;
* периодические проверки пользователей и администраторов на лояльность;
* установка дверей, решеток;
* резервирование оборудования, помещений, каналов связи, поставщиков;
* системы разграничения доступа, как встроенные в прикладное и системное ПО, так и внешние;
* системы обнаружения мошенничества;
* межсетевые и персональные сетевые экраны;
* антивирусные средства;
* прокси-сервера;
* системы аудита и мониторинга действий;
* системы обнаружения и предотвращения атак;
* механизмы контроля целостности данных;
* организация опечатывания системных блоков;
* средства криптографической защиты;
* системы обнаружения мошенничества;
* обманные системы и ловушки;
* системы ручного и автоматического пожаротушения;
* системы охранно-пожарной сигнализации;
* системы видеонаблюдения;
* средства и системы гарантированного электроснабжения;
* защитные кожухи, чехлы, кабель каналы;
* различные виды замков – механические, кодовые, биометрические;
* использование сторонних организаций предлагающих услуги по снижению ущерба от некоторых угроз (например, ремонтные организации, страховые организации, осуществляющие страхование рисков) и т.д. и т.п.

Контрмеры, в общем случае, зависят от:

* типов объектов, к которым они могут быть применены;
* множества угроз, на которые они влияют.

Сводные параметры контрмер представлены в таблице 2.5.

Таблица 2.5 – Сводные параметры контрмер

| **Параметр** | **Диапазон значений (ед. измерения)** | **Характеристика параметра** |
| --- | --- | --- |
| *Основные характеристики* |  |  |
| Тип контрмеры | «Индивидуальная», «Групповая» | Данный параметр определяет будет ли контрмера применена один раз для защиты группы объектов или несколько раз для защиты каждого объекта (если она индивидуальная) |
| Контролируемые свойства объектов | Все предопределенные свойства | Данный параметр определяет те свойства объектов, защиту которых обеспечить данная контрмера |
| Вероятность не работоспособности | от 0 до 1 | Вероятность работоспособности определяет вероятность того, что контрмера будет работоспособна в некоторый момент времени |
| *Стоимостные характеристики* |  |  |
| Время необходимое на обслуживание персоналом категории I | Положительное число (чел/часов в год) | Затраты времени на обслуживание контрмеры, например, обслуживание системы автоматического пожаротушения специалистами |
| Стоимость чел/часа персонала категории I | Положительное число (тыс. рублей за 1 чел/час) | Стоимость одного часа времени специалиста, трудозатраты которого определены выше |
| Время необходимое на обслуживание персоналом категории II | Положительное число (чел/часов в год) | Затраты времени на обслуживание контрмеры специалистами другой категории (с другим размером оплаты труда) |
| Стоимость чел/часа персонала категории II | Положительное число (тыс. рублей за 1 чел/час) | Стоимость одного часа времени специалиста, трудозатраты которого определены выше |
| Дополнительные затраты в год | Положительное число (тыс. рублей в год) | Ежегодные затраты, которые не учтены в других статьях затрат, например, затраты на электроэнергию, обслуживание и т.п. |
| Арендная стоимость в год | Положительное число (тыс. рублей в год) | Ежегодные затраты на аренду контрмеры, услуг и т.п. |
| Стоимость ввода в действие | Положительное число (тыс. рублей) | Единовременные затраты на покупку, установку, настройку контрмеры и т.п. |
| Стоимость лицензии на один защищаемый групповой контрмерой объект | Положительное число (тыс. рублей на один объект) | Единовременные затраты, позволяющие отразить зависимость стоимости групповой контрмеры от количества объектов, которые она защищает |
| Затраты, возникающие в случае проявления угрозы (тыс.) | Положительное число (тыс. рублей) | Переменные затраты, которые могут возникнуть если угроза произойдет, например, стоимость вызова ремонтной организации при обрыве кабеля |
| *Функции контрмеры* |  |  |
| Функции контрмеры в отношении каждой из угроз | Обнаружение, нейтрализация, предотвращение, восстановление | Перечень функций реализуемых контрмерой в отношении каждой из угроз, например, пожарная сигнализация реализует функцию «обнаружение» в отношении такой угрозы, как пожар |
| *Показатели функций* |  |  |
| Время, необходимое на обнаружение угрозы | Положительное число (дней) | Время, необходимое контрмере для реализации функции «обнаружение» в отношении выбранной угрозы |
| Время, необходимое на нейтрализацию угрозы | Положительное число (дней) | Время, необходимое контрмере для реализации функции «нейтрализация» в отношении выбранной угрозы |
| Вероятность не обнаружения угрозы | от 0 до 1 | Вероятность **не реализации** контрмерой функции «обнаружение» в отношении выбранной угрозы |
| Вероятность не нейтрализации угрозы | от 0 до 1 | Вероятность **не реализации** контрмерой функции «нейтрализация» в отношении выбранной угрозы |
| Вероятность не предотвращения угрозы | от 0 до 1 | Вероятность **не реализации** контрмерой функции «предотвращение» в отношении выбранной угрозы |
| Время ввода контрмеры восстановления в действие | Положительное число (дней) | Время, необходимое контрмере для начала работы контрмеры на «восстановление» после нарушения свойства. Данное время, например, связано, с необходимостью подключения дополнительного оборудования, настройки параметров восстановления |
| Стоимость восстановления единицы ресурса | Положительное число (тыс. рублей на ед.) | Характеристика контрмеры, позволяющая отразить зависимость стоимости контрмеры восстановления от объема ресурсов подлежащих восстановлению. Например, стоимость средств восстановления информации принято сравнивать по такому показателю, как рубль/Мбайт.  Единицей ресурса–информации в программном комплексе является Мбайт. Показатель используется для расчета стоимости владения контрмерой. |
| Время, необходимое на восстановление единицы ресурса | Положительное число (дней) | Время, необходимое контрмере для восстановления единицы ресурса. Данное время используется при расчете стоимости остаточного ущерба, связанного с недоступностью системы до момента восстановления всех ресурсов.  Единицей ресурса – информации в программном комплексе является Мбайт. |
| *Зависимости* |  |  |
| Связанные контрмеры обнаружения | Все предопределенные контрмеры обнаружения | Показатель характеризует возможность задания связей между контрмерами. В данном случае, для рассматриваемой контрмеры нейтрализации будут отражаться все возможные контрмеры обнаружения. Например, если рассматриваемая контрмера – система пожаротушения, то связанной контрмерой обнаружения может выступать система пожарной сигнализации |
| Связанные контрмеры нейтрализации | Все предопределенные контрмеры нейтрализации | Показатель обратный к предыдущему. В данном случае для рассматриваемой контрмеры обнаружения будут отражаться все возможные контрмеры нейтрализации |

* При задании контрмер необходимо соблюдать следующее правило – характеристики контрмеры должна соответствовать характеристикам защищаемых объектов и угроз.

*Например, если рассматривается угроза кражи конкретного устройства «X», то и вероятность обнаружения, нейтрализации и т.п. этой угрозы контрмерой, тоже должна рассчитываться исходя из того, что должна быть предотвращена не любая кража, а именно эта.*

* 1. Проекты

Проект – это конкретный набор объектов, для которых производится расчет оптимальной системы защиты.

Перед созданием проекта определяются:

* все возможные свойства объектов;
* все возможные угрозы;
* все возможные контрмеры;
* все типы объектов, которые будут существовать в проекте.

Сводные параметры проектов представлены в таблице 2.6.

Таблица 2.6 – Сводные параметры проектов

| **Параметр** | **Диапазон значений (ед. измерения)** | **Характеристика параметра** |
| --- | --- | --- |
| Период | Целое положительное число (годы) | Данный параметр определяет промежуток времени, на который создается система и на который будет рассчитана полная стоимость системы защиты |
| Перечень объектов входящих в проект |  | Приводимые в проекте параметры объектов описаны в разделе 2.2.  Для каждого объекта приводится:   * наименование; * свойства данного объекта; * ущерб по каждому свойству; * количество аналогичных объектов в проекте; * тип объекта; * объем защищаемых ресурсов объекта. |

1. Порядок работы с программным комплексом
   1. Общий порядок

Работа с программным комплексом включает следующие этапы:

* Определение всех возможных свойств объектов.
* Определение всех возможных угроз.
* Определение всех возможных контрмер.
* Определение всех возможных типов объектов безопасности.
* Управление проектом.
* Расчет проекта, получение результатов.
* Экспорт результатов.
  1. Определение всех возможных свойств объектов

Определение всех возможных свойств объектов производится в следующем порядке:

1. В главном окне программы (см. рис 3.1) нажмите кнопку «Справочная подсистема».

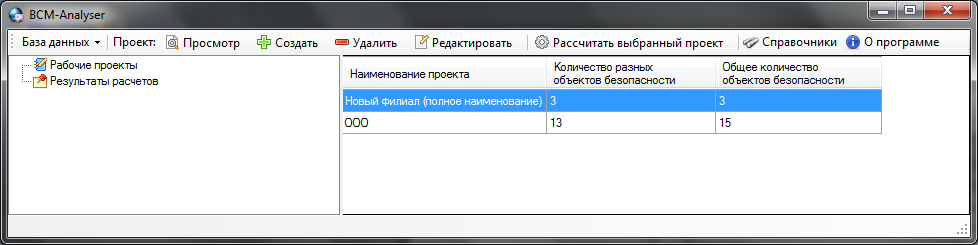


Рисунок 3.1 – Главное окно программы

1. В левом окне открывшегося «Редактора справочников» выберите пункт «Свойства объектов» (см. рис. 3.2).

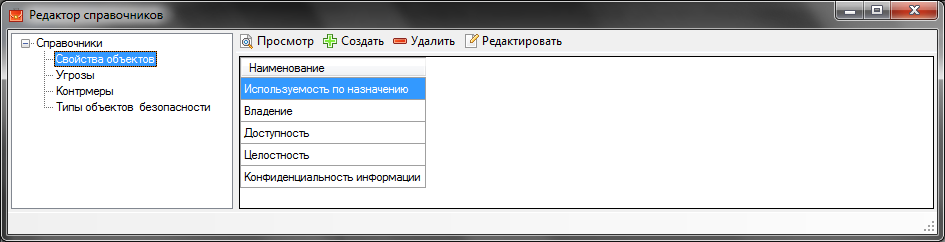


Рисунок 3.2 – Выбор пункта «Свойства объектов»

1. В правой части экрана, вы можете:

* просмотреть выбранное свойство, выделив его в правом окне «Редактора справочников» и нажав кнопку view.gif;
* добавить новое свойство нажатием кнопки add.gif;
* удалить имеющееся свойство, выделив его в правом окне «Редактора справочников» и нажав кнопку del.gif;
* редактировать имеющееся свойство, выделив его в правом окне «Редактора справочников» и нажав кнопку edit.gif.

1. При задании нового свойства (см. рис. 3.3) определяются следующие параметры:

* имя свойства;
* необходимость восстановления ресурсов объектов после нарушения данного свойства (установкой соответствующей галочки).

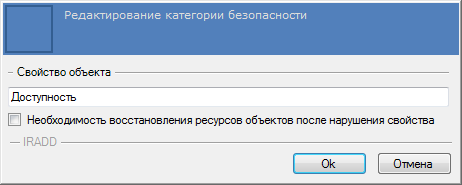


Рисунок 3.3 – Диалоговое окно задания нового свойства

1. Для сохранения введенных параметров нажмите кнопку «Сохранить».
   1. Определение всех возможных угроз

Определение всех возможных угроз производится в следующем порядке:

1. В левом окне «Редактора справочников» выберите пункт «Угрозы» (см. рис. 3.4).

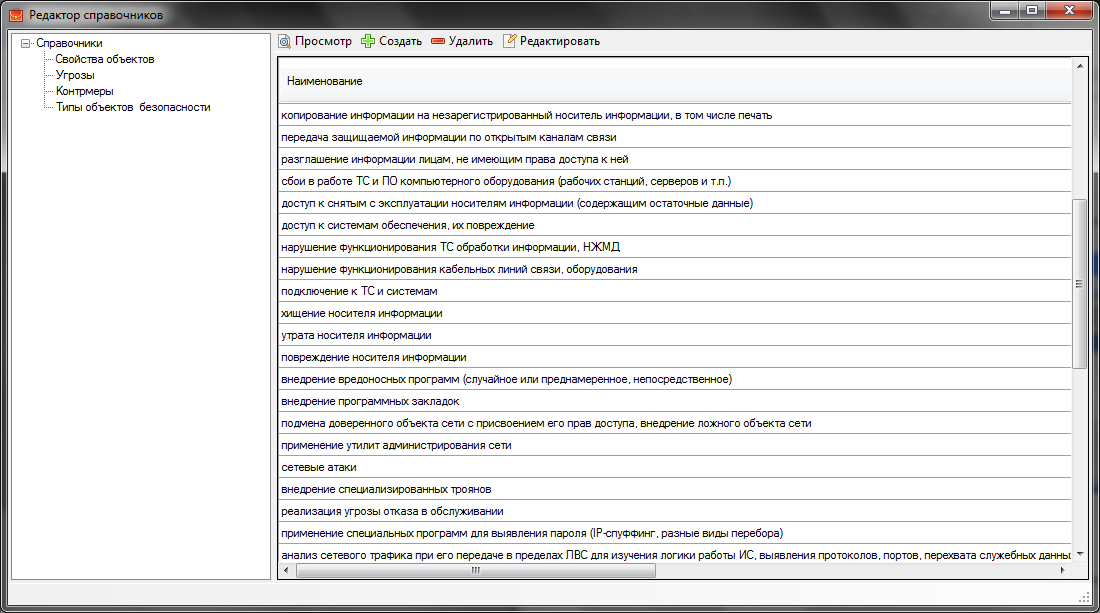


Рисунок 3.4 – Выбор пункта «Угрозы»

1. В правой части экрана, вы можете:

* просмотреть выбранную угрозу, выделив ее в правом окне «Редактора справочников» и нажав кнопкуview.gif;
* добавить новую угрозу нажатием кнопки add.gif;
* удалить имеющуюся угрозу, выделив ее в правом окне «Редактора справочников» и нажав кнопку del.gif;
* редактировать имеющуюся угрозу, выделив ее в правом окне «Редактора справочников» и нажав кнопку edit.gif.

1. При задании новой угрозы (см. рис. 3.5) определяются следующие параметры:

* имя угрозы;
* свойства, нарушение которых вызывает данная угроза в случае своей реализации;
* вероятность возникновения угрозы.

1. Для сохранения введенных параметров нажмите кнопку «Сохранить».

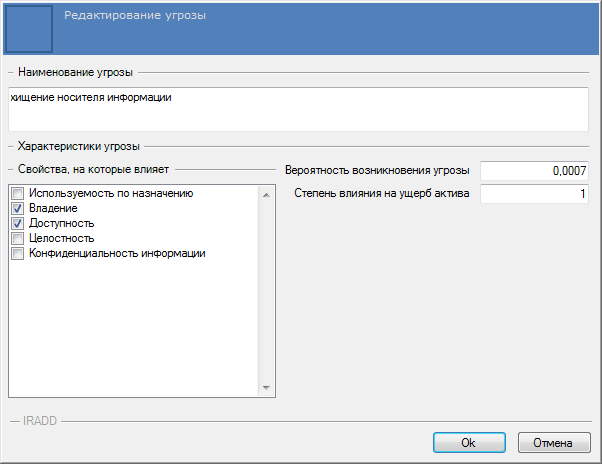


Рисунок 3.5 – Диалоговое окно задания новой угрозы

* 1. Определение всех возможных контрмер

Определение всех возможных контрмер производится в следующем порядке:

1. В левом окне «Редактора справочников» выберите пункт «Контрмеры» (см. рис. 3.6).

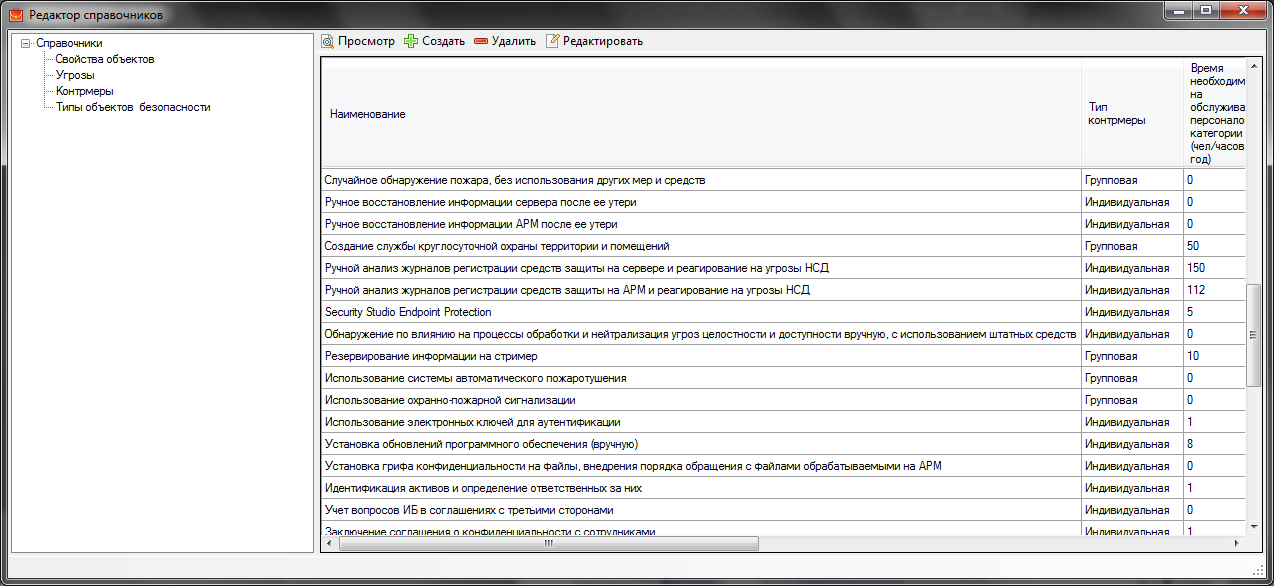


Рисунок 3.6 – Выбор пункта «Контрмеры»

1. В правой части экрана, вы можете:

* просмотреть выбранную контрмеру, выделив ее в правом окне «Редактора справочников» и нажав кнопкуview.gif;
* добавить новую контрмеру нажатием кнопки add.gif;
* удалить имеющуюся контрмеру, выделив ее в правом окне «Редактора справочников» и нажав кнопку del.gif;
* редактировать имеющуюся контрмеру, выделив ее в правом окне «Редактора справочников» и нажав кнопку edit.gif.

1. Задание новой контрмеры, после нажатия кнопки add.gif, производится в следующем порядке:

* на вкладке «Основные характеристики» контрмеры (см. рис. 3.7) определяется:
  + имя контрмеры;
  + свойства, защиту которых обеспечивает данная контрмера (указывается галочками в поле «Контролируемые свойства объектов»);
  + тип контрмеры – индивидуальная, либо групповая;
  + вычисленное значение вероятности не работоспособности (вводится через запятую в поле «Вероятность не работоспособности»).
  + ежегодные затраты на контрмеру;
  + единовременные затраты на контрмеру;
  + затраты возникающие в случае реализации угрозы.

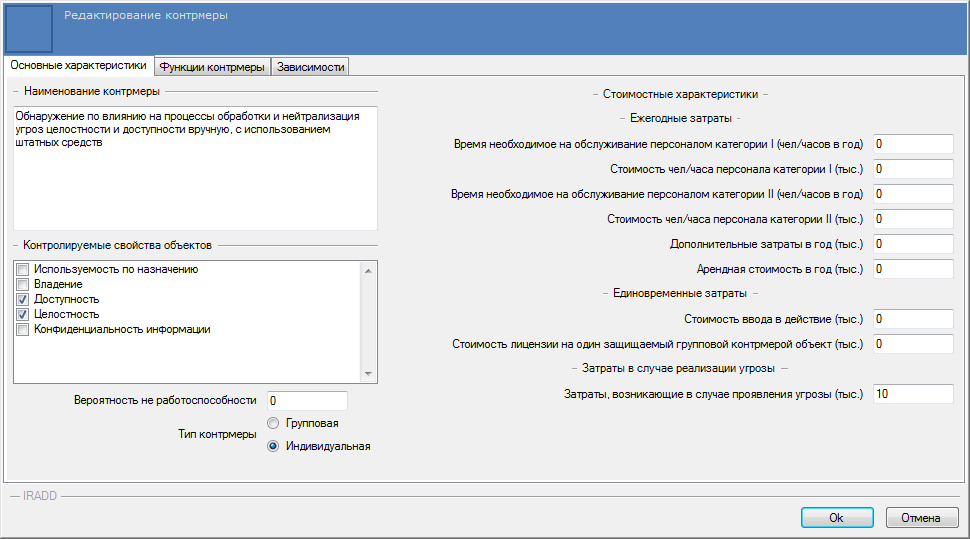


Рисунок 3.7 – Вкладка «Основные характеристики» новой контрмеры

Подробнее о значениях затрат см. раздел 2.5.

* на вкладке «Функции контрмеры» (см. рис. 3.8) производится задание функций контрмеры в отношении каждой угрозы, на которую данная контрмера действует, в следующем порядке:

1. в левой части окна, из списка возможных угроз, выделяется угроза, на которую действует контрмера, производится подтверждение выбора, нажатием кнопки add.gif;
2. в левой части окна, снизу ставятся галочки напротив функций, которые реализует контрмера, в отношении выделенной на предыдущее шаге угрозы;
3. производится сохранение функций контрмеры в отношении угрозы нажатием кнопки «Сохранить функции»;
4. шаги 1-3 повторяются для каждой угрозы, на которую действует контрмера.
5. в правой части окна производится задание показателей функций контрмеры (по угрозам и функциям, выбранным на предыдущем этапе), в следующем порядке:
   * для контрмер реализующих функции «Обнаружения» или «Нейтрализации» или «Предотвращения»:
6. из списка заданных ранее угроз, выделяется угроза, для которой планируется задать показатели;
7. указываются конкретные значения функций «Обнаружения», «Нейтрализации», «Предотвращения» - время, необходимое на выполнение каждой функции, вероятность не выполнения функций (подробнее про показатели функций см. раздел 2.5);
8. производится сохранение показателей функций контрмеры в отношении угрозы нажатием кнопки «Сохранить эффект»;
9. шаги 1-3 повторяются для каждой угрозы, на которую действует контрмера.
   * для контрмер реализующих функцию «Восстановления» в нижней части окна указываются характеристики функции восстановления.

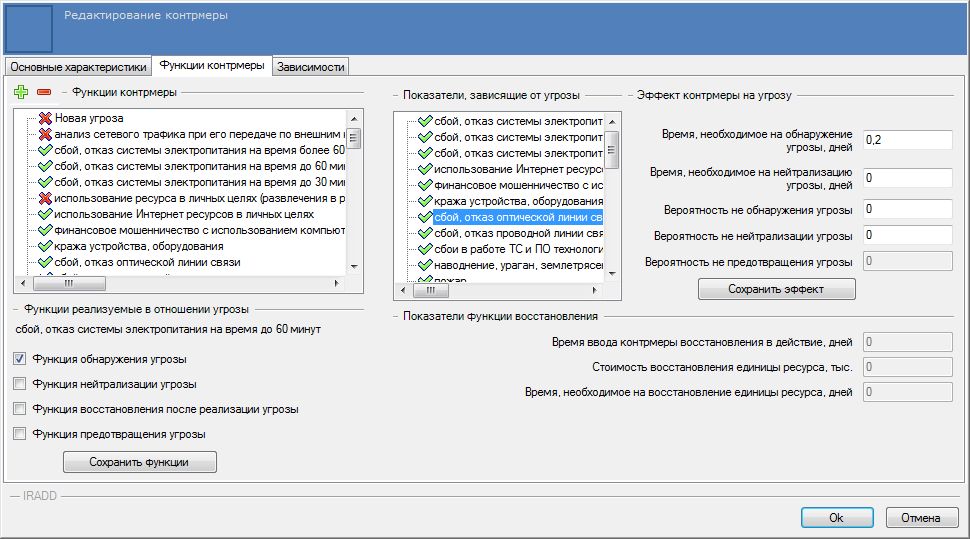


Рисунок 3.8 – Вкладка «Функции контрмеры»

* на вкладке «Зависимости» (см. рис. 3.9) производится задание связей с другими контрмерами (подробнее про связи контрмер см. раздел 2.5), в следующем порядке:
  + для контрмер реализующих функцию «Обнаружения»:

1. в правой части окна (см. заголовок «Связанные контрмеры нейтрализации») показываются все контрмеры нейтрализации, которые потенциально могут использовать результат выполнения функции «Обнаружения» для нейтрализации угрозы. Из данных контрмер производится выделение необходимой контрмеры и нажимается кнопка add.gif;
2. производится повтор шага 1 для каждой связанной контрмеры нейтрализации.
   * для контрмер реализующих функцию «Нейтрализации»:
3. в левой части окна (см. заголовок «Связанные контрмеры обнаружения») показываются все контрмеры обнаружения, результат выполнения которых потенциально может использовать рассматриваемая контрмера для выполнения функции «Нейтрализация». Из данных контрмер производится выделение необходимой контрмеры и нажимается кнопка add.gif;
4. производится повтор шага 1 для каждой связанной контрмеры обнаружения.

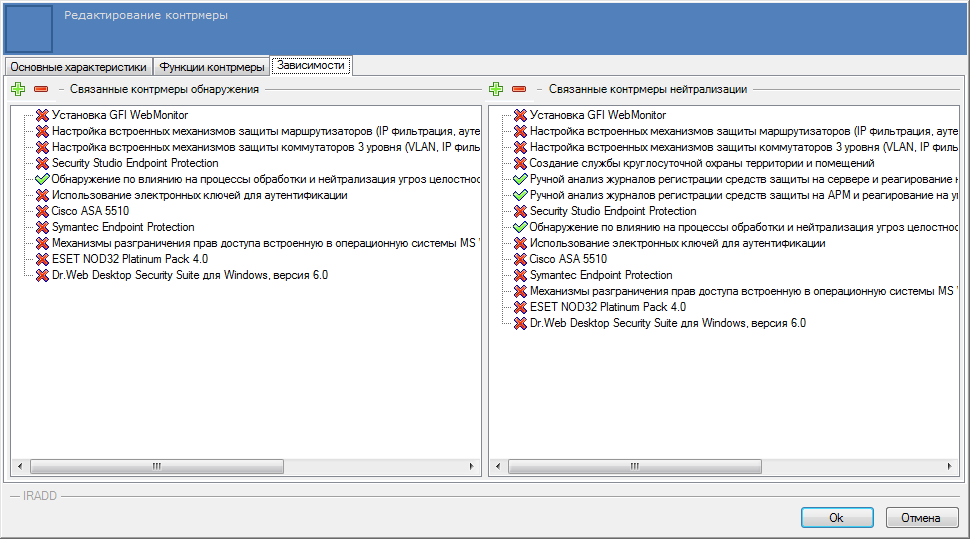


Рисунок 3.9 – Вкладка «Зависимости» новой контрмеры

* Для сохранения введенных параметров новой контрмеры нажмите кнопку «Сохранить».
  1. Определение всех возможных типов объектов безопасности

Определение всех возможных типов объектов производится в следующем порядке:

1. В левом окне «Редактора справочников» выберите пункт «Типы объектов безопасности» (см. рис. 3.10).

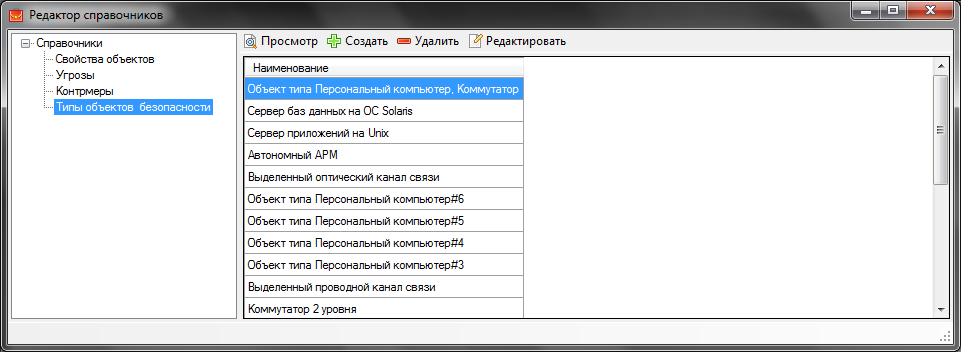


Рисунок 3.10 – Выбор пункта «Типы объектов безопасности»

1. В правой части экрана, вы можете:

* просмотреть выбранный тип объекта, выделив его в правом окне «Редактора справочников» и нажав кнопкуview.gif;
* добавить новый тип объекта нажатием кнопки add.gif;
* удалить имеющийся тип объекта, выделив его в правом окне «Редактора справочников» и нажав кнопку del.gif;
* редактировать имеющийся тип объекта, выделив его в правом окне «Редактора справочников» и нажав кнопку edit.gif.

1. Задание нового типа объекта, после нажатия кнопки add.gif, производится в следующем порядке (см. рис. 3.11):

* указывается имя нового типа объекта безопасности;
* в левой части окна (заголовок «Возможные контрмеры») определяются контрмеры, которые применимы для данного типа объекта безопасности, в следующем порядке:
  + выделяется применимая контрмера;
  + производится нажатие кнопки add.gif.
* в правой части окна (заголовок «Действующие на данный тип объекта угрозы») определяются угрозы, которые могут действовать на данный тип, в следующем порядке:
  + выделяется действующая угроза;
  + производится нажатие кнопки add.gif.

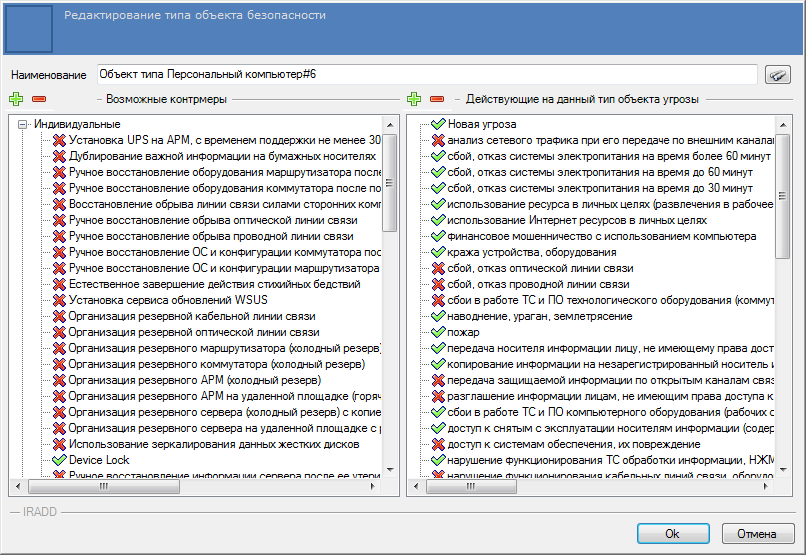


Рисунок 3.11 – Окно задания нового типа объекта безопасности

* в случае если типы объектов были импортированы из системы «Privacy-SPS» или «SIS-Analyser», то при нажатии кнопки  появляется окно показывающее список активов, которым был присвоен данный тип (см. рис. 3.11)

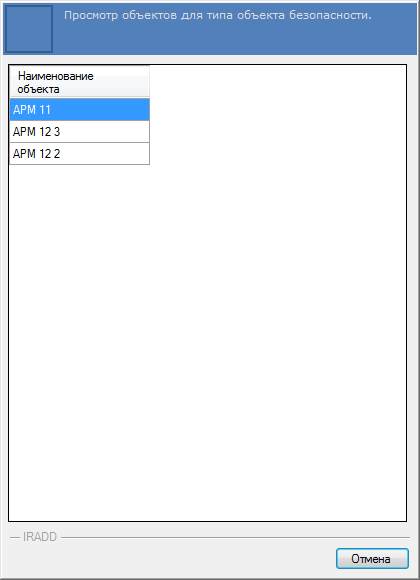


Рисунок 3.12 – Окно просмотра активов входящих в тип объекта

* После задания всех применимых контрмер и действующих угроз производится сохранение типа объекта нажатием кнопки «Сохранить».
  1. Управление проектом

Управление проектом производится в следующем порядке:

1. Отображение всех существующих проектов производится в главном окне программы (см. рис 3.13).

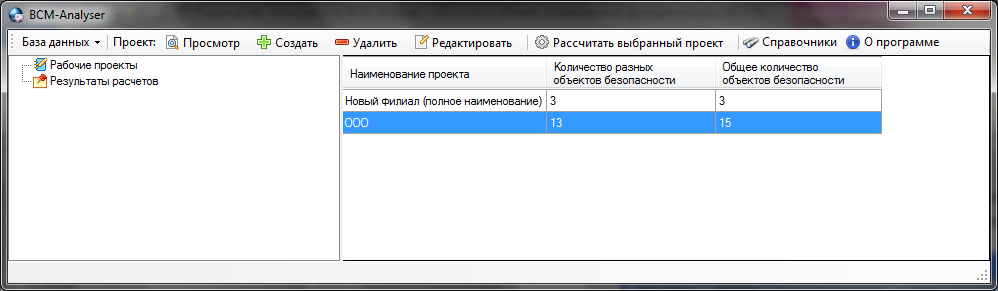


Рисунок 3.13 – Главное окно программы, перечень проектов

1. В правой части экрана, вы можете:

* просмотреть выбранный проект, выделив его в правой части главного окна программы и нажав кнопкуview.gif;
* добавить новый проект нажатием кнопки add.gif;
* удалить имеющийся проект, выделив его в правой части главного окна программы и нажав кнопку del.gif;
* редактировать имеющийся проект, выделив его в правой части главного окна программы и нажав кнопку edit.gif.

1. В строке меню, при нажатии кнопки «База данных\Синхронизировать с Privacy-SPS») осуществляется импорт из системы «Privacy-SPS» или «SIS-Analyser»:

* проектов. При этом в отдельные проекты выделяются активы, отнесенные к основной организации и филиалам,
* активов,
* значений ущерба данным активам,
* автоматическое создание типов объектов посредством определения применимости угроз и контрмер в отношении тех или иных активов.

1. Задание нового проекта, после нажатия кнопки add.gif, производится в следующем порядке (см. рис. 3.14):

* указывается имя нового проекта;
* указывается период (в годах), для которого будет производиться расчет стоимости рисков, стоимости владения и эксплуатации контрмер (в поле «Период»);

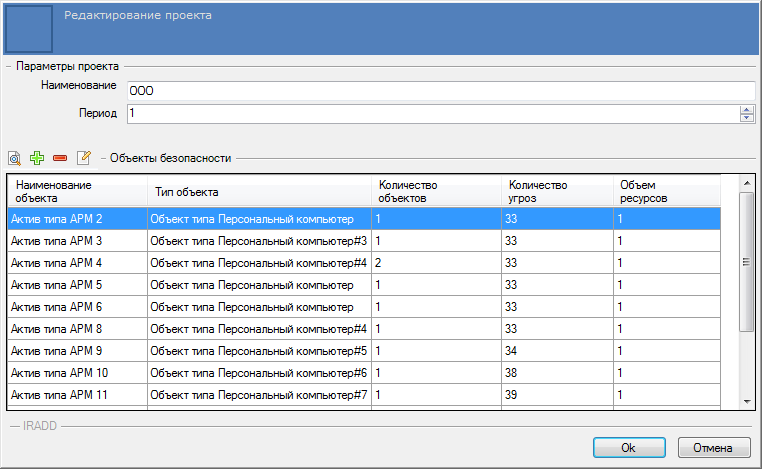


Рисунок 3.14 – Окно создания нового проекта

* производится задание объектов входящих в проект (подробнее про характеристики объектов, см. раздел 2.2), в следующем порядке:

1. в нижней части главного окна программы, нажатием кнопки add.gif, производится открытие окна задания нового объекта (см. рис. 3.15);
2. указывается имя нового объекта (в поле «Наименование объекта безопасности»);

*Например, в качестве имени такого объекта может выступать «АРМ оператора Call-центра».*

1. задается количество объектов имеющих аналогичные характеристики в проекте;

*Например, учитывая, что, как правило, функции на АРМ операторов Call-центра одинаковы, эти АРМ можно считать идентичными и задать их в проекте один раз – указав характеристики любого такого АРМ и общее количество таких АРМ в Call-центре.*

1. в случае если объекты были импортированы из системы «Privacy-SPS» или «SIS-Analyser», то при нажатии кнопки  появляется окно показывающее список типовых активов, которые входят в данный объект;
2. указывается тип данного объекта безопасности из типов заданных в разделе 3.5;

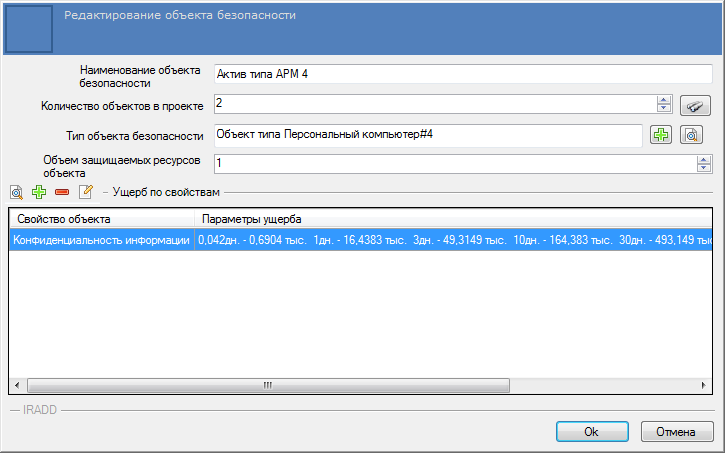


Рисунок 3.15 – Окно задания нового объекта в проекте

1. указывается объем защищаемых ресурсов объекта, которые будет необходимо восстанавливать в случае реализации соответствующих угроз;

*В отношении АРМ оператора Call-центра таким объемом может быть объем ценной информации, которая хранится на данном АРМ (в Мбайт).*

1. задаются все свойства объекта, которым может быть нанесен ущерб, нажатием кнопки add.gif, в разделе «Ущерб по свойствам». В появившемся окне (см. рис. 3.16) выбираются свойства (из определенных на этапе 2.3) и задается ущерб по данным свойствам (по каждому временному интервалу). После задания каждого свойства и ущерба по нему, свойство объекта сохраняется нажатием кнопки «Сохранить»;

*Например, реализация вирусной атаки на АРМ оператора Call-центра, при условии отсутствия контрмер, может привести к простою и постоянному наращиванию величины ущерба компании за простой. Если ущерб через 1 час будет 1 рубль, то через 3 часа уже может быть равен 3 рублям, через рабочий день 8 рублям и т.д.*

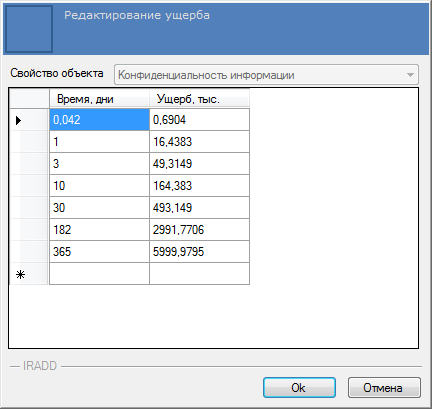


Рисунок 3.16 – Окно задания свойства объекта

1. после задания всех характеристик объекта производится его сохранение нажатием кнопки «Ок»;
2. для каждого объекта, который необходимо внести в проект, повторяются этапы 1-7;

* после задания всех объектов проекта и характеристик проекта, проект сохраняется нажатием кнопки «Сохранить».
  1. Расчет проекта, получение результатов

Расчет проекта, получение результатов производится в следующем порядке:

1. В главном окне программы (см. рис 3.13) выделяется проект, для которого необходимо подобрать оптимальную систему защиты.
2. После выделения проекта производится нажатие кнопки «Рассчитать выбранный проект». После нажатия кнопки и до получения результата, показывается предупреждающее окно «Идет расчет, ожидайте…».

* Во время проведения расчета, действия по редактированию данных проекта будут заблокированы. Обратите внимание, что расчет даже одного объекта проекта занимает порядка 5 секунд (время расчета также сильно зависит от количества контрмер действующих на данный объект), т.е. при большом количестве объектов (и контрмер) время пропорционально увеличивается.

1. После проведения расчета появится окно с результатами расчета (см. рис. 3.17). В окне «Результаты расчетов» показываются следующие данные:

* наименование проекта, для которого произведен расчет;
* для оптимального варианта системы защиты и варианта без контрмер:
  + стоимость остаточного риска в целом для системы;
  + стоимость остаточного ущерба для оптимального набора контрмер;
  + стоимость владения оптимальным набором контрмер;
  + общая стоимость системы защиты, как сумма остаточного риска, остаточного ущерба и стоимости владения набором контрмер;
* перечень объектов проекта, с указанием учтенных при выборе и выбранных контрмер в виде дерева (см. вкладку «Обычный вид» в нижней части окна);
* перечень объектов проекта, с указанием учтенных при выборе и выбранных контрмер в виде текста (см. вкладку «В виде текста» в нижней части окна).

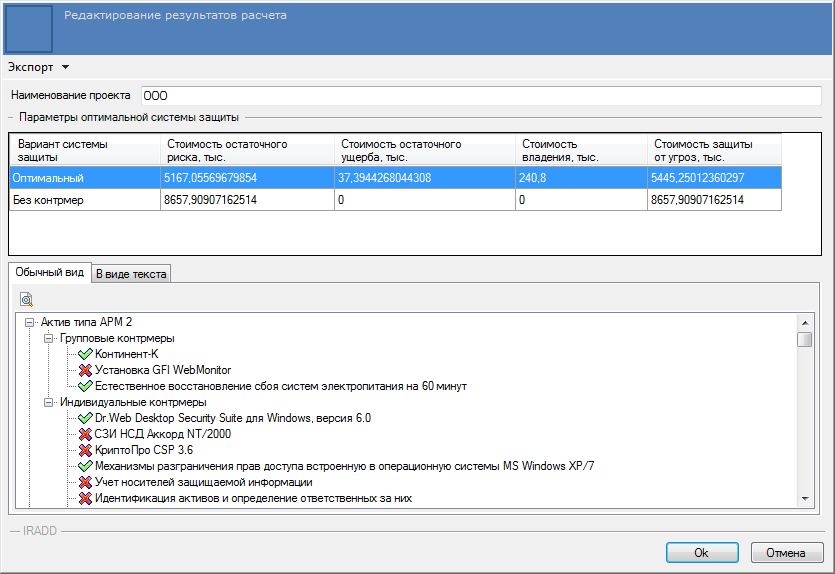


Рисунок 3.17 – Окно с результатами расчета

1. Результаты расчета можно сохранить, нажав кнопку «Сохранить». Результаты сохраненных расчетов можно просмотреть, выбрав пункт «Результаты расчетов» главного окна программы.

* Обратите внимание, что изменив множество возможных свойств, угроз, контрмер, типов объектов, новый расчет того же проекта, даст другие результаты, учитывающие внесенные изменения. Доступ к предыдущему сохраненному расчету возможен будет только в режиме просмотра на вкладке «Результаты расчетов» главного окна программы.
  1. Экспорт результатов

Экспорт результатов расчета проекта, производится из окна «Результаты расчетов» (см. рис. 3.18) в следующем порядке:

1. В левом верхнем углу окна нажимается вкладка «Экспорт».
2. В выпадающем меню «Экспорт» требуется выбрать необходимый формат файла экспорта:

* «Excel», если необходим экспорт в файл формата MS Excel 2003 (.xls);
* «Text», если необходим экспорт в стандартный текстовый формат (.txt).

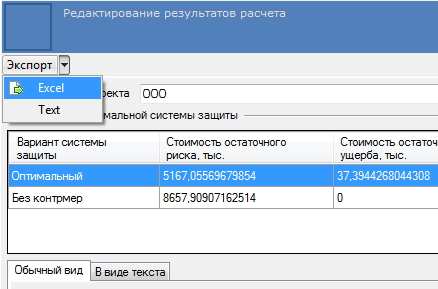


Рисунок 3.18 – Окно с результатами расчета

1. При экспорте в формат MS Excel 2003, автоматически открывается окно MS Excel с результатами экспорта, а исходный файл сохраняется в каталог «Reports» в корневом каталоге программы. При экспорте в текстовый формат выдается диалоговое окно сохранения файла.

Термины и определения

|  |  |
| --- | --- |
| Контрмера | Меры и средства позволяющие реализовать какую-либо стратегию управления риском |
| Обработка риска | Процесс выбора и осуществления мер по модификации риска |
| Объект безопасности (объект) | Объект физического мира, актив (оборудование, производственная площадь, люди или другой ресурс), используемый при выполнении бизнес-процесса и нарушение свойств которого может нанести ущерб бизнес-процессу |
| Остаточный риск | Риск, остающийся после его обработки |
| Остаточный ущерб | Ущерб, являющийся следствием использования контрмер для обработки риска. Остаточный ущерб связан с возможными затратами на контрмеру, возникающими при проявлении угрозы, либо частичным ущербом от угрозы, который появляется, если контрмера срабатывает на угрозу с некоторым запозданием |
| Проект | Совокупность объектов и их свойств, для которых строится система защиты |
| Свойство объекта | Характеристика объекта, от состояния которой зависит возможность эффективного использования объекта для осуществления рассматриваемого вида деятельности |

Приложение – Пример формы сбора данных об ущербе

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Наименование объекта:** |  | | | | | | |
| **Название вида ущерба** | **Величина ущерба при нарушении конфиденциальности, руб.** | | | | | | |
| 1 час | 1 день | 3 дня | 10 дней | 1 мес. | 6 мес. | 1 год |
| недополученная прибыль |  |  |  |  |  |  |  |
| увеличение затрат на сотрудников |  |  |  |  |  |  |  |
| увеличение выплат на социальные нужды |  |  |  |  |  |  |  |
| дополнительные затраты на материалы, энергию, сырье и т.п. |  |  |  |  |  |  |  |
| судебные издержки |  |  |  |  |  |  |  |
| дополнительные командировочные и представительские расходы |  |  |  |  |  |  |  |
| пени, неустойки, штрафы |  |  |  |  |  |  |  |
| **Название вида ущерба** | **Величина ущерба при нарушении целостности, руб.** | | | | | | |
| 1 час | 1 день | 3 дня | 10 дней | 1 мес. | 6 мес. | 1 год |
| недополученная прибыль |  |  |  |  |  |  |  |
| увеличение затрат на сотрудников |  |  |  |  |  |  |  |
| увеличение выплат на социальные нужды |  |  |  |  |  |  |  |
| дополнительные затраты на материалы, энергию, сырье и т.п. |  |  |  |  |  |  |  |
| судебные издержки |  |  |  |  |  |  |  |
| дополнительные командировочные и представительские расходы |  |  |  |  |  |  |  |
| пени, неустойки, штрафы |  |  |  |  |  |  |  |
| **Название вида ущерба** | **Величина ущерба при нарушении доступности, руб.** | | | | | | |
| 1 час | 1 день | 3 дня | 10 дней | 1 мес. | 6 мес. | 1 год |
| недополученная прибыль |  |  |  |  |  |  |  |
| увеличение затрат на сотрудников |  |  |  |  |  |  |  |
| увеличение выплат на социальные нужды |  |  |  |  |  |  |  |
| дополнительные затраты на материалы, энергию, сырье и т.п. |  |  |  |  |  |  |  |
| судебные издержки |  |  |  |  |  |  |  |
| дополнительные командировочные и представительские расходы |  |  |  |  |  |  |  |
| пени, неустойки, штрафы |  |  |  |  |  |  |  |

1. Описание проектов приведено в разделе 2.6 [↑](#footnote-ref-1)