

ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО ПРОДУКТА ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Курманбай А.К., студентка гр.17В41, IV курс
Научный руководитель: Разумников С.В., старший преподаватель
Юргинского технологического института (филиал)
Томского политехнического университета
Г. Юрга

Проблема обеспечения информационной безопасности (ИБ) современных автоматизированных и информационных технологиях (ИТ) является одной из самых важных. Сложность этих систем, разветвленность составляющих их основу компьютерных сетей еще больше усугубляют ситуацию.

Важность этого направления заключается, прежде всего, в обосновании необходимости применения тех или иных средств обеспечения уровня информационной безопасности и способов их использования, а также в определении их достаточности или недостаточности для определенных информационных систем и информационных технологий.

Сегодня не вызывает сомнений необходимость вложений в обеспечение информационной безопасности современных систем.

Основной вопрос – это как оценить и учесть уровень информационной безопасности при внедрении ИТ.

Целью данной работы является проектирование информационной системы, для автоматизации деятельности организации по оценке уровня ИБ программных продуктах.

На основе разработанной интегральной модели оценки информационной безопасности информационных технологий. Разработанная интегральная модель оценки ИБ эффективно выполняет свои задачи при определении рисков и соответствия новым требованиям постоянно обновляющейся ИТ.

Внедрение разрабатываемой ИС в практику работы организации позволит обеспечить:

- Централизованную регистрацию и учёт сведений об используемых или внедряемых ИТ;
- Оценка уровня ИБ ИТ по различным критериям и показателям;
- Расчет интегрального показателя ИБ;
- Организовать централизованное администрирование системы;
- Повышение качества внедряемых ИТ и уровня ИБ.

Предметной областью данной системы является сфера оценки и учета уровня ИБ программных продуктов.

Анализируется система критериев и показателей для оценки ИБ при внедрении ИТ, которая представлена в таблице 1.

Таблица 1 – Система критериев оценки ИБ

Название показателя ИБ	Роль показателя в оценке
1. Конфиденциальность (К)	

Название показателя ИБ	Роль показателя в оценке
Анонимность пользователей (анонимность сеансов работы с системой) (Ап)	Процесс защиты идентификатора и данных
Защита от мониторинга сеансов работы с системой (Змсп)	Процесс защиты системы
Использование псевдонимов (Ип)	Вымышленное имя, используемое для деятельности вместо настоящего (данного при рождении, зафиксированного в официальных документах);
2. Аудит (А)	
Анализ протокола аудита (Апа)	Систематический, независимый и документированный процесс получения свидетельств в форме наблюдений и их объективной оценки с целью определения степени выполнения требований ISO 9001:2008, государственных регламентов, внутренних стандартов предприятия, а также с целью оценки эффективности работы подразделения.
Доступ к протоколу аудита (Дпа)	Доступность протокола
Регистрация и учет событий (Рус)	Подтверждение факта передачи информации по требованию; автоматическое подтверждение факта передачи информации; подразумевает использование как стандартных средств операционных систем, так и специальных средств учета событий безопасности
3. Управление безопасностью (Уб)	
Управление средствами защиты (Усз)	Контроль и управление
Управление параметрами и конфигурацией средств защиты (Упксз)	Настройки средств защиты информации
Административные роли (Ар)	Роль администратора
Ограничение времени действия атрибутов безопасности (Овдаб)	Временные ограничения в использовании некоторых свойств системы
Управление атрибутами безопасности (Уаб)	Управление свойствами системы
4. Защита(З)	
Политика управления доступом (Пуд)	Определяет правила и методы защиты информационной системы
Импорт информации (Ии)	Перенос информации с одной среды в другую
Целостность внутрисистемной передачи информации при использовании внешних каналов (Цвпи)	Целостность информации состояние информации, при котором отсутствует любое ее изменение: либо изменение осуществляется; только преднамеренно субъектами, имеющими на него право
Средства управления доступом (Суд)	Совокупность программных и технических средств
5. Идентификация и аутентификация (ИиА)	

Название показателя ИБ	Роль показателя в оценке
Реакция на неудачные попытки аутентификации (Рнпа)	Действия при неудачных попытках
Атрибуты безопасности пользователей (Абп)	Свойства безопасности для пользователей
Аутентификация пользователей (Ауп)	Процедура проверки подлинности, например, проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей
6. Реализуемость (Р)	
Стоимость реализации обеспечения безопасности (Ср)	Денежные средства необходимые для обеспечения безопасности
Временные затраты на установление средств защиты (Вз)	Время необходимое для установки средств защиты

После оценки по интегральной модели вычисляется интегральный показатель ИБ для каждой оцениваемой ИТ.

Данная система должна выполнять следующие функции:

1. Учет сведений о программных продуктах.
2. Учет экспертных оценок.
3. Расчет критериев и интегрального показателя информационной

Функциональная модель КАК ЕСТЬ считается начальной точкой для анализа потребностей предприятия, выявления проблем и "узких" мест и разработки проекта совершенствования деловых процессов (на рисунке 1).



Рисунок 1 – Модель бизнес-процессов «как есть» (IDEF0)

Основные цели и задачи. Построить ИС, предназначенной для оценки уровня информационной безопасности программных продуктов.

Основные процессы автоматизации в программе:

- учет сведений о программных продуктах;
- учет экспертных оценок;
- расчет критериев и интегрального показателя информационной безопасности программных продуктов.

Моделирование процессов автоматизации представлено на рисунке 2.

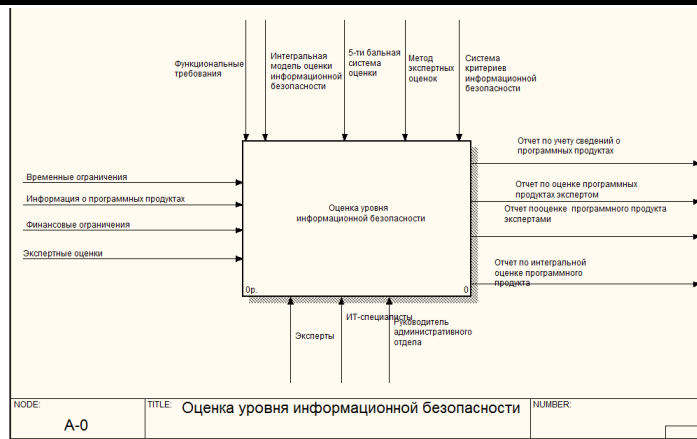


Рисунок 2 – Диаграмма IDEF0

Каждая работа в IDEF3 описывает какой-либо сценарий бизнес-процесса и может являться составляющей другой работы. В отличие от большинства технологий моделирования бизнес-процессов, IDEF3 не имеет жестких синтаксических или семантических ограничений, делающих неудобным описание неполных или нецелостных систем. Модель потоков работ (IDEF3) представлена на рисунке 3

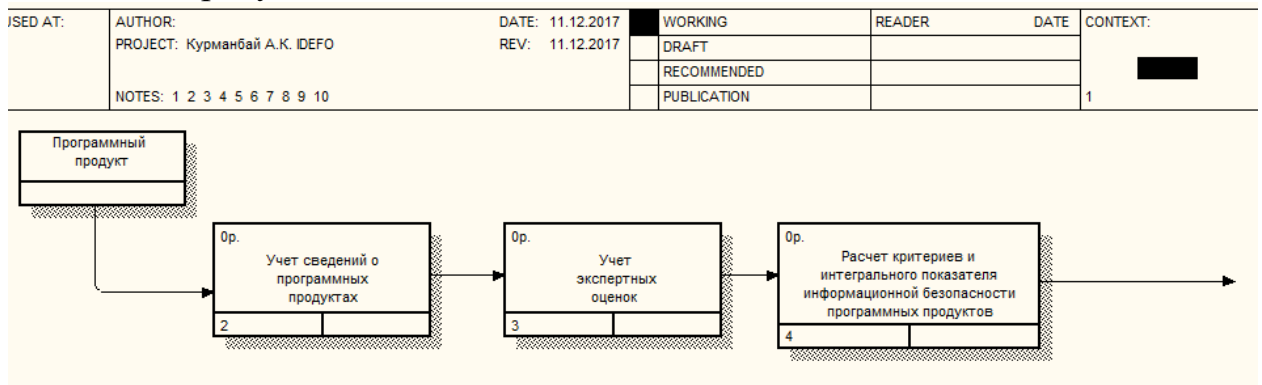


Рисунок 3 – Модель потоков работ (IDEF3)

Модель потоков данных (DFD) представлена на рисунке 4.

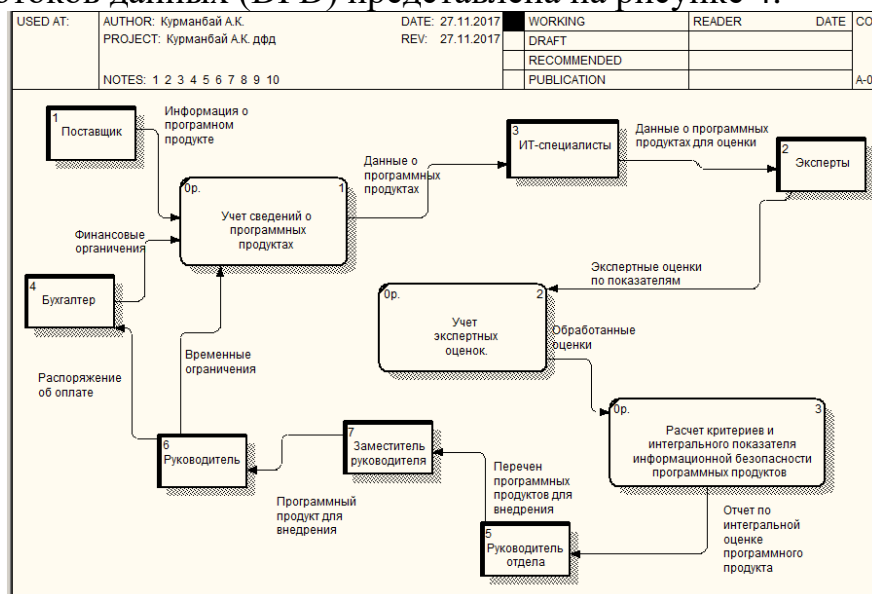


Рисунок 4 – Диаграмма потоков данных

Диаграмма сущность-связь (ERD) представлена на рисунке 5.

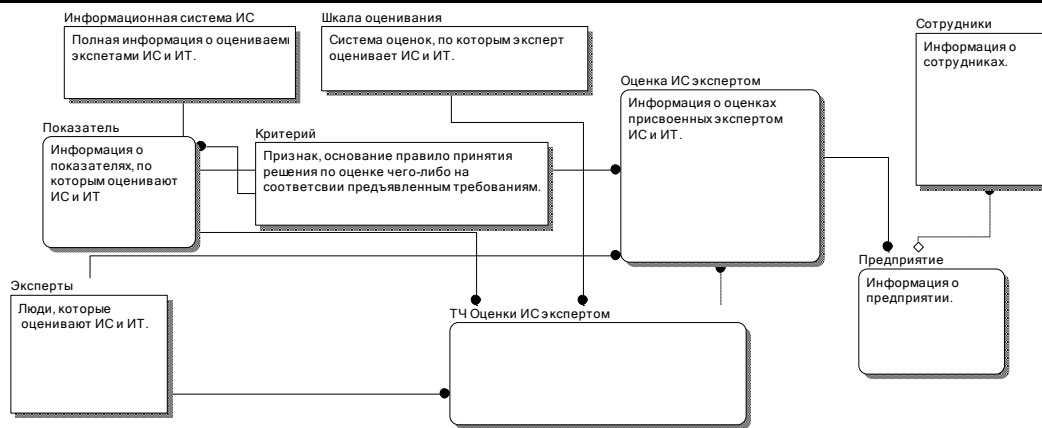


Рисунок 5 – Диаграмма сущность-связь (ERD)

Диаграмма КВ-уровня показывает логическую структуру связей сущностей, составляющих предметную область деятельности. Для описываемой предметной области концептуальная модель на уровне ключей представлена на рисунке 6.

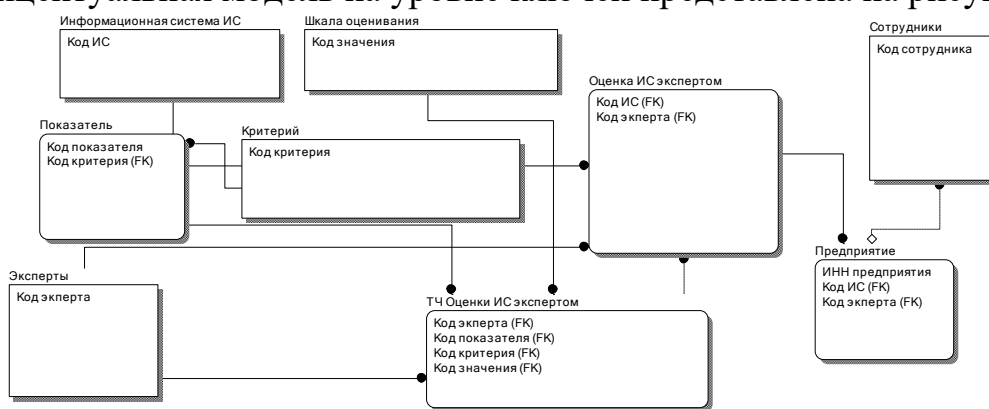


Рисунок 6 – уровень ключей концептуальной модели

В ходе выполнения данной работы спроектирована программный продукт оценки уровня информационной безопасности.

Список литературы

1. Похилько А.Ф., Горбачев И.В. CASE – технология моделирования процессов с использованием средств BPWIN и ERWIN – Ульяновск: Изд. УлГТУ, 2008.
2. Важдаев А.Н. Методические указания по дисциплине «Технология разработки программного обеспечения» по выполнению курсового проекта для студентов специальности 610302 «Прикладная информатика (в экономике)». – Юрга: Изд. ЮТИ ТПУ, 2006. – 44 с.
3. Важдаев А.Н. Технология создания информационных систем в среде 1С: Предприятие: учебное пособие / А.Н. Важдаев. – Юрга: Издательство Юргинского технологического института (филиал) Томского политехнического университета, 2007. – 132 с.