УТВЕРЖДАЮ

Директор

ООО «КФ-Системс»

_____/Рыбин А. А./

«___»_____2021 г.

«Экспертная система поддержки принятия решений по информационной безопасности C-Fence»

Описание функциональных характеристик программного обеспечения

Страниц 13

Ver.1.0

Калининград, 2021

Аннотация

В данном документе содержится описание основных функциональных характеристик системы «Экспертная система поддержки принятия решений по информационной безопасности C-Fence». Приводимые в документе англоязычные термины, принятые в данной предметной области, либо не имеющие русского аналога, употребляются без прямого перевода и пояснений, что в полной мере соответствует и воспринимается персоналом технической поддержки, обладающим необходимыми знаниями, навыками, имеющим необходимую подготовку и являющимся носителями профессиональной терминологии.

Оглавление

Введение 4

1. Назначение программного обеспечения 5

1.1. Основные свойства Системы 5

1.2. Основные возможности Системы 5

2. Информация, необходимая для установки и эксплуатации программного обеспечения ... 7

2.1 Требования к аппаратным средствам 7

2.2 Рекомендуемое программное окружение 7

3. Состав и функции программного обеспечения 8

3.1 Архитектура и среда разработки Системы 8

3.2 Функция «Администрирование» 9

3.3 Функции модуля «Графы» 9

3.4 Функции модуля «Отчёты» 10

3.5 Функции модуля «Алгоритмы» 11

3.6 Функции модуля «Обучение» 12

3.7 Функции модуля «Пользователи» 12

4. Входные и выходные данные 13

Введение

Настоящий документ описывает основные функциональные характеристики системы «Экспертная система поддержки принятия решений по информационной безопасности C-Fence».

Раздел «Назначение программного обеспечения» содержит сведения о назначении «Экспертной системы поддержки принятия решений по информационной безопасности C-Fence», области её использования и общее описание её функциональных возможностей. В разделе «Информация, необходимая для установки и эксплуатации программного обеспечения» представлены минимальные требования к оборудованию и базовому программному обеспечению, необходимому для работы Системы. В разделе «Состав и функции программного обеспечения» приведена архитектура системы, функций, входящих в состав, и модулей. В разделе «Входные и выходные данные» указаны источники поступления данных для обработки в Системе и варианты получения результатов обработки.

1. Назначение программного обеспечения

«Экспертная система поддержки принятия решений по информационной безопасности C-Fence» предназначена для автоматизированного исследования информационных систем на наличие угроз информационной безопасности, а также для поддержки принятия решений экспертами в сфере информационной безопасности.

Система позволяет экспертам составлять опросы, на основе которых данные собираются и анализируются. Эксперты могут обучать систему путём проверки и корректировки автоматически принятых решений.

1.1. Основные свойства Системы

«Экспертная система поддержки принятия решений по информационной безопасности C-Fence» является масштабируемым решением. Одновременно с системой может работать неограниченное число пользователей разного вида: эксперты, обычные пользователи, администраторы. Все модули системы являются обязательными, эксплуатация системы без одного из модулей невозможна.

Эксперты могут создавать опросы с помощью языка графов и задавать логику обработки агрегируемых данных. Обычные пользователи могут проходить опросы и получать в автоматизированном режиме рекомендации по устранению угроз информационной безопасности, сгенерированные системой.

Доступ пользователей к системе осуществляется через web-браузер.

1.2. Основные возможности Системы

«Экспертная система поддержки принятия решений по информационной безопасности C-Fence» обладает следующими возможностями:

- Создание и редактирование опроса с помощью языка графов;
- Создание логики обхода графа на основе ответов пользователей;
- Создание и редактирование шаблонов отчётов;
- Создание (определение) расчётных величин и алгоритмов их расчёта;

- Комплексный анализ ответов пользователей за счёт дедуктивных и эвристических алгоритмов, заложенных в систему;
- Расчёт вероятностей (рисков) возникновения событий;
- Обучение системы;
- Сбор эталонной базы решений для оптимизации работы встроенных алгоритмов;
- Создание аккаунта пользователя, отправка результатов аудита ему на e-mail;
- Редактирование пройденных пользователем опросов.
- Основные группы пользователей Системы:
- Администратор: управляет аккаунтами других пользователей, серверными настройками, имеет полный доступ ко всем подсистемам и модулям Системы; управляет разграничением прав к контенту системы (графы опросов, шаблоны отчётов, результаты прохождения);
- Эксперт: может создавать, редактировать и выполнять графы опросов и шаблоны отчётов;
- Проект-менеджер: может просматривать аккаунты пользователей, самостоятельно прошедших опрос, результаты анкетирования и сгенерированный в автоматическом режиме отчёт с рекомендациями;
- Пользователь: может проходить опросы, доступные классу пользователя, получать отчёт в виде PDF файла на электронную почту. Предусмотрено 2 класса пользователей: класс 1 - пользователи Системы, класс 2 - тестировщики (им доступны графы опросов и шаблоны отчетов, недоступные первому классу).

2. Информация, необходимая для установки и эксплуатации программного обеспечения

2.1 Требования к аппаратным средствам

Для развёртывания и дальнейшей эксплуатации Системы необходим сервер (виртуальная машина) следующей конфигурации (или производительнее):

- Процессор 8 CPU x 2 100 Mhz;
- Оперативная память 8 Gb;
- SSD 80 Gb.

Объем хранилища зависит от количества загружаемых документов и требований по индексированию, что следует учитывать при выборе технических средств. При больших объёмах данных и интенсивном потоке запросов желательно предусмотреть возможность горизонтального масштабирования.

2.2 Рекомендуемое программное окружение

Для функционирования «Экспертной системы поддержки принятия решений по информационной безопасности C-Fence» требуется следующее программное окружение:

- ОС Linux Ubuntu 20.04 LTS 64-разрядная (https://ubuntu.com/);
- Web-сервер Apache 2.2 (https://httpd.apache.org/);
- Сервер баз данных MySQL (https://www.mysql.com/);
- Интерпретатор скриптов PHP версии 7.4 (https://www.php.net/).

Инструкции по установке компонентов представлены на официальных сайтах разработчиков.

3. Состав и функции программного обеспечения

3.1 Архитектура и среда разработки Системы

Общая архитектура системы приведена на рисунке 1. Архитектура является модульной и расширяемой – гибкость в расширении базовых функций системы обеспечивается за счёт подключения дополнительных модулей.

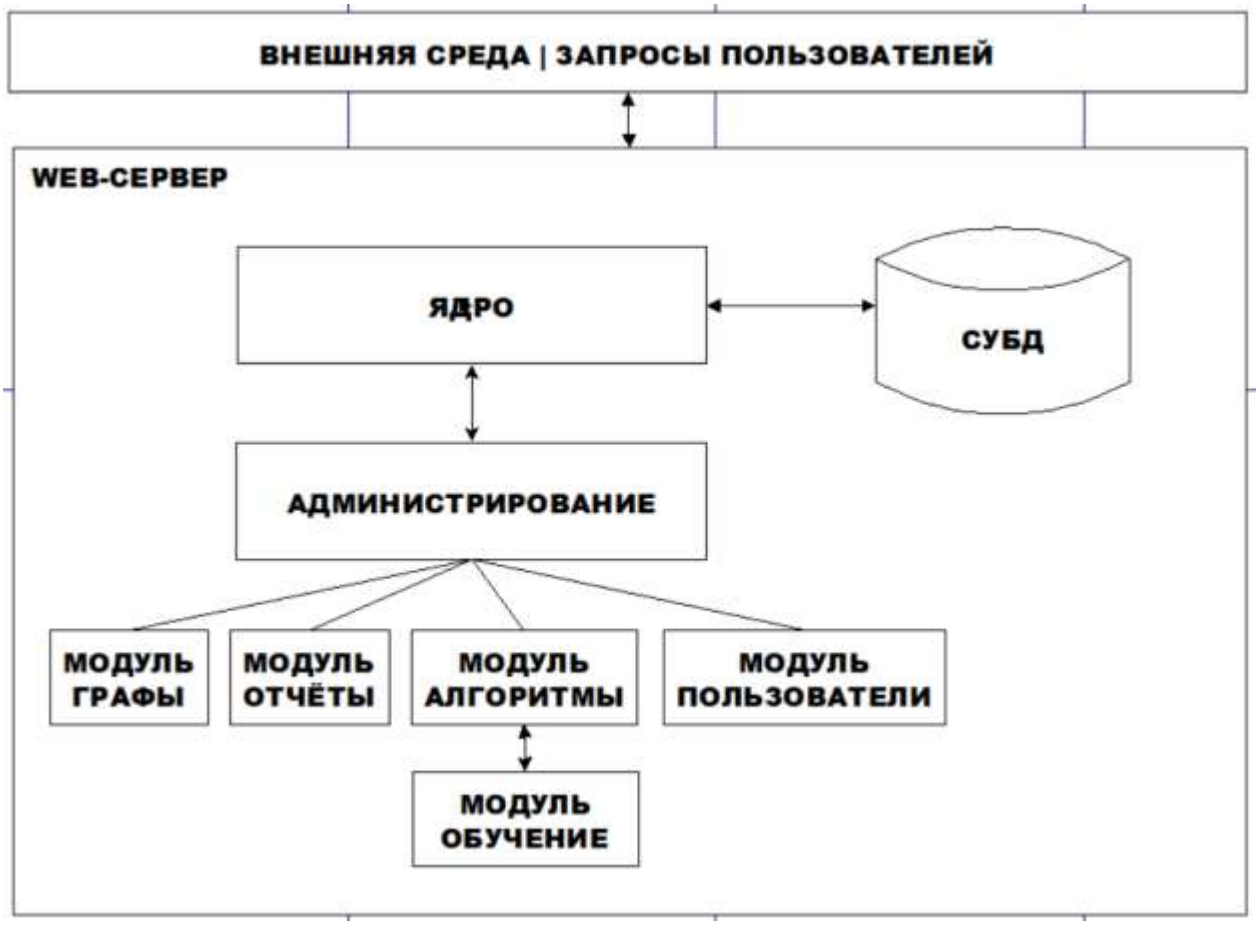

Рисунок 1. Модульная структура Системы

Модуль «Администрирование» отвечает за распределение прав доступа к другим модулям системы. Помимо разграничения прав доступа среди аккаунтов в модуле «Администрирование» реализованы функции создания / удаления / редактирования пользовательских аккаунтов. Модуль «Пользователи» используется для просмотра данных клиентских аккаунтов (пройденные опросы, контактные данные, полученные отчёты).

Система написана на фреймворке YII2. В качестве СУБД используется MySQL. Интерфейсы системы адаптированы под разрешение экрана 1180 пикселей по ширине и более.

3.2 Функция «Администрирование»

Модуль «Администрирование» доступен администратору системы. Основные функции модуля:

- Создание / редактирование / удаление пользовательских аккаунтов (эксперты, пользователи, администраторы);
- Функции архивации данных, очистки временных таблиц, перестройки индексов, очистки временных данных;
- Функции разграничения прав доступа к модулям;
- Сбор и отображение статистических данных об использовании Системы;
- Сбор статистики о действиях пользователей.

3.3 Функции модуля «Графы»

Модуль позволяет задавать опросы визуальными средствами с использованием сущностей языка графов: вершин и ребер. В рамках принятой концепции все ребра являются направленными. С помощью модуля возможно создавать опросы любой сложности:

- Опрос состоит из последовательности вопросов, при ответе на которые можно выбрать один или несколько вариантов ответов;
- В зависимости от выбранного ответа (совокупности ответов) структура опроса (последовательность вопросов) может перестраиваться;
- Количество вопросов в опросе ограничено только аппаратными возможностями сервера (группы серверов, облака), на котором функционирует система;
- Возможно создавать опросы, в которых заложена сложная (с большим количеством ветвей, условий, переменных) логика исполнения.

Предусмотрено 2 вида вершин: инклюзивные и эксклюзивные. Инклюзивные вершины позволяют выбрать более одного варианта ответа. Для всего множества возможных комбинаций ответов должны быть заданы исходы (номера последующих вершин). Эксклюзивные вершины позволяют выбрать только один вариант ответа. После ответа на вопрос, заключенный в эксклюзивной вершине графа, происходит переход по дуге (направленному ребру) к следующей вершине (вопросу). Основные функции модуля:

- Создание неограниченного количества вершин графа (вопросов) и задание переходов между ними (условный, безусловный);
- Выбор типа вершин (инклюзивные / эксклюзивные);
- Указание множественных исходов для инклюзивных вершин;
- Указание весов (коэффициентов) дугам (переходам) графов;
- Визуальный HTML-редактор для ввода расширенного описания вопроса (картинки, видео, документы, текст, HTML разметка);
- Функция проверки графа на полноту, целостность, циклы, рециклы, петли;
- Отладка графа через встроенный в модуль плеер;
- Запуск графа (прохождение опроса) для пользователей системы без привилегий;
- Определение наиболее часто встречающихся цепочек ответов пользователей;
- Определение цепочек, которые следует отобразить эксперту для проверки и добавления в базу знаний.

3.4 Функции модуля «Отчёты»

Модуль позволяет создавать шаблоны отчётов, которые формирует система после прохождения опроса. Шаблон задаётся в WYSIWYG редакторе в формате HTML с использованием внутренней разметки. Внутренняя разметка представляет собой динамически формируемые рекомендации в зависимости от ответов на вопросы, переменные, формулы. Основные функции:

- Создание / редактирование / удаление шаблонов отчётов и их привязка к созданным экспертами графам;
- Контроль версий (истории изменений) шаблона;
- Разметка шаблона, создание генерируемого отчёта и использование внутреннего языка разметки на основе XML;
- Вставка вариативных (динамических) частей отчёта;
- Использование переменных (расчётные коэффициенты, формулы, внутренние переменные) в теле отчета;
- Генерация отчёта в PDF;
- Отправка отчёта на почту;
- Сбор контактных данных пользователей.

3.5 Функции модуля «Алгоритмы»

Данный модуль используется для автоматизации расчёта рисков ИБ и оптимизации работы эвристических алгоритмов. Модуль интерпретирует математические формулы, заданные в шаблоне отчётов. По заданным экспертом правилам присваиваются начальные значения переменных в зависимости от данных ответов в ходе прохождения опроса. Основные функции:

- Встроенный набор функций для типовых (с описанной и утверждённой методикой) рисков ИБ;
- Возможность фиксировать (задавать) переменные и коэффициенты в зависимости от выбранного пользователем варианта ответа при прохождении опроса;
- Возможность создавать формулы, доступные для использования при генерации отчёта. Используется визуальный редактор формул с поддержкой расширенного набора математических операций.

3.6 Функции модуля «Обучение»

Данный модуль используется для проверки качества составленных опросов и генерируемых отчётов. В основе используется нейросетевое создание лексем, сформированных на основе цепочек ответов пользователей. Каждая цепочка формирует уникальную лексему. Анализ полученных лексем и результатов оценки рисков производится автоматизированно. Результаты, сильно отличающиеся «на входе» (цепочки ответов) или «выходе» (сгенерированные рекомендации), фиксируются и предоставляются эксперту на проверку. По мере одобрения или отклонения экспертом пары «лексема-результат» система пополняет словарь (набор контрольных значений). Параметр «сигма» указывает на допустимую степень расхождения морфологических форм в лексемах и в результатах. Степень расхождения, длина морфологической формы и алфавит (множество) формирования лексем могут быть изменены Администратором. Дополнительные функции модуля:

- Отображение результатов для проверки экспертом;
- Автоматическое определение «подозрительных» (возможно, ошибочных) рекомендаций, сгенерированных системой;
- Формирование базы знаний, автоматическая сортировка результатов на проверку по степени важности;
- Изменение настроек работы алгоритма;
- Возможность задания эталонных значений при прохождении опроса экспертом и последующая оценка результата.

3.7 Функции модуля «Пользователи»

Модуль представляет собой CRM-систему, в которой фиксируются пройденные пользователем опросы и полученные (сгенерированные) автоматически рекомендации.

Модуль позволяет пользователям просматривать историю ответов (цепочки ответов) и скачивать полученные отчёты в формате PDF (а также отправлять их на почту).

Эксперты могут вносить корректировки в отчёты, вести историю сгенерированных документов.

Менеджеры проектов могут просматривать контактные данные клиента и проставлять статус (этапы) проекта.

Предусмотрена возможность вставки на сторонние ресурсы JS кода, который позволит неавторизованному пользователю пройти анкетирование и получить рекомендации системы без регистрации.

Для обычных пользователей в этом модуле реализованы функции регистрации / восстановления пароля.

4. Входные и выходные данные

Входной информацией для «Экспертной системы поддержки принятия решений по информационной безопасности C-Fence» являются запросы пользователя, данные в базах данных, настройки модулей. Основными данными являются: графы, шаблоны отчётов, формулы и переменные, последовательность ответов пользователей при прохождении анкетирования.

Выходной информацией являются экранные и печатные формы, файлы (формат PDF), а также данные, которые могут быть экспортированы для использования во внешних системах.