А. В. Янушко, А. В. Бабанин, О. А. Кузнецова, С. В. Петрушенко, М. Ю. Чекмарев

ЗАЩИЩЕННЫЙ АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ЦЕНТРА ХРАНЕНИЯ ЭЛЕКТРОННЫХ КОПИЙ МАТЕРИАЛОВ УГОЛОВНЫХ ДЕЛ

Введение

Задача совершенствования информационно-аналитического обеспечения работы органов внутренних дел РФ включает в себя модернизацию системы формирования различных баз данных, обработки запросов и выдачи отчетности.

В то же время некоторые функционирующие в органах внутренних дел информационно-коммуникационные системы характеризуются отсутствием унифицированного программного обеспечения и наличием существенных функциональных ограничений, не позволяющих использовать современные информационные технологии для выполнения качественного анализа информации. Кроме того, не решены в полном объёме вопросы развития банков данных розыскной информации и обеспечения требуемого уровня информационной безопасности при доступе к защищенным информационным ресурсам. Необходимо также повышать полноту и достоверность предоставляемых данных и сокращать время поиска требуемой информации [1].

Задача проектирования, реализации и внедрения распределенной системы хранения разнородной информации, относящейся к уголовным делам, оконченным производством, является в данный момент достаточно актуальной. Такая система должна обеспечивать формирование и пополнение локальных баз данных, эффективный поиск информации, распределенную работу пользователей с санкционированным удаленным доступом, а также агрегирование сведений и централизованное управление на уровне руководящих структурных подразделений органов внутренних дел РФ.

Далее в статье используются следующие сокращения:

АПК – аппаратно-программный комплекс

ЕИТКС – единая информационно-телекоммуникационная система

ИМТС – интегрированная мультисервисная телекоммуникационная система

ЦБД – Центральная инсталляция аппаратно-программного комплекса «Невод-Р»

РБД – Региональная инсталляция аппаратно-программного комплекса «Невод-Р»

ДСС – Доверенный сеанс связи

Особенности создания АПК «Невод»

Центральная задача разработки заключалась в проектировании и реализации типового аппаратно-программного комплекса регионального центра хранения электронных копий материалов уголовных дел, оконченных производством «Невод-Р».

АПК представляет собой территориально-распределенную систему, обеспечивающую информационное обслуживание сотрудников Следственного комитета при МВД России, главных следственных управлений (следственных управлений, отделов) при МВД, ГУВД, УВД по субъектам Российской Федерации, УВД на транспорте, УВД (ОВД) на закрытых территориях и режимных объектах.

АПК обслуживает информационные потоки в органах предварительного следствия системы МВД России, которые обусловлены поступлением, накоплением и обработкой данных о физических и юридических лицах, проходящих по материалам уголовных дел.

АПК устанавливается на рабочих местах сотрудников региональных подразделений, а также сотрудников Следственного комитета на федеральном уровне. Функционирование АПК основывается на взаимодействии по защищенным каналам связи рабочих станций пользователей с серверными терминалами внутри ведомственных интегрированных телекоммуникационных сетей, построенных на основе государственных и коммерческих сетей связи и передачи данных системы органов внутренних дел.

Для обеспечения эффективного взаимодействия пользователей в процессе выполнения служебных задач, а также для обеспечения надежности работы АПК, в состав АПК включена единая система управления и организации доступа к формируемым информационным ресурсам на основе средств реализации доверенного сеанса связи «МАРШ!».

Основные функции системы

Аппаратно-программный комплекс:

— Предоставление сведений о физических и юридических лицах, проходивших по материалам уголовных дел;

— Ведение учета уголовных дел, оконченных производством, на основании информации:

- постановлений о возбуждении уголовных дел;
- резолютивных частей обвинительных заключений;
- постановлений о прекращении уголовных дел;
- постановлений о приостановлении уголовных дел;
- предусмотренных УПК приложений к обвинительным заключениям;
- ряда других процессуальных документов.

Кроме того, АПК может быть использован как источник практического опыта расследования преступлений, не имеющих широкого распространения и вызывающих наибольшие трудности.

Принципы построения системы

АПК построен в соответствии с концепцией распределения функций информационной системы по трем логическим уровням для обеспечения повышенной масштабируемости и надежности.

Система включает в себя следующие логические уровни (см. Рис. 1):

— Уровень доступа. Этот уровень содержит средства информационной безопасности обеспечивающие достаточный уровень защищенности информационного ресурса АПК «Невод-Р».

— Презентационный уровень. Интерфейс системы организован на основе Web-технологий. Данный уровень предназначен для предоставления функциональности системы пользователю и обеспечения оперативного ввода и изменения данных при наличии у пользователя определенных прав и доступа к системе. Данный уровень обеспечивает взаимодействие пользователей и клиентских приложений с системой.

— Уровень логики процессов. Данный уровень содержит программные объекты и программный код (функциональные модули), реализующие логику работы системы и непосредственно автоматизирующие пользовательские функциональные процессы. Данный уровень объединяет в единый комплекс все функциональные подсистемы и обеспечивает среду для их выполнения.

— Уровень данных. Уровень хранения данных обеспечивает долговременное эффективное хранение данных системы. Уровень включает в себя хранилища данных и все необходимые компоненты для доступа к данным. Уровень предоставляет программный интерфейс для объектов уровня логики процессов. На данном уровне сгруппированы все прикладные и системные данные, обеспечивающие информационное наполнение системы и работу функциональных подсистем.

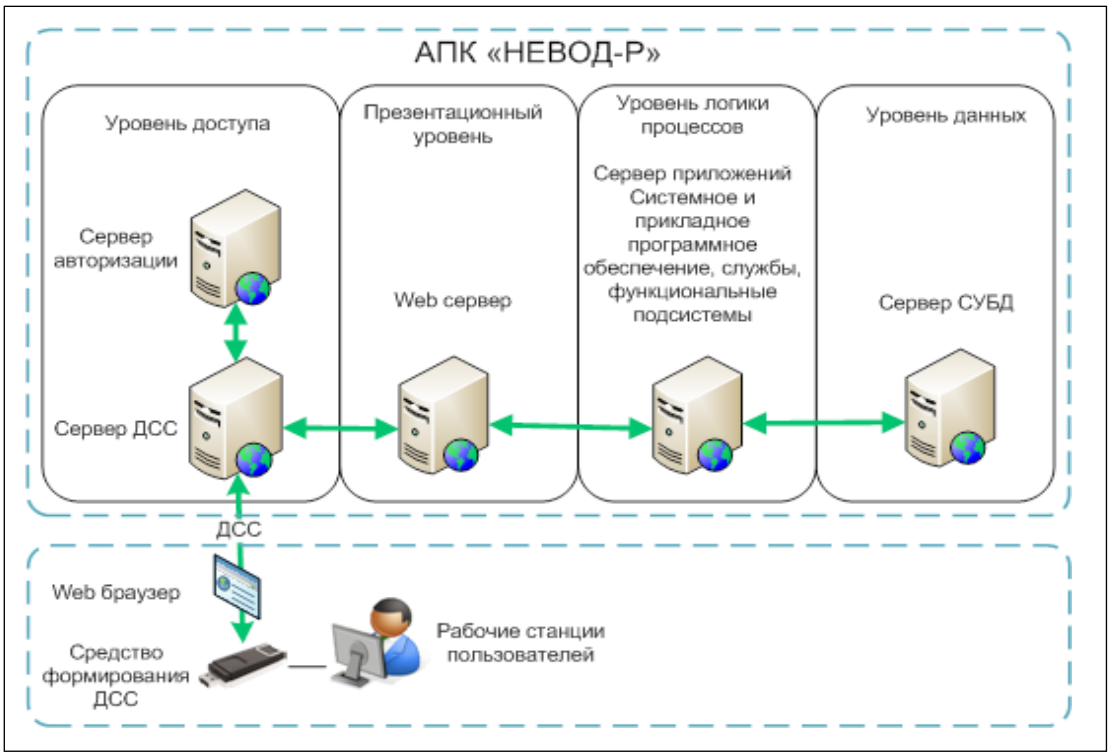

Рис. 1. Логические уровни АПК «НЕВОД-Р»

В основу АПК при его проектировании и разработке были положены следующие принципы [2]:

— Распределенное хранение формализованной и неформализованной информации в центральной и региональных базах данных;

— Консистентность — согласованность и непротиворечивость хранимых данных;

— Актуальность — полное соответствие последним по времени изменениям хранимых данных;

— Надежность централизованного хранения межведомственной информации;

— Безопасность — гарантированное исключение возможности несанкционированного доступа, модификации или уничтожения информации;

— Оперативный доступ, то есть возможность для чтения, пополнения и модификации данных для территориально распределенных клиентов в рамках определенных для них полномочий в режимах непосредственной работы с данными по ИМТС ЕИТКС ОВД и передачи данных и запросов без прямого подключения к банку данных;

— Надежность и безопасность доступа удаленных пользователей к центральной и региональным базам данных;

— Производительный формальный поиск информации по строго определенному набору атрибутов в едином банке данных для территориально распределенных клиентов в рамках определенных для них полномочий;

— Достоверность передачи информации по телекоммуникационным каналам;

— Гарантированное получение и доставка информации удаленным клиентам;

— Модульность архитектуры, где каждый из модулей представляет собой совокупность приложений.

Функциональные компоненты системы

В состав АПК входят следующие подсистемы:

— Подсистема загрузки, хранения и обработки данных;

— Подсистема поиска;

— Подсистема формирования отчетности;

— Подсистема обмена информацией между различными уровнями территориального деления;

— Подсистема аутентификации пользователей;

— Подсистема администрирования;

Подсистема загрузки, хранения и обработки данных

Подсистема предназначена для хранения разнородных формализованных и неформализованных данных с изменяемой в процессе эксплуатации структурой, а также для визуализации работы с информацией, хранящейся или поступающей в банк данных АПК.

В данной подсистеме хранятся:

- Системный журнал (включая архив запросов пользователей, архив просмотров пользователями документов, хранящихся в системе);
- Справочники и классификаторы;
- Архив справочников и классификаторов;
- Документы по уголовным делам, оконченным производством.

Реализованы следующие сервисные функции по обработке документарной информации:

- хранение документов по уголовным делам, оконченным производством;
- обмен документами на всех уровнях территориального деления;
- обеспечение защиты информации;
- синтаксический разбор русскоязычных текстовых документов и выделение атрибутов документа согласно заранее определенному списку атрибутов [4], [5].
- привязка дополнительной атрибутивной информации к нетекстовым объектам;
- формирование информации, автоматически отсылаемой из региональных баз данных в центральную.

Реализована возможность корректной работы с документами в форматах MS Office 2007 в режимах загрузки файлов в систему и просмотра.

Системный журнал содержит информацию:

- о режимах, с которыми работал пользователь;
- о записях, которые редактировал пользователь;
- о событиях доступа к функциям подсистем;
- дату и время входа в систему (выхода из системы);
- дату и время запроса данных и составления отчетов.

Наличие архива данных системы обеспечивает возможность создания альтернативной резервной копии данных. Структура архива представляет собой копию структуры базы данных системы. Кроме того, в архиве данных системы хранятся данные о пользователе системы, осуществившем последнюю транзакцию, дата и время осуществления транзакции для возможности восстановления системы при сбоях и аварийных ситуациях до состояния, предшествовавшего последней команде.

В архиве запросов пользователей хранится перечень атрибутов запросов, их значения, дата и время осуществления запроса документов и информации о пользователе, осуществившем запрос.

В архиве просмотров пользователями документов, хранящихся в системе, содержится информация о просмотренном документе, дате и времени просмотра документа и информация о пользователе, просматривавшем документ, хранящийся в системе.

Копирование информации в архив данных системы, в архив запросов пользователей и в архив просмотров пользователем документов предусмотрено регламентом выгрузки, параметры которого конфигурирует администратор системы.

Использование архивов обеспечивает формирование журнала аудита событий, и тем самым обеспечивает возможность эффективного поиска сведений в журнале аудита событий.

Документы, загружаемые в региональном подразделении, хранятся на сервере данного регионального подразделения.

При загрузке документов с систему производится индексирование текста по следующим атрибутам:

– Имя файла;
– Номер уголовного дела;
– Задержанный;
– Обвиняемый;
– Свидетель;
– Следователь;
– Статья/часть по УК РФ;
– Статья по УПК РФ;
– Дата возбуждения уголовного дела.

После завершения процесса индексации система автоматически прикрепляет к загружаемому документу «ярлык», содержащий перечень найденных в тексте документа атрибутов.

Указанные атрибуты являются базовым набором атрибутов, по которым может производиться поиск документов, хранящихся в АПК. Данный набор может быть расширен посредством разрабатываемого в рамках данной ОКР «конструктора». А именно: администратор центральной системы имеет возможность добавлять новые атрибуты в справочник атрибутов. Вновь добавленные атрибуты автоматически рассылаются во все региональные системы и становятся доступны всем пользователям. Пользователи системы имеют возможность прикрепить любые атрибуты из справочника атрибутов к любому доступному документу (при наличии соответствующих полномочий). Атрибуты, прикрепленные вручную, участвуют в поиске документов на равных правах с базовыми атрибутами, прикрепленными к документу автоматически.

В автоматическом режиме по каналам ИМТС ЕИТКС ОВД может осуществляться копирование документов уголовных дел по некоторым статьям УК и УПК, а так же по любым другим критериям, определяющим область заинтересованности федерального центра, из региональных систем в центр хранения электронных копий материалов уголовных дел Следственного комитета. Критерии и регламент передачи документов в ЦБД «Невод» задаются администратором системы.

Подсистема поиска

Подсистема предназначена для формального (по определенному набору атрибутов) поиска информации в едином банке данных для территориально распределенных пользователей, в рамках определенных для них полномочий.

Подсистема поиска позволяет осуществлять атрибутивный поиск по объектам и элементам ключевых объектов АПК, включая документы и справочники, а также фильтрацию данных в реестрах и списках АПК.

В данной подсистеме реализовано:

- отображение критериев поиска в удобной для пользователя форме, возможность составления запросов без применения языков программирования;
- поддержка формирования запросов как по атрибутам объектов, так и с использованием логических правил «И»/ «ИЛИ», при этом конструктор запросов позволяет строить логические выражения любой степени сложности;

- возможность осуществления повторного поиска документов методом уточнения результатов уже выполненного запроса;
- возможность осуществления поиска по строгому и нестрогому соответствию атрибутам, определение диапазона значений атрибута в зависимости от типа атрибута.

Для организации запросов информации между региональными центрами хранения банков данных, подсистема поиска обеспечивает выполнение следующих функций:
- получение в ЦБД запроса из РБД определенной формы, с заданными атрибутами поиска;
- автоматическую рассылку запросов из ЦБД во все региональные центры;
- получение в ЦБД информации по запрашиваемым данным из РБД;
- автоматическую передачу результатов запроса из ЦБД в запрашивавший информацию РБД;
- получение и просмотр документов из других РБД.

Подсистема формирования отчетности

Данная подсистема предоставляет средства формирования статистической отчетности, необходимой для мониторинга и анализа деятельности подразделений на разных уровнях детализации. Подсистема формирования статистической отчетности обеспечивает:

— возможность представления отчетов в виде страниц, содержащих цифровое представление данных;

— предоставление пользователю следующей функциональности для анализа данных:
- поддержка различных способов представления данных: табличное представление, диаграммы различных типов;
- возможность просмотра отчетов на различных уровнях детализации (детализация по регионам, детализация по периодам времени и т.д.);
- возможность сортировки и фильтрации данных по заданным критериям.

—экспорт отчетов в приложения MS Office для последующей обработки и использования;

— вывод отчетов на печать из интерфейса просмотра отчетов;

— получение статистической информации об объеме и характере документов, хранящихся в регионах под управлением РБД «Невод», о количестве запросов, поступающих в региональные центры хранения;

Подсистема обмена информацией между различными уровнями территориального деления

Данная подсистема предназначена для организации управления информационным взаимодействием центральной инсталляции с развернутыми в регионах периферийными инсталляциями.

Подсистема обмена информацией обеспечивает:

— информационный обмен между подсистемами и модулями АПК;

— информационное взаимодействие между различными функциональными и территориально-распределенными группами сотрудников;

— возможность работы со структурированными и неструктурированными данными;

— автоматическую загрузку в ЦБД документов, поступающих из РБД по каналам ИМТС ЕИТКС ОВД;

— предоставление пользователю ЦБД агрегированной информации в том случае, если он запрашивает документы, хранение которых осуществляется в РБД

Разработаны средства информационного взаимодействия, в том числе:

— средства для автоматической передачи в ЦБД документов, загруженных в РБД и относящихся к статьям УК и УПК, являющимся областью заинтересованности федерального центра, по каналам ИМТС ЕИТКС ОВД.

— средства для автоматического формирования агрегированной информации, которая предоставляется пользователю РБД в том случае, если он запрашивает документы по статьям УК и УПК, хранение которых осуществляется в других РБД или в ЦБД.

Подсистема аутентификации и авторизации пользователей

Данная подсистема предназначена для обеспечения безопасного использования данных АПК и для разграничения прав доступа пользователей к системе.

Подсистема аутентификации и авторизации пользователей обеспечивает:

— обеспечение надежности защиты информации за счет централизованного управления доступом к конфиденциальным данным;

— единую аутентификацию пользователей (назначение индивидуального имени пользователя и пароля);

— безопасный доступ к базе данных системы через пользовательский интерфейс.

Разграничение доступа к режимам функционирования системы осуществляется в соответствии с ролевой моделью.

Для эксплуатации АПК определены следующие роли:

— Администратор;

— Оператор;

— Аналитик.

Способ реализации ролевой модели доступа позволяет конфигурировать список ролей пользователей администратором системы через пользовательский интерфейс.

Перечень функций, выполняемых пользователями различных ролей:

— Администратор — обеспечивает функционирование технических и программных средств подсистем, сохранность данных системы и реализацию ролевой политики. В его функциональные обязанности входит:

- настройка и диагностирование подсистем и их частей;
- управление общесистемным ПО;
- управление техническим обеспечением;
- управление доступом к системе и ее частям;
- разработка и исполнение плана резервного копирования данных подразделения, исходя из следующих условий:
- резервное копирование данных;
- контроль целостности данных;
- восстановление данных.

В части управления доступом к системе Администратор осуществляет:

- формирование рабочих групп пользователей (определение привилегий и прав доступа на уровне групп пользователей);
- распределение полномочий и прав доступа к данным и функциям между операторами;
- проведение аудита работы пользователей;
- управление списком ролей пользователей и соответствующих категорий должностных лиц, с целью реализации ролевого доступа к системе;
- управление профилями и полномочиями ролевого доступа пользователей, в которых указываются права доступа каждой роли пользователя к функциям;
- проведение мониторинга работы средств защиты АПК от НСД.

— Оператор — обеспечивает технологический процесс функционирования АПК. В его функции входит:

- ввод информации из первичных документов;
- формирование запросов и получение информации из БД;
- формирование и вывод выходных документов и материалов.

— Аналитик — обеспечивает процессы обработки информации, хранящейся в АПК. В его функции входит:

- поиск и чтение информации из документов;
- формирование запросов и получение информации;
- сбор, группировка и сортировка информации для получения сведений статистического характера, составления отчетов.

Реализована возможность совмещения одним должностным лицом нескольких ролей.

АПК обеспечивает аутентификацию и авторизацию пользователей, программных средств, рабочих станций, серверов и другого сетевого оборудования, обратившегося к технологическому узлу для получения доступа к функциям АПК.

Подсистема позволяет создавать функциональные группы; разграничение прав доступа для группы реализовано в рамках той же ролевой модели, что и для пользователя. Доступ пользователя к функциям АПК предоставляется в зависимости от включения его в функциональные группы; пользователь может одновременно входить в несколько групп.

Подсистема администрирования

Подсистема администрирования предназначена для управления процессом ввода базовых данных и предоставления иных сервисных функций. Ее интерфейсы доступны только пользователям, имеющим полномочия администратора.

Подсистема предусматривает использование широких функциональных возможностей по систематизации сведений, содержащихся в базе данных, и оптимизации процессов ее использования.

Подсистема включает в себя набор следующих функций:

— заполнение справочников;

— управление справочниками настроек соединения с регионами;

— обеспечение безопасности и разграничение прав доступа к данным на уровне организаций-участников проекта, отделов, рабочих групп и пользователей:

- добавление, изменение и удаление групп пользователей;
- добавление и изменение учетных записей пользователей;
- настройка прав доступа пользователей и групп пользователей к информационным разделам и функциям АПК;
- проверка прав доступа пользователей и групп пользователей к информационным разделам и функциям АПК;
- блокировка доступа пользователей к АПК или его частям.

— мониторинг операций, совершаемых пользователями АПК, и полное протоколирование (сохранение в системном журнале) информации о попытках доступа к служебной информации на уровне:

- отдельных пользователей;
- отдельных записей банка данных;

— возможность создания резервных копий базы данных;

— возможность восстановления информации из резервной копии базы данных в случае возникновения нештатных ситуаций.

Средства обеспечения информационной безопасности

Для организации защищенного доступа пользователей к АПК «Невод» применяется технология доверенных сеансов связи, позволяющая на определённый период времени (сеанс) организовать на пользовательском компьютере доверенную вычислительную среду и установить защищённое VPN-соединение с сервером АПК. При этом компьютер может работать в двух режимах: открытый режим и режим доверенного сеанса связи.

Для входа в режим доверенного сеанса связи [6] пользователь выполняет доверенную загрузку операционной системы с персонального USB-устройства «МАРШ!». Устройство автоматически устанавливает VPN-соединение с сервером ДСС и сервером авторизации АПК, сервер авторизации выполняет проверку прав доступа пользователя и в случае наличия необходимых прав переключает его на пользовательский web-интерфейс АПК с учетом роли и прав пользователя. Таким образом, пользователь осуществляет доверенное взаимодействие с защищаемым ресурсом, работая в доверенной среде с возможностью применения ЭЦП.

Указанные решения, позволяют обеспечить защиту целостности и конфиденциальности электронной информации, а также защиту от несанкционированного доступа.

Система поддерживает работу в том числе с криптопровайдером «КриптоПро CSP», что обеспечивает передачу данных между компонентами АПК по защищенному протоколу https согласно ГОСТ Р 34.11-94 [3].

Опыт практического внедрения АПК

В рамках создания АПК выполнены работы по проектированию региональной и центральной систем и проведена разработка программного обеспечения; проведено функциональное и нагрузочное тестирование в ручном и автоматическом режимах, тестирование безопасности и совместимости. Организовано и проведено обучение эксплуатационного персонала. АПК укомплектован руководством пользователя и администратора системы.

АПК успешно прошел процедуру приемо-сдаточных испытаний и в настоящее время эксплуатируется в пилотных регионах Российской Федерации. АПК установлен и введен в эксплуатацию в УВД по Рязанской области в рамках работ по формированию сегмента Единого информационного пространства ОВД.

СПИСОК ЛИТЕРАТУРЫ:

1. *Захаров В. Н., Костогрызов А. И., Цыганков В. С., Чекмарев М. Ю.* О требованиях к создаваемым и модернизируемым системам для подключеия их к ЕИТКС ОВД // Системы и средства информатики, специальный выпуск «Научно-техничесие вопросы построения и развития единой информационно-телекоммуникационной системы органов внутренних дел». М., 2009. С. 213–227.
2. *Илюшин Г. Я., Лиманский В. И., Боков А. М., Подгорнов Ю. Г.* Основные принципы и методы интеграции информационных ресурсов // Системы и средства информатики, специальный выпуск «Научно-техничесие вопросы построения и развития единой информационно-телекоммуникационной системы органов внутренних дел». М., 2009. С. 34–63.
3. *Николаев Ю. В.* Использование Crypto API [Электронный ресурс] // RSDN Magazine #5-2004. URL: http://www.rsdn.ru/article/crypto/usingcryptoapi.xml (Дата обращения 15.01.2011).
4. *Parr T.* The Definitive Antlr Reference: Building Domain-Specific Languages // Pragmatic Bookshelf. Texas, USA, 2007. – 384 p.
5. *McCallum A.* Information Extraction: Distilling Structured Data from Unstructured Text // ACM Queue – Social Computing. New York, NY, USA, 2005. Vol. 3. Issue 9. P. 49–57.
6. *Чекмарёв М. Ю.* Принципы и последовательность организации доверенного сеанса связи // Безопасность информационных технологий. 2010. № 3. С. 153–156.