Таким образом, несмотря на то, что в Российской Федерации за довольно короткое время сформировалась достаточно обширная нормативная правовая база в области информационной безопасности и защиты информации, в настоящее время существует острая необходимость в ее дальнейшем совершенствовании.

VI Заключение

В заключение хотелось бы сказать несколько слов о международном сотрудничестве Российской Федерации в области защиты информации.

С учетом исторического опыта в качестве основных партнеров для сотрудничества в данной области Российская Федерация рассматривает государства – члены СНГ. Однако нормативная база по вопросам защиты информации в рамках СНГ развита недостаточно.

Представляется перспективным осуществлять указанное сотрудничество в направлении гармонизации законодательной базы государств, их национальных систем стандартизации, лицензирования, сертификации и подготовки кадров в области защиты информации.

В рамках практической реализации Соглашения о взаимном обеспечении сохранности межгосударственных секретов, подписанного 22 января 1993 года в г. Минске, Правительством Российской Федерации был заключен ряд международных договоров в области защиты информации (с Республикой Казахстан, Республикой Белоруссия и с Украиной).

Наиболее успешно в рамках указанных двусторонних международных договоров осуществляется сотрудничество Российской Федерации с Республикой Белоруссия. Подготовлен ряд совместных документов, направленных на создание условий и оснований для гармонизации национальных законодательств России и Белоруссии в области защиты информации, создание унифицированной системы нормативно-методических и технических документов в области защиты информации, унификацию национальных систем лицензирования деятельности в области защиты информации и сертификации средств защиты информации.

Активизируется сотрудничество в области защиты информации с Республикой Казахстан. В частности, планируется проведение переговоров с республикой Казахстан по целому ряду аспектов двустороннего сотрудничества, включая вопросы, связанные с нормативной базой, осуществлением лицензирования и сертификации в области защиты информации, подготовки и переподготовки кадров в данной области.

К сожалению, несмотря на заключенное между Россией и Украиной в 1996 году в г. Киеве межправительственное Соглашение о сотрудничестве в области технической защиты информации, взаимодействие между нашими государствами в рамках указанного международного договора практически не осуществляется.

УДК 681.226.1

КОМПЛЕКСНЫЙ ПОДХОД К ПОСТРОЕНИЮ СИСТЕМЫ БЕЗОПАСНОСТИ В GIS – ТЕХНОЛОГИЯХ

Владимир Чаинский
Физико-технический институт НТУУ "КПИ"

Анотація: **GIS - технології чутливі до якості інформації. Це робить актуальним питання розробки Системи Безпеки інформації. В роботі наводиться приклад використання комплексного підходу для побудови Системи Безпеки GIS - технології. Аналіз проводиться з урахуванням п'яти рівнів абстракції Автоматизованих Систем Обработки та Реєстрації інформації.**

Summary: **GIS - technologies are sensitive for information quality. So, development of Information Security Systems is very impotent. There is an example of usage of Security System for GIS - technology in this article. The five levels of abstraction of recording and processing information systems are taken into account for analysis.**

I Задачи построения СБ при использовании комплексного подхода

GIS-системы есть разновидность Автоматизированной Системы Обработки и Регистрации Информации (АСОРИ). Для построения Системы Безопасности (СБ) в GIS-системе был использован комплексный подход, являющийся универсальным для любой АСОРИ.

Комплексный подход требует проведения анализа обобщенной GIS - системы на каждом из пяти уровней абстракции АСОРИ.

1. Первый уровень абстракции представляет правило использования технологии для поддержания необходимых бизнес процессов. Это восприятие технологии с точки зрения пользователя (пользователей). На этом уровне для СБ определяются полномочия пользователя при использовании данного АСОРИ.
2. Второй уровень объединяет набор функций, которые реализуют алгоритмы поддержки установленной технологии. Они не только поддерживают бизнес-процессы. При реализации этого уровня проходит проектирование обмена информацией между пользователем и АСОРИ (GIS - системой) на права и полномочия, определяемые СБ. Функции обязаны вернуть результат своей работы только при полном соответствии результата работы и полномочий пользователя.
3. На третьем уровне определяется набор системных функций и серверов, которые привлекаются при построении GIS - системы. Каждый элемент из этого набора анализируется на наличие механизмов защиты информации. Речь идет о возможности привлечения этих механизмов для построения СБ.
4. Четвертый уровень представляет собой данные, сохраняемые в определенном формате. Данные делятся на три группы: параметры для функционирования функций, поддерживающие второй уровень абстракции, параметры для функционирования услуг, описываемые на третьем уровне абстракции, информация принимающая участие в формировании ответов на запрос пользователя – GIS-информация. Форматы и обработка при хранении этих данных должны полностью поддерживать функционирование реализации предыдущих уровней.
5. Аппаратно – программная инфраструктура, на которой функционирует АСОРИ, описывается на пятом уровне абстракции.

Анализ GIS - системы, как АСОРИ, проводился на каждом уровне абстракции. Результаты анализа представлены в таблице 1:

Таблица 1

Первый уровень	GIS – системы имеют четкий, давно устоявшийся режим использования. Выделяется следующие задачи: 1. Подготовка визуализация GIS – информации - оформление информации в электронном виде. 2. Лицензионное распространение информации клиентам. 3. Замкнутый программно – технический комплекс на базе GIS – систем. Объединение первых двух задач в одном комплексе.
Второй уровень	Функции, поддерживающие требуемые бизнес процессы интегрируются в единый законченный продукт. Они не требуют и не допускают модификаций, поскольку выражены в визуализации результатов тех или иных запросов. Функции чувствительны к состоянию данных, поскольку существуют семантические взаимосвязи между данными. Права и полномочия по обработке информации можно зафиксировать в разнообразных рабочих пространствах (Workspace).
Третий уровень	Механизмы, привлекаемые услугами третьего уровня, являются внутрисистемными (OS), стандартными и не могут быть модифицированы пользователями. Интегрированные оболочки в основном привлекают объекты типа Windows для визуализации и услуги доступа к структурированным данным (DataBase).
Четвертый уровень	Данные GIS – системы хранятся в структурированных файлах согласно существующим стандартам. Формат данных различен. Интегрированные оболочки допускают некоторые варианты выбора хранения данных - структурированные файлы, свободные таблицы, базы данных, промышленные СУБД.
Пятый уровень	Инфраструктура представляет собой отдельное автоматизированное рабочее место или одно-ранговую сеть с клиентскими местами, с установленными Windows 95/98.

Введение уровней абстракции позволило сформулировать следующие требования к СБ АСОРИ:

- СБ есть система заданная на объекте - АСОРИ.
- АСОРИ не может предоставлять свои услуги без функционирования СБ.
- СБ работает непрерывно, все события, проходящие в АСОРИ должны быть обработаны и/или санкционированы СБ.

- Механизмы защиты информации объединяются в один комплекс. Если протокол использования данного механизма невозможно включить в этот комплекс, тогда должна быть компенсация его отсутствия.
- СБ проектируется с учетом представления на каждом уровне абстракции.

С учетом особенностей и возможности модификаций реализации GIS-системы, была выработана обобщающая схема реализации СБ. Были выделены отдельные компоненты, которые требуют различных схем использования механизмов защиты информации. Их интеграция в единую систему должно проводится с учетом уникальности конкретной задач.

Первый компонент: *Запуск ПО GIS – системы.*

Второй компонент: *Организация рабочего места (Workspace) с учетом полномочий пользователя.*

Третий компонент: *Безопасное хранение информации и защита от несанкционированного копирования.*

Четвертый компонент: *Направленная передача GIS – информации клиенту с поддержкой установленных правил лицензирования.*

Перечисленные компоненты СБ GIS – системы были реализованы с учетом упрощения их интеграции в единую систему, в соответствии с результатами системного анализа

II Компоненты защиты информации в GIS – системах

Запуск ПО GIS - технологии.

Запуск программного обеспечения контролируется Операционной Системой (ОС). Запуск выполняется в два этапа:

- запуск сервера , где хранятся GIS - информация (Windows NT);
- запуск клиентской станции, которая используется для доступа пользователя к GIS - информации (Windows 95/98).

Все действия контролируются ОС, что дает право предположить, что данный компонент эквивалентен Системе Защиты от Несанкционированного Доступа (СЗ НСД) к общим ресурсам в режиме контроля запуска на выполнение. Анализ показал, что использование аутентификации ОС не является надежным, поскольку используемые в них механизмы хорошо изучены. Разработка же этих механизмов велась с учетом более низкого уровня защищенности, чем может потребовать GIS – информация. Представленные на рынке дополняющие системы аутентификации имеют слабый интерфейс с GIS – системой. Отсутствие подобного интерфейса делает невозможным построение непрерывной защиты информации.

Предлагается контроль запуска серверной компоненты возложить на организационные мероприятия. С этой целью сам компьютер оборудуется специальным дополнительным устройством санкционирования включения аппаратных средств.

Все рабочие станции необходимо оборудовать специально разработанным программно-аппаратным комплексом аутентификации пользователя. Сам комплекс есть расширение стандартных механизмов аутентификации и использует дополнительный идентификатор на базе Touch Memory. Внутри комплекса, после проведения аутентификации сохраняются параметры данного пользователя. Эти параметры даже в памяти компьютера не находятся в открытом состоянии, а открываются на минимально требуемое время, для подтверждения своих прав.

Для доступа к серверу используется Имя пользователя и результат работы функции **F(“Имя”, “Пароль”, “код Touch Memory”).**

При запуске ОС проводится строгая аутентификация (в соответствии с рекомендациями X. 509) на клиентском месте. При негативном результате процедуры аутентификации блокируется консоль данного рабочего места, что автоматически приводит к невозможности работать с GIS - системой. Процедура аутентификации производится во время функционирования GIS - системы в установленном порядке (рисунок 1).

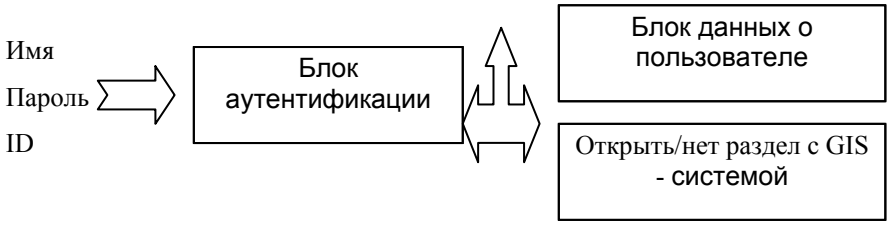

Рисунок 1

Организация рабочего места (Workspace) с учетом полномочий пользователя

GIS - системы предоставляют возможность сформировать для каждого пользователя рабочее место в соответствии с его полномочиями. Описание этого рабочего места находится в файле, который имеет достаточно простую структуру. Следовательно, создание и редактирование этого файла может проводиться вне GIS – системы.

Сам файл (файлы) или его (их) описание хранится в блоке данных о пользователе (рисунок 2). Доступ к нему возможен по результатам процедуры аутентификации (описание первого компонента). Получить содержимое файла несанкционированно нет возможности поскольку он зашифрован с использованием параметров пользователя. Модификация содержимого возможно при разрешении администратора, поскольку хеш - функция на хранящейся в ней информации считается на параметрах СБ.

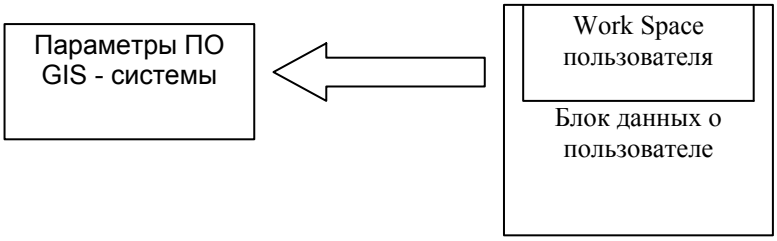

Рисунок 2

Проблема запрета формирования новой рабочей области при работающем ПО GIS – системы решается автоматически, так как файл описания рабочей области сохраняется как параметр пользователя. Следовательно, его изменения эквивалентны расширению полномочий пользователя, что происходит с привлечением администратора GIS - технологии.

Безопасное хранение информации и защита от несанкционированного копирования.

Этот компонент легко реализуется благодаря тому, что в GIS - системах хранение GIS - информации и ее обработка разнесены.

В том случае, когда GIS - информация сохраняется в отдельных структурированных файлах, содержимое этих файлов обрабатывается криптографическими алгоритмами. Параметры этих криптографических преобразований, как и полномочия по доступу к ним может получить пользователь, параметры которого предусматривают получение параметров преобразований – задача, эквивалентна задаче распределения параметров криптографических преобразований. Организация и структура доступа к данным подробно описаны в проекте. Ниже приводится лишь общая схема (рисунок 3).

Поскольку, логической единицей есть “слой”, шифрование слоя ведется на отдельном наборе параметров (ключи и прочее). Параметры шифрования слоя зашифровываются на “вторичных системных ключах”. Набор “Вторичных системных ключей” поставляются в блок данных о пользователе. Там они сохраняются в зашифрованном виде на мастер – ключе пользователя.

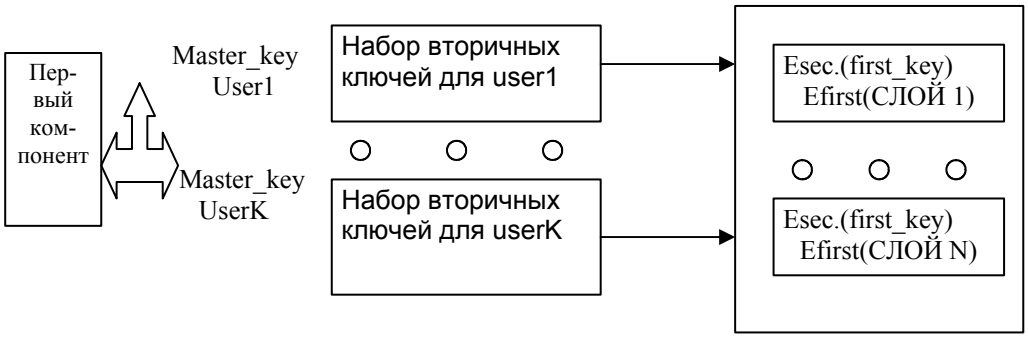

Рисунок 3

Если для хранения GIS – информации используется СУБД с хорошей системой безопасности, схема претерпевает некоторые изменения (рисунок 4). В основу будут положены механизмы защиты СУБД и своеобразие организации способа хранения информации (структурированный файл, Data Base, общий файл,

прочее). Есть смысл создать некоторый сервер (Front End), который проверяет полномочия посланного запроса на информацию. При этом данные о пользователе можно сохранять средствами той же СУБД.

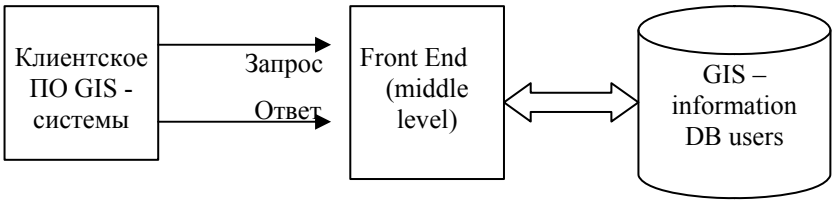

Рисунок 4

Направленная передача GIS – информации клиенту с поддержкой установленных правил лицензирования.

Подготовленная GIS – информация может передаваться внешним организациям без права распространения. Такая передача может быть: полной – информация передается один раз и полностью; пополняемая – дополнение к ранее переданной. Каждый из вариантов имеет свою реализацию.

- Полная:

Вне зависимости от носителя – CD, Hard disk, other – данные шифруются. Доступ к данным возможен через специальный Soft или драйвер. Параметры шифрования согласуются с параметрами работы конкретного спец. ПО и параметрами пользователя.

Следовательно. Фирма, которая готовит GIS – информацию, должна обладать комплексом "лицензирования" этого предоставления информации.

- Пополняемая:

Если фирма–получатель обладает второй и третьей компонентой, тогда вопрос решается достаточно просто.

Пополнение информации проходит с носителя (CD) в файлы или СУБД при помощи специального "Загрузчика", задача которого не только перекачать информацию, но и аутентифицировать как источник, так и приемник информации. Пополнение информации происходит лишь при положительном результате аутентификации.

При отсутствии второй и третьей компоненты у фирмы получателя, эту задачу решить нельзя.

III Вопросы интеграции СБ в общую структуру GIS – системы

Особый интерес представляют предприятия GIS – система которых представляет собой интегрированный комплекс, при помощи которого производится замкнутый цикл обработки GIS – информации. В технологическом цикле идет создание информации, контроль содержимого, визуализация и нанесение информации на твердый носитель.

По определению, для построения СБ такой GIS – системы будет интегрироваться в единую службу три первых компонента. Ключевым моментом есть способ хранения GIS- информации.

Если для хранения информации используется промышленная СУБД, то основные функции возлагаются на создаваемый транзакционный сервер (Front End). Мы имеем четкую, централизованную систему, которая может поддерживать любую принятую политику безопасности. К этому транзакционному серверу можно подключить АРМ администратора безопасности, на котором реализуются функции учета, арбитража и аудита. На рабочих местах сохраняется информация, необходимая для работы подсистемы аутентификации.

Если информация сохраняется в отдельных файлах, то схема построения усложняется. Ключевым моментом СБ в такой GIS – системе есть информационное взаимодействие между компонентами. Такое взаимодействие проводится на базе параметров пользователя. Следовательно, основной упор в организации СБ делается на разработку подсистемы аутентификации, имеющий хороший гибкий интерфейс с механизмами как ОС, так и с реализацией криптографических преобразований. Информация для работы СБ, механизмы присутствуют в каждом элементе инфраструктуры предприятия. Учет и контроль за изменениями необходимо делать как на уровне сервера, так и на уровне рабочих мест.