УДК 504:001+551.501

ЗАЩИТА ГИС-ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ КЛЮЧЕЙ

М.Т. Ибрагимов

В статье рассматриваются возможности защиты данных ГИС (электронные карты, пространственные базы данных, и др.) с использованием электронных ключей. Рассматриваются возможные плюсы и минусы данной технологии.

На сегодняшний день во всем мире широко используются Геоинформационные Системы (ГИС) – средства пространственного анализа данных. Они применяются как различными государственными структурами и учреждениями (например, военные ведомства, исследовательские институты, органы власти и управления и др.), так и коммерческими организациями (например, для решения задач прокладывания на карте оптимального маршрута грузоперевозок, и т.п.). Нельзя обойтись без карт в географии, гидрографии, метеорологии, сейсмологии и других науках, связанных с исследованием нашей планеты.

В отличие от западных стран, где ГИС-данные создаются в больших количествах и используются повсеместно, в нашей стране общедоступные данные в удобных для использования цифровых форматах только начинают появляться. Это сдерживает использование ГИС в решении различных актуальных задач (в основном, ГИС сейчас используют в органах государственной власти и управления, а также в крупных компаниях). Но, тем не менее, процесс внедрения и распространения ГИС все-таки идет. Рынок насыщается цифровой картографической продукцией. Но данная продукция имеет некоторые особенности.

Цифровые топографические основы отличает высокая себестоимость работ по их созданию. Следовательно, возникает вопрос об авторских правах на цифровые карты. Карты, как и другая информация, как правило, являются интеллектуальной собственностью их создателя. Высокой ценностью обладает тематическая информация цифровых карт, используемая в ГИС. Очевидно, что содержание цифровых карт, которые используются в военных целях, также не является информацией общего

пользования. Картографические данные, несущие определенную информацию, в большинстве случаев имеют некоторую ценность для организаций использующих ГИС, и, как следствие, требуют организации ограничения доступа к ним.

Широкое применение сетевых технологий при работе с ГИС имеет немало преимуществ (например, одновременный доступ к цифровым картам, возможность обращения к картографическим базам данных, обмен данными без использования автономных носителей и т. п.). Но наравне с преимуществами имеются и недостатки (возрастает возможность утечки данных из корпоративной сети, несанкционированного доступа к конфиденциальной картографической информации).

Поэтому достаточно актуальной стала проблема защиты цифровых карт и картографических баз данных от несанкционированного доступа и пиратского копирования. К сожалению, как показывает опыт, административно воспрепятствовать данным правонарушениям чрезвычайно сложно.

Программно – аппаратные решения данной проблемы существуют, но и они не являются универсальными. Таким образом, на сегодняшний день, различные источники, связанные с защитой информации, выделяют два основных способа защиты цифровых карт: *с помощью встроенных средств ГИС*, а также *программных и аппаратных решений сторонних производителей*.

Очевидно, что наиболее удобным для пользователя было бы решение данной проблемы в рамках программных продуктов ГИС. Но, к сожалению, разработчики не торопятся встраивать системы защиты цифровых карт в свои программные продукты, так как это не соответствует их коммерческим интересам (цифровые карты - бесплатно, программные продукты - за деньги). Имеющиеся в некоторых программных продуктах возможности создают только иллюзию защиты и не являются проблемой для знающих людей. Так, например, в *ArcView 3.2a*, все пароли, предназначенные для блокировки "тем" (Themes), вы можете легко обнаружить в файле **.apr* просто поискав теги с именами *"password"*№ используя обычный текстовый редактор (например, Блокнот (*Notepad*), входящий в стандартный состав пакета *Windows*):

(FTheme.15
Name: "Index"
Source: 16
Password: "**Key_word**"

Flags: 0x15
Legend: 32
Threshold: 45
View: 5
GSet: 46
LegEditScript: "View.EditLegend"
TxPos: 47
LabelField: 26)

Ввиду этого, в настоящее время, использование лишь специализированных продуктов сторонних производителей является, пожалуй, серьезным и, наверное, единственным решением данной проблемы. На сегодняшний день самый распространенный вид программно-аппаратной защиты данных – *электронные ключи*. Данные устройства позволяют защищать цифровую карту (т.е. файлы из которых она состоит) с помощью специальных алгоритмов шифрования.

Реализация защиты с помощью электронных ключей должна производится так, чтобы пользователи, работающие с защищаемыми файлами данных, имели бы полный доступ к ним (как на чтение, так и на запись). В то же время необходимо обеспечить, чтобы информация, содержащаяся в файлах, не выходила, в своем исходном виде, за пределы некоторого ограниченного "пространства" (локального компьютера, организации) или была растиражирована в строго определенном количестве экземпляров. При этом заранее считается, что пользователи не заинтересованы в обеспечении защиты организационными методами.

Наиболее известными фирмами, занимающиеся производством электронных ключей и предоставляющих описанный метод обеспечения безопасности данных, являются фирмы: *Aladdin, Eutron, Rainbow* и др.

Каким образом функционирует система защиты с использованием электронных ключей?

Рассмотрим вышеприведенный рисунок, на котором отображена упрощенная схема обеспечения защиты на программном и аппаратном уровне при чтении информации. Программа, считывающая и интерпретирующая данные в каком-либо файле, обращается к диску компьютера (или какому-либо логическому устройству) для считывания данных посредством вызова специальных функций операционной системы (подсистема ввода-вывода). Она получает данные из участка файла, интерпретирует их

и затем записывает (при необходимости) обратно на диск. Решение проблемы состоит в том, чтобы перехватить операции "чтения-записи" либо на уровне операционной системы, либо на аппаратном уровне и провести дешифрирование-шифрование считываемых или записываемых данных.

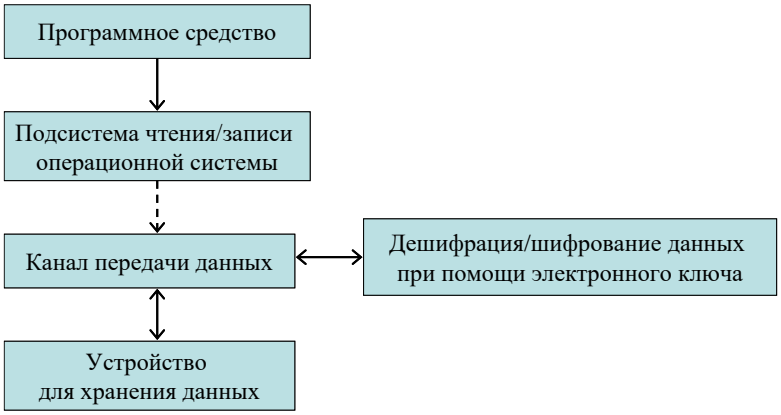

Рис. Схема обеспечения защиты при помощи электронного ключа.

Как с точки зрения пользователя выглядит работа с защищенными данными?

1) В параллельный, последовательный, *USB* или *PCMCIA* порт компьютера устанавливается специальное устройство: ключ. Его назначение: идентифицировать легальность копии и генерировать код для шифрования/дешифрирования данных. Ключи или аппаратные платы шифрования могут так же устанавливаться в слоты внутри компьютера,

2) Инсталлируется особый драйвер (эта операция чрезвычайно проста и не требует задания каких-либо параметров для инсталляции),

3) Доступ к защищенным файлам осуществляется только в том случае, если ключ остается подключенным к компьютеру. В противном случае программное средство перестает "узнавать" данные файлы и генерирует ошибку (при этом, как правило, стабильность его работы не нарушается). Для работы с защищенными файлами программное средство ГИС должно быть специальным образом подготовлено поставщиком карты.

4) В случае если осуществляется копирование защищенного файла средствами ГИС-продукта, то созданная копия так же будет зашифрованной (но не обязательно, это зависит от настроек установленных поставщиком карты)

5) При работе с защищенными файлами наблюдается некоторое замедление работы (как правило, незначительное), вызванное осуществлением операций кодирования/декодирования.

Рассмотрим достоинства и недостатки защиты электронных карт с помощью электронных ключей.

К достоинствам можно отнести следующее: 1) Простота в инсталляции и эксплуатации; 2) Реализация достаточного уровня защиты посредством шифрования/дешифрования; 3) Совместимость со всеми видами платформ.

К недостаткам: 1) Потеря ключа (по любой причине) приводит к потере данных, поскольку работа с ними без ключа невозможна; 2) Случаи сбоев в портах *LPT* и *USB* также приводят к проблемам в работе программы.

Резюмируя все выше сказанное можно отметить, что данный метод достаточно эффективен (простота реализации для конечного пользователя и достаточный уровень безопасности), но защищать свои данные подобным методом могут только крупные компании, создающие и распространяющие ГИС-данные. Поскольку они могут позволить себе заказать производство электронных ключей для всего объема данных, чего нельзя сказать о небольших компаниях.

Казахский научно-исследовательский институт экологии и климата

ЭЛЕКТРОНДЫҚ КІЛТ КӨМЕГІМЕН ГХЖ – МӘЛІМЕТТЕРІН ҚОРҒАУ

М.Т. Ибрагимов

Мақалада электрондық кілт көмегімен ГХЖ мәліметтерін (электрондық карта, мәліметтің кеңістіктік базасы т.б.) қорғаудың мүмкіндіктері қарастырылады. Берілген технологияның артықшылықтары мен кемшіліктері талданады.