



УДК 004.9:528.9

Сергей ЛЕВЧИК, заместитель заведующего отделом геоинформационных технологий РУП «БелНИЦзем»

## ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ГЕОГРАФИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ И ЗАЩИТЫ КАРТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ

(на примере Государственного комитета по имуществу Республики Беларусь)

Настоящая статья посвящена вопросам обеспечения безопасности государственных географических информационных систем. В статье предпринимается попытка описания новых концептуальных подходов к задачам обеспечения информационной безопасности геоинформационных систем.

### Введение

Государственные информационные ресурсы стали одним из главных источников информационной мощи как государства в целом, так и отдельных финансовых, научно-исследовательских и производственных субъектов в частности.

Информация, учитывая ее доступность и скорость распространения средствами Интернет, в современном мире активно влияет на все сферы жизнедеятельности не только отдельных обществ и государств, но и всего мирового сообщества. Однако в определенных случаях информация может использоваться не только во благо, но и во вред интересам личности, общества и государства. Поэтому роль информационной безопасности в системе национальной безопасности не только существенно возрастает, но и выходит на первый план.

На взгляд автора, в контексте государственной информационной политики, речь должна идти не только об обеспечении условий для реализации прав граждан, юридических лиц и государства на свободное получение, распространение и использование информации, но и о необходимости защиты и рациональном использовании государственных информационных ресурсов, защите конфиденциальной информации и интеллектуальной собственности.

Настоящая статья посвящена безопасности государственных географических информационных систем. Автор обратился к этой теме потому, что обеспечение конфиденциальности,

защищенности данных в информационных системах Государственного комитета по имуществу Республики Беларусь (далее – Госкомимущества) является необходимым условием доверия пользователей к информации предоставляемыми такими системами.

В целях создания защищенных информационных систем и обеспечения защиты картографо-геодезической информации (далее – геоинформации), необходимо решить две взаимоувязанные задачи:

1) создание систем, с которыми пользователь мог бы чувствовать себя комфортно и безопасно, информация которых защищена от искажений, подделки, хищений;

2) обеспечение защиты информационных ресурсов не только внутри создаваемых систем, а и за ее пределами.

### Теоретическое обоснование

Если посмотреть на один из аспектов безопасности информации – обеспечение безопасности в неконтролируемом окружении, то данная проблематика в Госкомимуществе недостаточно разработана, и защита информации обеспечивается в основном организационно-правовыми мерами (особенно это касается защиты картографической информации).

Значительная часть картографической информации, передается пользователям незащищенной техническими методами, и пользователь сам должен обеспечить защиту информации, что недопустимо, учитывая известные сегодня технические методы защиты. В связи с этим представляется необходимым проведение

исследований, разработка, внедрение технических методов защиты информационных ресурсов, имеющих в распоряжении Госкомимущества и подчиненных ему предприятий, в том числе информационного ресурса картографо-геодезического фонда Республики Беларусь (Госкартгеофонда).

### Основная часть

Во избежание разночтений в терминологии, определим два основных аспекта информационной безопасности, имеющие, на взгляд автора, принципиальное значение для исследуемой темы: безопасность систем и информации в контролируемом окружении и безопасность систем и информации в неконтролируемом окружении.

В контексте данной статьи под безопасностью в контролируемом окружении понимается обеспечение безопасности государственной информационной системы, функционирующей в организации, которая обеспечивает защиту этой системы и информации в ней от угроз исходящих извне организации.

Под безопасностью в неконтролируемом окружении понимается обеспечение безопасности системы или информации, переданных в организации, ведомства или любым другим пользователям, которые не могут или не должны проводить мероприятия по защите получаемой ими информации. Данный аспект безопасности становится все более актуальным в связи с развитием карманных компьютеров, смартфонов, коммуникаторов, навигаторов и обычных мобиль-

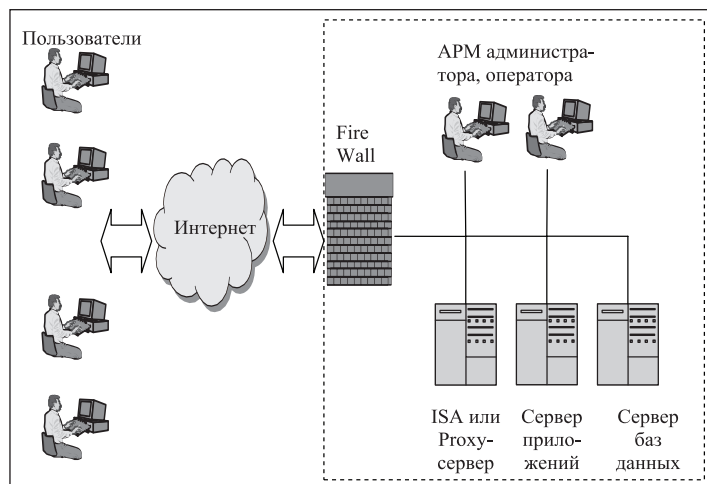


Рисунок 1. Схема структуры государственной информационной системы.

ных телефонов. Как пример, можно упомянуть цифровые навигационные карты, которые передаются пользователям персональных навигаторов GPS. Такие системы или информация должны иметь встроенные механизмы, которые способны автономно обеспечивать защиту от несанкционированного доступа, копирования, внесения ложной информации и других угроз безопасности.

Для обоих этих аспектов можно определять безопасность информации, исходя из трех основных показателей: обеспечивает ли система безотказную (надежную) работу, защиту информации и является ли обеспечение безопасности экономически целесообразным.

Ситуация с обеспечением защиты информационных ресурсов в Госкомимуществе и подчиненных ему предприятиях, является типичной для большинства министерств и ведомств Республики Беларусь, где до недавнего времени защита информации обеспечивалась в основном организационными или организационно-правовыми мерами, но с развитием информационных технологий акценты защиты информации все чаще стали смещаться в сторону технических мер.

Для защиты государственных информационных ресурсов Госкомимуществе проводятся исследования и разрабатываются концепции информационной безопасности. В частности, специалистами ГУП «Национальное кадастровое агентство», при участии УП «Научно-исследовательский институт технической защиты информации» была разработана подсистема защиты информации Единого государственного регистра недвижи-

мого имущества, прав на него и сделок с ним (ЕГРНИ). Однако данной разработкой определен полный комплекс организационно-технических мер обеспечивающих защиту информации ЕГРНИ в контролируемом окружении,

когда доступ к информации, перечень пользователей информации являются контролируемыми параметрами безопасности.

Типичная структура государственной информационной системы представлена на рисунке 1.

FireWall – комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов.

ISA или Proxy-сервер – служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам;

АРМ – автоматизированное рабочее место.

За защиту информации отвечают аппаратный или программный FireWall, а также ISA или Proxy-сервер. Пунктирной линией обведена область контроля безопасности внутри организации – владельца информационной системы. Здесь хорошо видно, что защита информации осуществляется исключительно в контролируемом окружении, причем по внутренней сети информация, как правило, передается в открытом виде. Данное архитектурное решение на сегодняшний день уже не соответствует существующим потребностям отрасли, не обеспечивает необходимый уровень защиты информации и требует совершенствования.

Если же посмотреть на другой обозначенный автором аспект безопасности – обеспечение безопасности в неконтролируемом окружении, то работы в данном направлении начаты Госкомимуществом, но сегодня защита информации обеспечивается в основном организационно-

правовыми мерами, особенно это касается защиты геоинформации, и в частности, цифровых карт. Так, цифровые карты, передаются пользователю в открытом виде, и пользователь уже сам отвечает за обеспечение защиты информации, что недопустимо.

В этой связи практический интерес представляет правовое обеспечение защищенности цифровых карт, как объекта требующего наиболее полного комплекса мер защиты, по следующим причинам:

1) Цифровые карты являются результатом творческой деятельности и защищаются законами об авторском праве (Закон Республики Беларусь от 16 мая 1996 года «Об авторском праве и смежных правах»).

2) В Республике Беларусь в текущем году принята новая редакция закона «О геодезической и картографической деятельности».

3) Как информационный продукт, цифровые карты попадают под действие законов об информации (Закон Республики Беларусь «Об информации, информатизации и защите информации»).

4) Цифровые карты являются потенциально важным объектом для обеспечения национальной безопасности и обороноспособности Республики Беларусь.

5) Для выхода на зарубежный рынок отечественная геоинформационная продукция должна соответствовать мировым стандартам.

Ситуация осложняется отсутствием правовых документов, однозначно регулирующих использование картографической продукции, а также практически полным отсутствием судебной практики в этой области.

Важнейшим источником белорусского авторского права являются международные договоры и соглашения. Однако, как показывает практика применения авторского права к цифровым картам в разных странах, национальные законодательства большинства стран до настоящего времени не имеют четких правовых документов по этому вопросу (возможно, за исключением Великобритании). При решении вопросов создания и использования цифровой картографической информации в зарубежных странах, как правило, правовое регулирование осуществляет-

ся по трем направлениям: авторское право, охрана баз данных и конкуренция.

В Республике Беларусь данные вопросы частично регламентируются Законом Республики Беларусь «О геодезической и картографической деятельности», который констатирует, что «Геодезические и картографические материалы и данные являются объектами интеллектуальной собственности. Защита авторских прав на использование объектов интеллектуальной собственности, полученных в результате геодезической и картографической деятельности, осуществляются в соответствии с законодательством об интеллектуальной собственности», а также частично Законом Республики Беларусь «Об авторском праве и смежных правах» и Гражданским кодексом Республики Беларусь.

Таким образом, на взгляд автора, имеет место недостаточное развитие законодательной базы в данной области. Поэтому в коммерческих договорах на поставку геоинформационной продукции, в том числе за рубеж, особое внимание следует уделить вопросам авторского права и защиты геоинформации.

В целях урегулирования пробелов, имеющих в законодательстве Республики Беларусь по вышеприведенным вопросам, Госкомимуществом (РУП «БелНИЦзем») разрабатываются нормативные документы, посвященные вопросам правовой охраны материалов Госкартгеоцентра.

Самостоятельной проблемой является распространение геоинформации (цифровых карт) по сети Интернет. Вопросы правового регулирования авторских прав в сети Интернет в настоящее время являются предметом активных дискуссий. Предлагаемые в них решения в полной мере могут быть применимы и к картографическим произведениям.

Однако защиту информации ни законы, ни организационные мероприятия не обеспечат, если для этого не будут использованы эффективные технические средства. Автор недаром остановился на характерном примере обеспечения безопасности цифровых карт. Из вышесказанного видно, что их защита, как в организационно-правовом, так и в техническом плане, совершенно не адекватна их ценно-

сти, в том числе и для национальной безопасности и обороноспособности Республики Беларусь. Таким образом речь идет не только о защите информации от копирования, но и том, что государство должно иметь возможность ограничить публичный доступ к информации в случае, когда такой доступ может иметь нежелательное влияние на:

а) конфиденциальность действий органов государственной власти и местного самоуправления;

б) международные отношения, общественную безопасность или национальную оборону;

в) деятельность судебных органов, на ход судебного процесса или способность государственного органа вести следствие уголовного или дисциплинарного характера;

г) конфиденциальность торговой или промышленной информации;

д) конфиденциальность персонализированных данных;

е) интересы или охрану любого лица;

ж) охрану окружающей среды.

Как уже говорилось выше, защита информации является комплексом нормативно-технических и организационных мер, и поэтому параллельно с развитием нормативной правовой базы необходимо разрабатывать способы технической защиты цифровой картографической информации, уделяя особое внимание методам обеспечения безопасности в неконтролируемом, недружественном окружении.

Разумеется, не существует абсолютно надежных способов защиты информации. Но любые способы защиты должны быть направлены на минимизацию последствий действий нарушителя безопасности. В то же время определение способов защиты информации напрямую зависит от характера и типа угроз, от метода, которым осуществляется «взлом» информационного ресурса, его иное повреждение либо несанкционированное копирование. Рассмотрим несколько примеров технических методов защиты информации цифровых карт.

Наиболее стойким к «взлому» является метод, использующий вычисления на удаленном сервере. В этом случае пользователь у себя на компьютере вводит исходные данные

или формирует запрос и передает их серверу, возможно, используя защищенные каналы информации. Затем, данные или запрос обрабатываются на сервере, и сервер передает пользователю только результат обработки. При этом минимизируется обмен защищаемой информацией и, соответственно, минимизируются угрозы безопасности.

Но для передаваемых пользователю цифровых карт такой метод защиты не применим. Для подобных случаев широко используется метод защиты информации, когда информация зашифровывается с помощью общего для всех пользователей ключа, сгенерированного с помощью специальных алгоритмов, и передается пользователям в зашифрованном виде. Для расшифровки полученной информации, пользователь использует ключ, который формируется на основе идентификатора компьютера пользователя и идентификатора информации. К сожалению, такой метод защиты можно легко обойти, подменив идентификатор компьютера.

Автор может предложить несколько методов обеспечения защиты информации в недружественном окружении, которые, на его взгляд, способны обеспечить адекватную защиту информации.

В этих методах цифровая карта или иная геоинформация зашифровывается с помощью специальных алгоритмов, и передается пользователям в зашифрованном виде и для расшифровки используется одна из приведенных ниже технологий.

**Метод 1.** Метод заключается в создании библиотеки, программные элементы которой встраиваются в программное обеспечение информационной системы. Расшифровка полученной информации осуществляется с использованием функций этой библиотеки. Данный метод обеспечивает надежную защиту для обычных информационных систем и информации, не имеющей государственного значения.

**Метод 2.** Создание программного элемента, который будет работать в адресном пространстве программного обеспечения информационной системы, но не будет являться частью программного обеспечения. Этот программный элемент и производит рас-



шифровку полученной информации. Данный способ может быть менее надежным, чем Метод 1, так как он использует внешние, по отношению к информационной системе, процедуры.

**Метод 3.** Создание аппаратного устройства, являющегося промежуточным звеном между устройством хранения зашифрованной информации и информационной системой (информацией). Алгоритмы шифрования (ключи) могут храниться в этом устройстве, которое и осуществляет расшифровку. Этот метод является наиболее надежным и может применяться для обеспечения защиты конфиденциальной информации, имеющей государственное значение. Но данный метод наиболее сложен и дорогостоящ в реализации.

Существуют и иные способы защиты информации, в том числе при передаче информации в сети Интернет, но их соответствие сегодняшним пожеланиям по обеспечению защиты цифровой картографической информации требует, по мнению автора, дополнительного изучения.

В любом случае, каждый из методов защиты информации требует дополнительной проработки по оценке его применимости для решения именно задачи защиты геоинформации, в том числе и с обязательной оценкой экономических показателей для выбора наиболее оптимальных решений.

В качестве основы для структуризации решений по обеспечению защиты информации, можно использовать предложенный в стандарте ISO/IEC 27001:2005 цикл Шухарта-Деминга [6] (рисунок 2).

СМЗИ – Системы Менеджмента Защиты Информации.

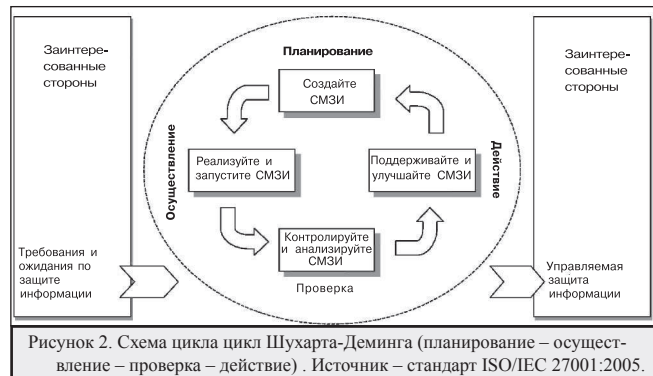
В заключение хотелось бы отметить, что успех обеспечения безопасности геоинформации в системе Го-

ском имущества будет зависеть в том числе и от выполнения комплекса мероприятий, осуществляемых на общегосударственном и международном уровнях. Это такие мероприятия как:

- активизация участия в совершенствовании системы международных договоров и нормативных правовых актов международных организаций, участником которых является Республика Беларусь, в том числе Содружества Независимых Государств;
- развитие и совершенствование системы обучения персонала по вопросам информационной безопасности;
- совершенствование законодательства, регулирующего отношения в области электронного документооборота и использование электронной цифровой подписи;
- создание условий для развития отечественной индустрии средств защиты информации, обеспечения технологической независимости Республики Беларусь в важнейших областях информатизации, включая разработку отечественных операционных систем на основе открытого программного обеспечения
- урегулирование вопросы использования импортных аппаратных и программных средств защиты информации;
- развитие системы сертификации современных информационных технологий, средств информатизации, телекоммуникации и связи в соответствии с современными требованиями безопасности информации;
- совершенствование государственной системы защиты информации в Республике Беларусь;
- совершенствование правовых механизмов борьбы с правонарушениями в области защиты картографо-геодезической информации;
- разработка методики по оценке размера ущерба, причиняемого правонарушениями в информационной сфере;
- создание системы страхования информационных рисков.

**ЛИТЕРАТУРА**

1. Закон Республики Беларусь от 16 мая 1996 года «Об авторском праве и смежных правах».
2. Закон Республики Беларусь от 5 мая 1999 года «О научно-технической информации».
3. Закон Республики Беларусь от 10 января 2000 года «Об электронном документе».
4. Закон Республики Беларусь от 10 июня 2008 года «О геодезической и картографической деятельности»
5. Закон Республики Беларусь «Об информации, информатизации и защите информации». Принят палатой представителей Республики Беларусь 9 октября 2008 года.
6. ISO/IEC 27001:2005 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования.
7. СТБ 34.101.1–2001 Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
8. СТБ 34.101.2–2001 Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
9. СТБ 34.101.3–2001 Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Часть 3: Гарантийные требования безопасности.
10. «Основы информационной безопасности. Учебное пособие для вузов» Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. Горячая линия – Телеком, – 2006.
11. Домарев, В.В. «Безопасность информационных технологий. Методология создания систем защиты». – К.: ТИД Диа Софт, – 2002.
12. Щеглов, А. «Защита конфиденциальной информации и персональных данных в современных условиях. Задачи и возможности реализации». <http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=21687>.
13. В.Л. Цирлов «Основы информационной безопасности автоматизированных систем краткий курс». – Феникс, – 2008.



информационной сфере; – создание системы страхования информационных рисков.

Фото Я. Ждановой