Т.М. Татарникова

ЗАДАЧА СИНТЕЗА КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ГИС

T.M. Tatarnikova

THE PROBLEM OF SYNTHESIS OF AN INTEGRATED SECURITY SYSTEM IN GIS

Приводится структурно-функциональная модель ГИС, из которой определены элементы, подверженные угрозам информационной безопасности. Перечислены наиболее характерные виды угроз для ГИС. Выполнена постановка задачи синтеза системы защиты информации в ГИС и раскрыты этапы ее решения.

Ключевые слова: Информационная безопасность, угроза, система защиты информации, вероятность угрозы, комплексное решение.

Provides structural and functional model of GIS, which sets out the elements at risk for information security. Are the most typical types of threats for a GIS. Formulation of the problem is made of synthesis of information security in the GIS and disclosed the steps of the solution.

Key words: Information security, threat, security system, the probability of threats, comprehensive solution.

Введение

Обеспечение информационной безопасности ГИС, как и для любой неоднородной сложной информационной системы, решается с применением комплексного подхода, который в соответствии с общей концепцией информационной безопасности включает вопросы конфиденциальности, доступности и целостности информации [2].

Для различных ГИС, решающих определенные задачи требуется соответствующая стратегия по защите данных. В ситуации, когда ГИС используется для решения корпоративных задач, карты и их содержание обладают коммерческой ценностью. Поэтому необходимо обеспечить как конфиденциальность хранимой и передаваемой информации, так и разграничение доступа к ней. В ситуации же, когда используется ГИС массового использования, больший упор должен быть сделан в сторону защиты информации от повторного использования. В свою очередь, стоит обратить внимание, что при организации защиты ГИС государственного значения помимо разработки технических и программных средств согласно требованиям федеральной службы по техническому и экспортному контролю необходима сертификация систем и средств защиты информации и аттестацию объектов информатизации по требованиям безопасности [1].

Структурно-функциональные элементы ГИС, подверженные угрозам информационной безопасности

ГИС, как систему в целом, можно разделить на несколько структурно-функциональных элементов, среди которых выделим следующие:

– автоматизированное рабочее место пользователя (АРМ), которое включает в себя системное и прикладное программное обеспечение (ПО), а именно: средства хранения, ввода и вывода информации.
– сетевой сервер, содержащий специализированное программное обеспечение, используемое для хранения данных ГИС. Сервер содержит средства хранения, ввода и вывода информации, а также системное и прикладное ПО. Помимо перечисленного неотъемлемой частью является система управления базами данных (СУБД).
– телекоммуникационная система, обеспечивающая передачу информации по каналам связи (Internet, выделенные каналы). Составляющими, снабженными специальным программным обеспечением, являются модем и маршрутизатор, который пересылает пакеты данных между различными сегментами сети, и в случае необходимости принимает решения о пересылке.

Также в состав ГИС помимо АРМ пользователя входят и иные служебные рабочие места. Речь идет о программистах, техническом персонале, администраторе сети и администраторе безопасности – все они важны при организации любой значительной структуры ГИС.

Ниже на рис. 1 схематически отображена модель ГИС.

Во время информационного взаимодействия структурно-функциональных элементов ГИС между собой и с внешней средой возникает вероятность возникновения угрозы. Наиболее характерными видами угроз для ГИС являются:

– кража информации и носителей информации, несанкционированное копирование. Данный вид угроз возникает на этапах первоначального сбора информации средствами ввода, получение доступа к которым и является причиной возникновения угрозы.
– перехват информации по линиям электропитания и по посторонним проводникам за счет побочного электромагнитного излучения или по акустическому каналу. Такие угрозы возникают во время доставки или обмена информацией между различными АРМами и сервером с применением телекоммуникационной системы.
– подмена данных. Данный вид угроз возможен на этапе вывода информации при получении злоумышленником несанкционированного доступа вследствие слабой системы аутентификации и идентификации, в том числе разграничения прав доступа.
– уничтожение программного обеспечения, данных ГИС, файлов, в том числе паролей и ключевой информации. Данному виду угроз подвержены средства хранения информации.
– ошибки при установке различного программного обеспечения (ПО), операционной системы и базы данных, а так же при написании и эксплуатации ПО. Угрозы этого вида характерны для сервера ГИС при получении несанкционированного доступа к нему.

– подмена или модификация операционных систем, систем управления базами данных, прикладных программ, различных данных, ключевой информации и правил доступа. Такой вид угроз направлен на сервер ГИС.
– нарушение правил доступа, иными словами, взлом. Угроза направлена на сервер ГИС после успешной реализации предыдущей угрозы.
– уменьшение скорости обработки информации, пропускной способности каналов связи, объемов свободной оперативной памяти и дискового пространства, нарушение электропитания. Эта угроза является некоторым следствием реализации выше перечисленных угроз.

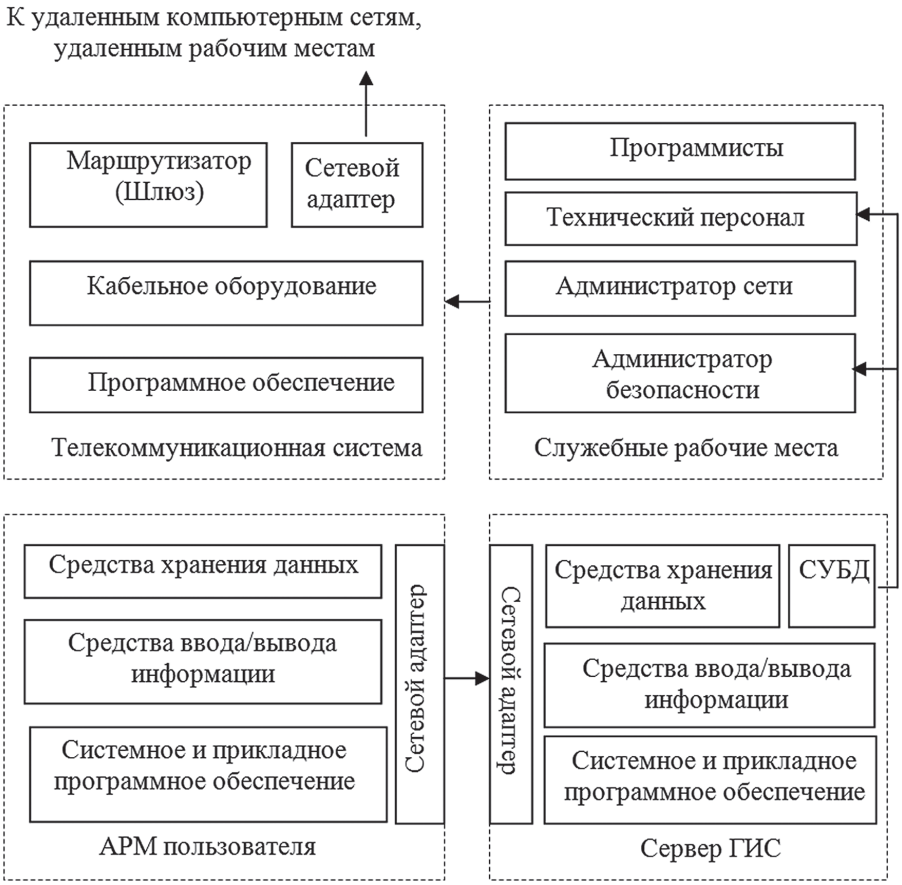

Рис. 1. Структурно-функциональная модель ГИС

Таким образом, широкий спектр угроз для безопасности ГИС говорит о необходимости использования комплекса защитных мер по обеспечению безопасности данных в ГИС.

Комплекс защитных мер по обеспечению безопасности данных в ГИС

Согласно ГОСТ Р ИСО/МЭК 17799-2005 информационная безопасность в информационных системах в целом сводится к защите конфиденциальности, целостности и доступности.

Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям. Другими словами каждый пользователь должен получать доступ только к информации, для которой у него есть необходимые права.

Целостность: обеспечение достоверности и полноты информации и методов ее обработки. Иными словами данные не должны быть изменены при их хранении, передачи или представлении.

Доступность: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости. Иными словами беспрепятственная реализация прав доступа субъектами, авторизованных в системе, к информации в соответствии с политикой доступа.

Конфиденциальность в ГИС решается криптографическими методами, среди которых важное место занимает шифрование. К примеру, при использовании мобильного приложения ArcGis, пользователям ГИС предоставляется возможность применить шифрование КЭШ-памяти своего мобильного устройства. Для приложений ArcPad применяется шифрование файла данных и карт памяти. В ГИС «Панорама» встроены средства шифрования пространственных данных 256-битным ключом при отправке и получении, что предотвращает перехват или подмену данных в процессе передачи. Отметим, что применение шифрования уменьшает скорость передачи данных – время задержки составляет от 3 до 10 процентов от общего времени.

Другой способ обеспечения конфиденциальности данных – это предоставление доступа только авторизованным пользователям (субъектм доступа), который решается через задачу разграничения доступа. Субъектом доступа называется лицо или процесс, действия которого регламентируются правилами разграничения доступа. В ГИС субъектом доступа могут быть сотрудники, которые наделены уникальными идентификаторами, и которые являются пользователями сети. Сетевые потоки, которые обеспечивают связь между сотрудником и сервером ГИС, или сетевые потоки, которые являются запросами к базе данных ГИС, также являются субъектами доступа.

Методы разграничение доступа (в основном по паролю) широко распространен в ГИС от КБ «Панорама», программах компании ESRI – ArcGis, ArcSDE, в службах Oracle Advanded Security и СУБД Oracle.

Постановка задачи синтеза системы защиты информации в ГИС

Пусть информация ГИС подвержена некоторой совокупности угроз со стороны злоумышленника. Каждая угроза характеризуется вероятностью появления и наносимым ущербом. Уменьшение общего ущерба, наносимого ГИС обеспечивается применением системы защиты информации (СЗИ).

Введем следующие обозначения:

P_i – вероятность появления i-й угрозы, $i = \overline{1,n}$;
q_i – ущерб, наносимый i-й угрозой;
$\overline{W}$ – общий предотвращенный ущерб ГИС;
$\overline{w}_i$ – предотвращенный ущерб за счет ликвидации воздействия i-й угрозы;
$P_i^{\text{устр}}$ – вероятностью устранения каждой i-й угрозы.

Тогда, задачу синтеза системы защиты информации в ГИС в общем виде сформулируем следующим образом: выбрать вариант реализации СЗИ, обеспечивающий максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на СЗИ [3].

Формальная постановка задачи примет вид: найти

$$T^{\text{доп}} = \max \overline{W}(T), \quad T^{\text{опт}} \in T^{\text{доп}} \tag{1}$$

при ограничении

$$C = \left(T^{\text{доп}}\right) \le C_{\text{доп}}, \tag{2}$$

где C – вектор стоимости аппаратной реализации СЗИ; T – вектор, характеризующий вариант аппаратной реализации СЗИ; $T^{\text{доп}}$, $T^{\text{опт}}$ – допустимое и оптимальное значение вектора T; $C_{\text{доп}}$ – допустимые затраты на СЗИ.

Для решения задачи необходимо сформировать показатель качества функционирования системы защиты информации $\overline{W}(T)$.

Тогда, предотвращенный ущерб в общем виде выражается соотношением:

$$\overline{W} = F\left(P_i, q_i, P_i^{\text{устр}}\right), \quad i = \overline{1,n}. \tag{3}$$

Предотвращенный ущерб за счет ликвидации воздействия i-й угрозы:

$$\overline{w}_i = P_i \cdot q_i \cdot P_i^{\text{устр}}, \quad i = \overline{1,n}. \tag{4}$$

При условии независимости угроз и аддитивности их последствий получаем

$$\overline{W} = \sum_{i=1}^{n} P_i \cdot q_i \cdot P_i^{\text{устр}}. \tag{5}$$

Вероятность появления i-й угрозы P_i определяется статистически и соответствует относительной частоте ее появления

$$P_i = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} = \overline{\lambda}, \tag{6}$$

где λ_i – частота появления i-й угрозы.

Ущерб q_i, приносимый i-й угрозой может определяться в абсолютных единицах: экономических потерях, временных затратах, объеме уничтоженной или «испорченной» информации и т.д. Однако, на практике оценить ущерб затруднительно, особенно

на ранних этапах проектирования СЗИ. Целесообразно вместо абсолютной оценки ущерба использовать относительную, который представляет собой степень опасности i-й угрозы для ГИС. Степень опасности может быть определена экспертным путем в предположении, что все угрозы для ГИС составляют полную группу событий, то есть

$$0 \le q_i \le 1,\ \sum_{i=1}^{n} q_i = 1$$

Наиболее сложным вопросом является определение вероятности устранения i-й угрозы $P_i^{\text{устр}}$ при проектировании СЗИ. Примем допущение о том, что эта вероятность определяется тем, насколько полно учтены качественные и количественные требования к СЗИ при их проектировании, то есть

$$P_i^{\text{устр}} = f_i\left(x_{i1},\ldots,x_{ij},\ldots,x_{im}\right), \tag{7}$$

где x_{ij} – степень выполнения j-го требования к СЗИ для устранения i-й угрозы, $i = \overline{1,n}$; $j = \overline{1,m}$.

Пусть первые k требований будут количественными ($j = \overline{1,k}$) остальные ($m–k$) – качественными ($j = \overline{k+1,m}$).

Степень выполнения j-го количественного требования определяется его близостью к требуемому (оптимальному) значению. Для оценки степени выполнения j-го количественного требования к СЗИ удобнее всего использовать его нормированное значение $x_{ij}(j = \overline{1,k})$, $0 \leqslant x_j < 1$.

Для нормирования удобно использовать функцию вида

$$\overline{x}_{ij} = \frac{x_{ij} - x_{ij}^{\text{нх}}}{x_{ij}^{\text{нл}} - x_{ij}^{\text{нх}}}, \tag{8}$$

где x_{ij} – текущее значение j-го требования; $x_{ij}^{\text{нл}}$, $x_{ij}^{\text{нх}}$ – наилучшее и наихудшее значения.

Степень выполнения j-го качественного требования определяется функцией принадлежности к наилучшему значению $\mu(x_{ij})$.

Разложив функцию (8) в ряд Макларена и ограничившись первыми членами ряда, получим

$$P_i^{\text{устр}} = P_i^{\text{устр}}\left(0\right) + \sum_{i=1}^{m} \frac{\partial P_i^{\text{устр}}}{\partial x_{ij}} \cdot x_{ij}. \tag{9}$$

где $P_i^{\text{устр}}(0) = 0$ – вероятность устранения i-й угрозы при невыполнении требований и СЗИ; $\dfrac{\partial P_i^{\text{устр}}}{\partial x_{ij}}$ – величина, характеризующая степень влияния j-го требования на вероятность устранения i-й угрозы (важность выполнения j-го требования для устранения i-й угрозы), $0 \leqslant \alpha_{ij} < 1$; $\sum_{i=1}^{m} \alpha_{ij} = 1$ для $i = \overline{1,n}$.

После подстановки в (9) соответствующих значений получаем

$$P_i^{\text{устр}} = \sum_{j=1}^{n} \alpha_{ij} \bar{x}_{ij} + \sum_{j=k+1}^{m} \alpha_{ij} \mu\left(x_{ij}\right). \tag{10}$$

Окончательно формула (5) для оценки величины $\overline{W}$ предотвращенного ущерба принимает вид

$$\overline{W} = \sum_{i=1}^{n} \sum_{j=1}^{k} \bar{\lambda} q_i \alpha_{ij} \bar{x}_{ij} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \bar{\lambda} q_i \alpha_{ij} \mu\left(x_{ij}\right). \tag{11}$$

Таким образом, задача синтеза СЗИ в виде (1), (2) сводится к оптимальному обоснованию количественных и качественных требований к СЗИ при допустимых затрат и принимает следующий вид [4]:

Найти

$$\max \overline{W}\left(x_0, i = \overline{1,n}, j = \overline{1,m}\right) \tag{12}$$

при ограничении

$$C\left(x_{ij}\right) \le C_{\text{доп}}; \quad i = \overline{1,n}; \quad j = \overline{1,m}.$$

При отсутствии информации об угрозах для решения задачи (12) может быть использован показатель вида

$$\overline{W} = \sum_{i=1}^{n} \sum_{j=1}^{k} \alpha_{ij} \bar{x}_{ij} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \alpha_{ij} \mu\left(x_{ij}\right).$$

Этапы решения задачи

В соответствии с формулировкой задачи (12) основными этапами ее решения являются:

- сбор и обработка экспертной информации о характеристиках угроз: частоте появления i-й угрозы $\bar{\lambda}$ и ущербе q_i, $i = 1,n$;
- сбор и обработка экспертной информации для определения важности выполнения j-го требования для устранения i-й угрозы α_{ij} и функции принадлежности x_{ij}, $i = 1,n$; $j = 1,m$;
- оценка стоимости СЗИ для конкретного варианта ее реализации, зависящая от степени выполнения требований x_{ij}, $i = 1,n$; $j = 1,m$;
- разработка математической модели и алгоритма выбора рационального варианта построения СЗИ в соответствии с постановкой (12) как задачи нечеткого математического программирования.

Литература

1. *Бабенко Л.К., Басан А.С., Журкин И.Г., Макаревич О.Б.* Защита данных геоинформационных систем: учеб. пособие для студентов вузов. / Под ред. И.Г. Журкина. – М.: Гелиос АРВ, 2010. – 336 с., ил.
2. *Бескид П.П., Татарникова Т.М.* О некоторых подходах к решению проблемы авторского права в сети Интернет. // Ученные записки РГГМУ, 2010, № 15.
3. *Татарникова Т.М., Яготинцева Н.В.* Постановка задачи синтеза комплексной защиты от воздействия угроз в телекоммуникационной системе. // Информационные технологии и системы: управление, экономика, транспорт, право. Межвузовский сборник научных трудов. Выпуск 1(9). – СПб., 2011.
4. *Татарникова Т.М., Яготинцева Н.В.* Принципы организации экспертной системы выбора надежных средств защиты информации VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России». Санкт-Петербург, 26–28 октября 2011 г.