DOI: 10.17117/na.2016.01.01.521

<http://ucom.ru/doc/na.2016.01.01.521.pdf>

Поступила (Received): 29.01.2016

Татарникова Т.М., Яготинцева Н.В. Модель обеспечения информационной безопасности ГИС

Tatarnikova T.M., Yagotinceva N.V.
Model of information security 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

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

Татарникова Татьяна Михайловна

*Доктор технических наук, профессор
Санкт-Петербургский государственный
университет аэрокосмического приборостроения
г. Санкт-Петербург, ул. Большая Морская, 67*

Tatarnikova Tatiana Mikhailovna

*Doctor of Engineering Sciences, Professor
Saint-Petersburg state university of aerospace
instrumentation
St. Petersburg, Bolshaya Morskaya st., 67*

Яготинцева Наталья Владимировна

*Аспирант
Российский государственный
гидрометеорологический университет
г. Санкт-Петербург, Малоохтинский проспект, 98*

Yagotinceva Natalia Vladimirovna

*Graduate
Russian state hydrometeorological university
Saint-Petersburg, Malookhtinsky ave., 98*

Обеспечение информационной безопасности ГИС, как для любой неоднородной сложной информационной системы, решается с применением комплексного подхода [1, с. 69]. Для различных ГИС, решающих определенные задачи требуется обеспечить как конфиденциальность хранимой и передаваемой информации, так и разграничение доступа к ней [2, с. 15].

Структурно-функциональными элементами ГИС, подверженным угрозам информационной безопасности являются:

- автоматизированные рабочие места пользователей (АРМ);
- серверы, содержащие специализированное программное обеспечение, используемое для хранения и обработки данных ГИС, базы данных [3, с.38];
- телекоммуникационная система, обеспечивающая передачу информации по каналам связи [4, 5, с. 1883];

Во время информационного взаимодействия структурно-функциональных элементов ГИС между собой и с внешней средой возникает вероятность возникновения угрозы. Наиболее характерными из них являются [6]: кража информации и носителей информации, несанкционированное копирование; перехват информации по линиям электропитания и по посторонним проводникам за счет побочного электромагнитного излучения или по акустическому каналу; подмена данных; уничтожение программного обеспечения, данных ГИС, файлов, в том числе паролей и ключевой информации; ошибки при установке различного программного обеспечения (ПО), операционной системы и базы данных, а так же при написании и эксплуатации ПО; подмена или модификация операционных систем, систем управления базами данных, прикладных программ, различных данных, ключевой информации и правил доступа; нарушение правил доступа, иными словами, взлом; уменьшение скорости обработки информации, пропускной способности каналов связи [7, с. 37], объемов свободной оперативной памяти и дискового пространства, нарушение электропитания.

Широкий спектр угроз безопасности ГИС говорит о необходимости использования комплексного подхода к обеспечению безопасности ГИС.

Пусть каждая угроза со стороны злоумышленника характеризуется вероятностью появления и наносимым ущербом. Уменьшение общего ущерба, наносимого ГИС обеспечивается применением системы защиты информации (СЗИ) и необходимостью моделирования для оценки этого ущерба [8].

Задачу синтеза СЗИ сформулируем как задачу выбора варианта реализации СЗИ, обеспечивающего максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на реализацию СЗИ [9, с. 28].

Формальная постановка задачи примет вид: найти

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

при ограничении

$$C = (T^{\text{доп}}) \leq C_{\text{доп}}, \quad (2)$$

где $\bar{W}$ – общий предотвращенный ущерб ГИС;

T – вектор, характеризующий вариант аппаратной реализации СЗИ;

$T^{\text{доп}}, T^{\text{опт}}$ – допустимое и оптимальное значение вектора T ;

C – вектор стоимости аппаратной реализации СЗИ;

$C_{\text{доп}}$ – допустимые затраты на СЗИ.

Предотвращенный ущерб при условии независимости угроз и аддитивности их последствий выражается соотношением:

$$\bar{W} = \sum_{i=1}^n P_i \cdot q_i \cdot P_i^{\text{устр}} \quad (3)$$

где P_i – вероятность появления i -й угрозы, $i = \overline{1, n}$; q_i – ущерб, наносимый i -й угрозой; $P_i^{\text{устр}}$ – вероятностью устранения каждой i -й угрозы.

Вероятность P_i определяется статистически и соответствует относительной частоте 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.п.

Наиболее сложным 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

$$P_i^{\text{устр}} = f_i(x_{i1}, \dots, x_{ij}, \dots, x_{im}) \quad (4)$$

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 ($j = \overline{k + 1, m}$). Тогда степень выполнения j -го количественного требования может быть определена его близостью к требуемому (оптимальному) значению, а для оценки степени выполнения j -го количественного требования к СЗИ можно использовать его нормированное значение $\bar{x}_{ij}(j = \overline{1, k})$, $0 \leq x_{ij} < 1$. Степень выполнения j -го качественного требования определять функцией принадлежности к наилучшему значению.

Тогда основными этапами решения поставленной задачи являются:

- сбор и обработка экспертной информации о характеристиках угроз: частоте появления i -й угрозы и наносимом ею ущербе;
- сбор и обработка экспертной информации [10, с. 142] для определения важности выполнения j -го требования для устранения i -й угрозы и функции принадлежности x_{ij} , $i = \overline{1, n}$; $j = \overline{1, m}$;
- оценка стоимости СЗИ для конкретного варианта ее реализации, зависящая от степени выполнения требований x_{ij} , $i = \overline{1, n}$; $j = \overline{1, m}$;
- разработка математической модели и алгоритма выбора рационального варианта построения СЗИ.

Список используемых источников:

1. Советов Б.Я., Колбанев М.О., Татарникова Т.М. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности // Геополитика и безопасность. 2014. № 1. С. 69-77.
2. Воробьев А.И., Колбанев М.О., Татарникова Т.М. Оценка вероятностно-временных характеристик процесса предоставления информационно-справочных услуг // Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 15-18.
3. Колбанев М.О., Пойманова Е.Д., Татарникова Т.М. Физические ресурсы информационного процесса сохранения данных // Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 38-42.
4. Курузов О. И., Сергеев В. Г., Татарникова Т. М. Коммутаторы в корпоративных сетях. Моделирование и расчет. СПб: Судостроение, 2003.
5. Tatarnikova T., Kolbanev M. Statement of a task corporate information networks interface centers structural synthesis // IEEE EUROCON-2009. St. Petersburg, 2009. С. 1883-1887.
6. Татарникова Т.М. Задача синтеза комплексной системы защиты информации в ГИС // Ученые записки Российского государственного гидрометеорологического университета. 2013. № 30. С. 204-211.
7. Колбанев М.О., Татарникова Т.М., Воробьев А.И. Модель балансировки нагрузки в вычислительном кластере центра обработки данных // Информационно-управляющие системы. 2012. № 3. С. 37-41.
8. Курузов О.И., Татарникова Т. М. Моделирование систем и сетей телекоммуникаций. СПб.: РГГМУ, 2012.
9. Колбанев М.О., Татарникова Т.М., Малков К.О. Подход к организации адаптивного согласующего центра корпоративной сети // Информационно-управляющие системы. 2008. № 3. С. 28-31.
10. Татарникова Т.М., Яготинцева Н.В. Принципы организации экспертной системы выбора структуры локальной сети корабля // Современное общество, образование и наука. Тамбов, 2015. С. 142-144.