УДК 004.056.5

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ

Кузнецов К. В.
Студент-магистрант
ФГБОУ ВО "МГУ им. Н. П. Огарёва",
Россия, Саранск

Аннотация

В связи с развитием цифровизации, распространившейся во все сферы жизни человека, использование информационных систем становится повсеместным. Поэтому возникает вопрос безопасного использования этих систем. Актуальность темы исследования заключается в том, что для принятия эффективных управленческих решений необходимо использовать современные информационные технологии, которые смогут представить в доступном виде требуемую информацию. Цель исследования – исследовать методы безопасного использования ГИС-систем. Научная новизна статьи заключается в обзорном исследовании современных решений безопасности информационных систем. ГИС – интегрированная система, основанная на работе с большим объемом географических данных, используемых в различных целях. Главная задача остается в обеспечении безопасности информационных систем. Современные технологии должны отвечать всем требованиям безопасности данных, основанных на качественном анализе системы на предмет угроз. В ходе исследования были выделены основные угрозы безопасности, их классификация и способы защиты информации с учетом новейших решений и технологий.

Ключевые слова: геоинформационная система (ГИС); информация; информационная безопасность; данные.

SECURITY ISSUES IN USING GEOINFORMATION SYSTEMS

Kuznetsov K.V.
master student
National Research Mordovia State University,
Russia, Saransk

Annotation

In connection with the development of digitalization, which has spread to all spheres of human life, the use of information systems is becoming widespread. Therefore, the question arises of the safe use of these systems. The relevance of the research topic is that for the adoption of effective management decisions it is necessary to use modern information technologies that can present the required information in an accessible form. The purpose of the study is to investigate methods for the safe use of GIS systems. The scientific novelty of the article lies in a survey of modern solutions to the security of information systems. GIS is an integrated system based on working with a large amount of geographic data used for various purposes. The main task remains to ensure the security of information systems. Modern technologies must meet all data security requirements based on a qualitative analysis of the system for threats. During the study, the main threats to security, their classification and ways of protecting information, taking into account the latest solutions and technologies, were identified.

Keywords: geographic information system (GIS); information; Information Security; data.

Геоинформационная система (*сокращенно ГИС*) – это метод цифрового картографирования, который связывает данные с географическим положением. ГИС основана на сборе, хранении, анализе и географической визуализации

пространственных данных и связанной с ними информацией об объектах. ГИС-система позволяет анализировать, искать и заниматься редактированием цифровых карт. Также благодаря инструменту ГИС можно получить такую информациях об объектах как высота здания, адрес, количество жильцов и т.п. [4].

Преимущества использования геоинформационных систем трудно переоценить, главная эффективность применения ГИС зависит от стратегически правильного составленного плана работы в зависимости от выбранной специфики задачи [3].

Компоненты геоинформационных систем включаются следующие пункты: программное обеспечение (хранение, визуализация информации); аппаратное (стационарный компьютер); данные (самый важный компонент); исполнители (технический персонал) [3].

Информация об объектах в ГИС-системе хранится в виде тематических слоев, которые объединены в зависимости от их положения (географического). Географическая информация включает сведения о положении в пространстве (адресные ссылки и т.). Также к преимуществам ГИС можно отнести функциональность карты как динамичной системы; лёгкости в использовании и управлении; высокий уровень автоматизации; доступная визуализация данных, возможность вносить изменения в исходные данные [3].

Первые ГИС-технологии были разработаны в середине XX века в США и Канаде. Наиболее масштабной из них была CGIS (Canada Geographic Information System), разработанная под руководством английского географа Роджера Томлинсона. Основными задачами данной ГИС были картографирование земельных ресурсов и их классификация [2].

Большую роль в ускорении развития геоинформационных технологий сыграло появление бесплатных ГИС. В их числе стоит отметить GRASS (Geographic Resources Analysis Support System), которая разрабатывалась по заказу США, но в 1994 году была выпущена для бесплатного пользования всем желающим, и ее стали активно применять различные частные компании, программисты и обычные пользователи для решения задач, связанных с планированием землеустройства, картографирования, а также разработки собственных приложений [2].

Безопасность при использовании геоинформационных систем основана на таких важнейших пунктах – сохранение, защита информации и поддержание жизнеобеспечения инфраструктуры от преднамеренного мошеннического вмешательства. Основные принципы безопасности при использовании геоинформационных систем: конфиденциальность данных, целостность хранящейся информации, надежность доступа к информации со стороны уполномоченных лиц [1].

Прогресс в области развития информационных систем и технологий порождает и новые проблемы, связанные со структурой безопасности данных.

Угроза безопасности может быть как с внутренней, так и внешней стороны, в том числе и естественные угрозы и искусственно созданные [5].

- Естественные угрозы безопасности могут быть связаны с природными факторами, данные угрозы не зависят от манипуляций человека.
- Искусственные угрозы основаны антропогенном вмешательстве, делятся на преднамеренные (с целью завладеть или нарушить целостность информации) или непреднамеренные (по неосторожности или незнанию).
- Внутренние угрозы – внутри системы ГИС (нарушение работоспособности программных устройств).

- Внешние – за пределами (нарушение работоспособности технических устройств).

Преднамеренные угрозы считаются самыми опасными, т.к. оно наносят самый значительный ущерб деятельности геоинформационных технологий. Поэтому, чтобы обезопасить программный комплекс от угроз нужно уделять больше времени информационной безопасности.

Средства защиты информации подразделяются на следующие категории по своему воздействию.

- Организационные представляют собой совокупность организационно-технических средств, в том числе и организационно-правовые средства;
- Программные средства, основанные на защите, контроле информации;
- Аппаратные средства – технические устройства.

Следовательно, на основе данных угроз, можно выделить задачи, которые нужно учитывать:

- запрет на несанкционированный доступ;
- своевременное обнаружение несанкционированного проникновения и устранение причин последствий.

Основные способы, которые необходимы при запрете несанкционированного доступа, является подтверждение прав доступа пользователей в систему или доверенных лиц, включает следующие этапы:

- идентификация пользователя;
- установление подлинности – аутентификация.

Идентификатор – это последовательность символов (пароль), сохраненная в базе администратора службы безопасности. Благодаря идентификация, система не будет воспринимать проникновение в ресурс как угрозу [6].

Аутентификация основана на более сложной процедуре проверке, включая технические средства, которые проверяют индивидуальные характеристики человека (отпечатки пальцев, голос и т.п.).

Чаще всего пользователи используют пароли для защиты данных. Пароли подразделяются на простые или же динамически изменяющиеся. Простой пароль остается неизменным от сеанса к сеансу. А сложный – подвержен изменению. Сложный может выдавать как «запрос-ответ» или же модифицировать простые пароли [5].

Далее нужно учитывать, какие права имеются в наличии у пользователей для доступа к ресурсам. Они могут иметь как полный доступ, так и частичный или же временный. Защита информационных данных от копирования предлагает криптографические способы защиты информации. Криптография заключается в преобразовании исходной текстовой информации в шифротекст. В шифре можно выделить такие основные элементы – шифр и ключ. Ключ задается алгоритмическое значение параметров [5].

Также может возникнуть угроза доступа к данным, которые называются «остаточными» в оперативной внешней памяти. Уничтожениями остаточных данных сейчас занимаются специализированные программы и утилиты [4].

В настоящее время геоинформационная система (ГИС) является современной интегрированной системой, которая отвечает требованиям и запросам современного общества. Поэтому обеспечение ГИС-системы современными средствами защиты информации от несанкционированного доступа, кражи и нанесении ущерба данных в системе, следует уделять больше внимания. В проведенном обзоре угроз безопасности и методах защиты информации можно сделать вывод, что выявление угрозы на начальном этапе может предотвратить похищение ценной информации. Злоумышленники также могут нарушить целостность данных, что станет угрозой для безопасности всей

системы. Исходя из предложенных методов защиты ГИС информации, самым актуальным остается использование, идентификации и аутентификации в комплексе с более сложными паролями, а для сохранения данных от хищения следует использовать шифрование с помощью криптографических методов.

Библиографический список:

1. Быкова Н. Н. Обеспечение безопасности информационных систем / Н. Н. Быкова, В. А. Волкова // Молодой ученый. – 2015. – № 23. – С. 43-46.

2. Дупленко А. Г. Этапы и тенденции развития геоинформационных систем / А. Г. Дупленко // Молодой ученый. – 2015. – № 9. – С. 115-117.

3. Журкин И. Г. Геоинформационные системы / И. Г. Журкин, С. В. Шайтура. – М.: Кудиц-пресс, 2009. – 272 с.

4. Капралов Е. Г. Геоинформатика / Е. Г. Капралов, А. В. Кошкарев и др. – М.: Академия, 2010. – 480 с.

5. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А. Ю. Щербаков. – М.: Книжный мир, 2009. – 352 с.

6. Явтуховский Е. Ю. Современные технологии защиты информации в распределённых системах / Е. Ю. Явтуховский, С. О. Кошелев // Молодой ученый. – 2016. - № 28 [Электронный ресурс]. — Режим доступа — URL: https://moluch.ru/archive/132/36986/ (Дата обращения 12.05.2020)

Оригинальность 91%