МОНАХОВ М.Ю., д.т.н.,проф. кафедры ИЗИ

АСТАФЬЕВА Е.С., студентка группы КЗИ-108

АНАЛИЗ ВОЗМОЖНОСТЕЙ И МЕТОДОВ ВИЗУАЛИЗАЦИИ СОСТОЯНИЯ И ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СЕТИ ПРЕДПРИЯТИЯ

Основной задачей является исследование всевозможных способов визуализации данных, которые анализируются администратором безопасности предприятия для оптимизации процесса принятия решений и обеспечения более высокого уровня защищенности информационной системы на предприятии.

Обеспечение информационной безопасности на предприятии является очень актуальной проблемой и на сегодняшний день в этой области сложилась достаточно четко очерченная система концептуальных взглядов. Полноценная информационная безопасность предприятий и организаций подразумевает непрерывный контроль в реальном времени всех важных событий и состояний, влияющих на безопасность данных. Защита должна осуществляться круглосуточно и круглогодично и охватывать весь жизненный цикл информации - от её поступления или создания до уничтожения или потери актуальности.

Для комплексной защиты информации от возможных угроз необходимо использовать различные средства безопасности. А вместе с ростом количества средств защиты существенно увеличивается и объём информации, которую должен обработать администратор безопасности. Это в свою очередь приводит к увеличению времени, которое должен тратить оператор для анализа всей информации, поступающей от различных средств защиты для принятия адекватных решений по реагированию на выявленные атаки. Исходя из этих критериев, самым наглядным и практичным средством является визуализация и картографирование, то есть представление состояний информационной безопасности в виде карт.

Основной целью работы является общее изучение возможных способов визуализации состояния защищенности информации на предприятии, процессов сбора и анализа информации, поступающей от различных средств защиты для последующей помощи в принятии решений и

реагированию на выявленные угрозы. Для этого необходимо изучить возможные методы графического представления аналитических данных применимо к данной тематике, сравнить их и выбрать самые оптимальные и перспективные для дальнейшего их использования в разработке определенной модели мониторинга и обеспечения информационной безопасности предприятия.

Сегодня на мировом рынке существуют готовые решения, наглядно реализующие процессы управления информационной безопасностью для крупных информационных сетей на предприятиях. **Системой мониторинга** называется комплекс программно-технических средств, предназначенных для автоматизации процесса сбора и анализа событий информационной безопасности. В западной терминологии системы мониторинга обозначаются аббревиатурой SIM (Security Information Management) или SIEM (Security Information and Event Management).

В настоящее время наибольшее распространение получили следующие коммерческие системы мониторинга событий информационной безопасности: ArcSight, Cisco MARS, RSA Envision, NetForensics, NetIQ, Symantec, и др. Необходимо отметить, что кроме коммерческих существуют также и бесплатные системы мониторинга с открытым кодом. Примером такой системы является продукт Prelude Universla SIM.

Для визуализации результатов работы подобных систем используется консоль администратора, которая в реальном режиме времени позволяет проводить разделение событий по категориям, корреляцию событий, как по ресурсам, так и по злоумышленникам, а также осуществлять подробный анализ. С помощью карты нарушений безопасности можно получить представление об отклонениях в параметрах безопасности. Также консоль предоставляет возможности для подготовки табличных и графических отчетов о безопасности. На сегодняшний день всё больше и больше компаний приходят к пониманию того, что использование систем мониторинга позволяет значительно повысить эффективность процесса

обнаружения и реагирования на инциденты информационной безопасности. Это обеспечивается за счет автоматизации процесса сбора и анализа информации, которая регистрируется в автоматизированной системе компании.

Данные системы являются достаточно хорошим средством визуализации, но зачастую они охватывают только информационную безопасность компьютерной сети предприятия, не учитывая другие виды угроз и соответственно не использующие технические и организационные меры по защите информации. Поэтому с помощью таких систем нельзя рассчитать и проанализировать общее состояние защищенности информационной системы предприятия, поэтому их можно использовать в комплексе с другими продуктами.

К задаче визуализации данных сводится проблема представления в наглядной форме данных эксперимента и результатов теоретического исследования. Традиционные инструменты в этой области – графики и диаграммы – плохо справляются с задачей визуализации, когда возникает необходимость изобразить более трех взаимосвязанных величин. Очевидно, что графики и диаграммы являются самыми доступными и распространенными способами представления результатов анализа данных, в том числе и для оценки защищенности информационной безопасности. На примере систем мониторинга можно еще раз в этом убедиться. В основном подобные системы используют достаточно скромный набор стандартных линейных графиков и диаграмм (круговые, столбчатые). Но существуют и другие интересные виды, которые можно использовать при анализе защищенности информационной сети.

В качестве основных применений методов визуализации можно указать следующие:

- наглядное представление геометрической метафоры данных;

- лаконичное описание внутренних закономерностей, заключенных в наборе данных;
- сжатие информации, заключенной в данных;
- восстановление пробелов в данных.

В качестве дополнительных возможных средств представления визуальных данных о состоянии информационной безопасности предприятия можно использовать двумерные диаграммы рассеяния, вероятностные графики, категоризованные тернарные графики, трехмерные гистограммы.

На сегодняшний день также существует мощнейший инструмент изображения информации – это большой арсенал ГИС-технологий. Географическая информационная система (ГИС) - это современная компьютерная технология для картографирования и анализа объектов реального мира, а также событий, происходящих в нем. Эта технология объединяет традиционные операции работы с базами данных, такими как запрос и статистический анализ, с преимуществами полноценной визуализации и географического (пространственного) анализа, которые предоставляет карта. Эти возможности отличают ГИС от других информационных систем и обеспечивают уникальные возможности для ее применения в широком спектре задач, связанных с анализом и прогнозом явлений и событий. В ГИС карта становится действительно динамическим объектом в смысле:

- изменяемости масштаба;
- преобразования картографических проекций;
- варьирования объектным составом карты;
- возможности опрашивать через карту в режиме реального времени
- многочисленные базы данных;

- изменения способа отображения объектов (цвет, тип линии и т.п.), в том числе и определения символогии через значения атрибутов, то есть синхронизации визуализации с изменениями в базах данных;
- легкости внесения любых изменений.

ГИС помогает ускорить и повысить эффективность процедуры принятия решений, обеспечивает ответы на запросы и функции анализа пространственных данных, представления результатов анализа в наглядном и удобном для восприятия виде. Требуемая для принятия решений информация может быть представлена в лаконичной картографической форме с дополнительными текстовыми пояснениями, графиками и диаграммами. Именно поэтому я считаю, что использование ГИС и составление карт для визуализации процессов и входящих данных является очень важным и полезным средством для администратора безопасности предприятия.

На сегодняшний момент существует достаточно много различный ГИС, которые применяются для различных целей и в разных областях деятельности людей. Среди них можно выделить такие как ArcView GIS, Geographic Resources Analysis Support System (GRASS), Quantum GIS (QGIS), System for Automated Geoscientific Analyses (SAGA) и др.

В результате, были проанализированы способы графического представления и обработки многомерных данных, которые могут поступать администратору безопасности о состоянии защищенности информационной сети предприятия. Среди таких способов визуализации можно выделить представление данных в виде графиков, диаграмм, гистограмм, пиктограмм, а также карт, основанных на применении ГИС. Каждый из этих способов в свою очередь может быть наиболее эффективен для определенного рода подзадач, которые решает администратор безопасности. На сегодняшний

день не существует единого комплекса мониторинга и управления информационной безопасностью предприятия, который бы охватывал весь основной перечень угроз, касающийся не только компьютерной сети передачи данных. Исходя из этого, целью дальнейшей работы будут более глубокие исследования в области визуального представления данных, в особенности применения геоинформационных систем, а также работа будет направлена на создание общего комплекса мониторинга состояния информационной безопасности, который сможет способствовать повышению качества и эффективности работы администратора безопасности на предприятии.

Литература

1. Замай С.С., Якубайлик О.Э. Программное обеспечение и технологии геоинформационных систем: учеб. пособие: Красн. гос. университет. Красноярск, 1998 г., 110 с.
2. Сердюк В.А., генеральный директор ЗАО «ДиалогНаука» - «Практический опыт построения комплексных систем мониторинга информационной безопасности», материалы конференции «ИНФОФОРУМ 2012»
3. Зиновьев А.Ю. Визуализация многомерных данных. - Красноярск: Изд-во КГТУ, 2000.
4. Зиновьев А.Ю., Питенко А.А. Картографирование произвольных данных. // "Студент и научно-технический прогресс": Информационные технологии. Материалы XXXVIII международной научной студенческой конференции.- Новосибирск: НГУ.- 2000.
5. Зиновьев А.Ю., Питенко А.А. Система визуализации произвольных данных. // 2-я Всероссийская научно-техническая конференция "Нейроинформатика-2000". Ч.1. М.: МИФИ.- 2000

6. Горбань А.Н., Зиновьев А.Ю., Питенко А.А. Визуализация данных методом упругих карт // Информационные технологии, изд-во "Машиностроение". - М. - 2000. № 6
7. Эйдензон Д., Шамрони Д, Корпорация NovoSpark, Воловоденко В. Визуализация и анализ многомерных данных с использованием пакета NovoSpark® Visualizer, Ватерлоо, Канада
8. Дьяченко Н.В. Использование ГИС-технологий в решении задач управления. - http: // www. nocnit. ru/2st/materials/Diachenko. html
9. Графические методы анализа данных, http://www.statsoft.ru
10. Лукацкий А.В., Информационная безопасность и геоинформационные системы, PC Week/RE № 8, 2001
11. Журкин И. Г., Шайтура С. В. Геоинформационные системы. — М., «КУДИЦ-ПРЕСС», 2009
12. Капралов Е.Г., Кошкарев А.В. , Тикунов В.С. и др.; под ред. Тикунова В.С., Основы геоинформатики: В 2-х кн. Кн. 1: учеб. пособие для студ. вузов / – М.: Издательский центр "Академия", 2004.
13. Капралов Е.Г., Кошкарев А.В. , Тикунов В.С. и др.; под ред. Тикунова В.С., Основы геоинформатики: В 2-х кн. Кн. 2: учеб. пособие для студ. вузов / – М.: Издательский центр "Академия", 2004
14. Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В. Информационная безопасность открытых систем. В 2-х тт. Том 1. Угрозы, уязвимости, атаки и подходы к защите. М.: Горячая Линия — Телеком, 2006. Том 2. Средства защиты в сетях. М.: Горячая Линия — Телеком, 2008.
15. Скотт Б., Разработка правил информационной безопасности. М.: Вильямс, 2002.
16. Игнатьев В.А., Информационная безопасность современного коммерчекого предприятия, Старый Оскол: ТНТ, 2005
17. Цыганок Д.А., Геоинформационные системы, Красноярск, 2004
18. Самардак А.С., Геоинфомационные системы, Владивосток, 2005

19. Цветков В.Я. Основы работы с MapInfo, Методические указания, Москва, 1998