На правах рукописи

БУЛГАКОВ СЕРГЕЙ ВЛАДИМИРОВИЧ

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДОВ И СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ ГИС

25.00.35 – Геоинформатика

Автореферат
диссертации на соискание учёной степени
кандидата технических наук

Москва – 2011

Работа выполнена на кафедре прикладной информатики Московского государственного университета геодезии и картографии (МИИГАиК).

Научный руководитель: доктор технических наук, Розенберг Игорь Наумович.

Официальные оппоненты:

доктор технических наук, профессор Журкин Игорь Георгиевич.

кандидат технических наук, доцент Силаев Антон Валерьевич.

Ведущая организация: Центральный научно исследовательский институт геодезии и картографии (ЦНИИГАиК).

Защита состоится 17 февраля 2011 г. в 12 часов на заседании диссертационного совета Д.212.143.03 при Московском государственном университете геодезии и картографии (МИИГАиК) по адресу: Москва 105064, Гороховский переулок 4, МИИГАиК, зал заседаний Ученого Совета.

С диссертацией можно ознакомиться в библиотеке Московского государственного университета геодезии и картографии (МИИГАиК).

Автореферат разослан « » 2011 г.

Учёный секретарь
диссертационного совета Климков Ю.М.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. Информационная среда и информационные ресурсы являются важным фактором жизнедеятельности современного общества. Эта совокупность включает коллекции информации, информационные потоки, информационные объекты, информационные инфраструктуры, а также системы регулирования возникающих при этом общественных отношений. Все более повышается роль субъектов, осуществляющих сбор, формирование, распространение и использование информации.

Об особом значении геоинформации в сфере безопасности говорит тот факт, что в США создано национальное агентство геопространственной разведки (National Geospatial Intelligence Agency - NGA). NGA обеспечивает своевременную, точную и геопространственную разведку в поддержку агентства национальной безопасности. Ее продукция и услуги используются для различных военных, гражданских и международных потребностей разведки. Поэтому разработка методов и технологий повышения информационной безопасности в геоинформатике, в том числе и в части защищенности инфраструктуры геоинформационных систем является актуальной задачей.

Информационные угрозы для информационных и геоинформационных систем имеют устойчивую тенденцию к росту и модифицируемости. К настоящему времени в области обнаружения вторжений в информационные и геоинформационные системы преобладает подход обнаружения злоупотреблений, который основан на построении модели атаки непосредственно на систему ГИС. Однако, данный подход имеет очевидный недостаток, связанный, прежде всего, с недостаточным учетом влияния инфраструктуры и компьютерной среды. С целью устранения этого недостатка и решения проблемы организации защиты инфраструктуры ГИС был предложен подход рассмотрения сложных систем ГИС-инфраструктура, инфраструктура – компьютерная среда при деструктивных воздействиях.

Состояние изученности проблемы. Общетеоретические аспекты исследования информационной безопасности представлены в публикациях Е. Б. Белова, Е. А. Ерофеева, В. Н. Лопатина, А. А. Стрельцова, В. А. Тихонова, В. В. Райх,

Ю. С. Уфимцева. Крупный вклад в развитие теории и практики информационной безопасности внесли И.И. Быстров, В.А. Герасименко, О.Ю. Гаценко, А.А. Грушо, В.С. Заборовский, П.Д. Зегжда, Д.П. Зегжда, В.А. Конявский, А.А. Малюк, А.А. Молдовян, Л.Г. Осовецкий, М.П. Сычев, С.П. Присяжнюк, С.П. Расторгуев, А.Г. Ростовцев, В.А. Садовничий, А.А. Стрельцов, А.А. Тарасов, Л.М. Ухлинов, В.П. Шерстюк, А.Ю. Щербаков и другие ученые.

В сфере геоинформатики работы в области информационной безопасности проводили Журкин И.Г., Иванников А.Д., Кулагин В.П., Майоров А.А., Макаревич О.Б., Тихонов А.Н., Цветков В.Я. и другие ученые.

Вопросам устойчивого функционирования геоинформационных систем посвящены работы Берлянта А.М., Бугаевского Ю.Л., Демиденко А.Г., Журкина И.Г., Майорова А.А., Малинникова В.А., Матвеева С.И., Нехина С.С., Карпика А.П, Кужелева П.Д., Кулагина В.П., Розенберга И.Н., Савиных В.П., Симонова А.В., Соловьева И.В., Цветкова В.Я. и других ученых.

Возрастающая роль информационной безопасности в сфере геоинформатики обусловливает необходимость расширения научных исследований не только в рамках информационной безопасности ГИС, но в области ее инфраструктуры.

За рубежом интенсивно изучают угрозы системам с электронными информационными инфраструктурами. В нашей стране этому вопросу уделяют значительно меньше внимания, что повышает актуальность диссертационных исследований. Изложенные обстоятельства определяют обоснованность темы диссертационного исследования.

Цель и задачи исследования. Целью диссертации является исследование организационно-технологических особенностей обеспечения информационной безопасности ГИС и ее информационной инфраструктуры, позволяющий повысить защищенность информационной инфраструктуры ГИС от внешних и внутренних угроз. Для достижения этой цели решены следующие задачи:

- изучены и систематизированы современные информационные угрозы применительно к ГИС, ее информационной инфраструктуре и компьютерной среде, в которой они находятся;

- построена модель информационной инфраструктуры ГИС (ИИГИС) с позиций информационной защищенности;
- исследована взаимосвязь систем ГИС, ИИГИС и компьютерной среды, в которой они находятся, в аспекте информационной безопасности ГИС и ИИГИС;
- проведен системный анализ безопасности ИИГИС;
- проведено исследование сетевых угроз для ИС и ИИГИС, в частности, новые угрозы, создаваемые беспроводными технологиями и мобильной средой;
- разработана математическая модель определения оптимальной частоты резервного копирования;
- разработана проектная модель защиты в дополнение к известным моделям информационной безопасности;
- исследован и предложен эвристический анализ как инструмент информационной безопасности, разработан алгоритм такого анализа;
- построена модель дополнительных угроз от спама применительно к передаваемой или принимаемой геоинформации.

Объект и предмет исследования. Объектом исследования является геоинформационная система и ее инфраструктура. Предметом исследования являются геоинформационные технологии, методы и модели, повышающие защищенность ГИС и ее инфраструктуры.

Методы исследования. В процессе исследований использовались системный анализ, теория геоинформатики, теория надежности, теория построения алгоритмов, абстрактно-логический, расчетно-конструктивный методы исследования. В работе использовались методы теории принятия решений, импакт-анализа и исследования операций. При разработке методики и моделей применялись методы теории множеств, а также теория математической статистики. Использовалось моделирование на персональных ЭВМ.

Научная новизна исследования состоит в обосновании и разработке ряда методологических и методических положений по определению приоритетных

направлений организации информационной безопасности ГИС и информационной инфраструктуры ГИС, и включает в себя:

- модель информационной инфраструктуры ГИС;
- концептуальная модель защищенности ИИГИС;
- методы минимизации деструктивных воздействий;
- модель проектной защиты;
- математическая модель определения оптимальной частоты резервного копирования;
- алгоритм эвристического анализа информационной безопасности.

Практическая значимость результатов. Реализация результатов исследования на практике способна обеспечить:

проведение более обоснованной и целенаправленной политики информационной безопасности в сфере геоинформатики и в геодезическом производстве, связанном с использованием информационных систем и технологий;

более экономное использование технологических и интеллектуальных ресурсов при организации защиты информации и информационных систем и их инфраструктур;

значение исследований представляет интерес не только в сфере геоинформатике, но и при защите других информационных систем.

Результаты исследований внедрены в качестве учебного материала при изучении курса «информационная безопасность» студентами МИИГАиК.

Предлагаемые в работе методы, алгоритмы и рекомендации имеют достаточно универсальный характер и поэтому могут быть применены для формирования стратегии информационной безопасности широкого спектра предприятий, имеющих в своем составе ИС, ГИС и другие системы.

Апробация работы. Основные положения диссертации нашли отражение в 16 научных публикациях автора, включая 5 журналов, рекомендованных ВАК, и трех монографиях. Они докладывались и получили положительную оценку на научно-технических конференциях студентов, аспирантов и молодых ученых МИИГАиК, на международных конференциях «Современные проблемы науки и

образования» РОССИЯ (Москва) 2010, «Развитие научного потенциала высшей школы» ОАЭ (ДУБАЙ) 2010, «Современные наукоемкие технологии» Хургада (Египет) 2010.

Структура и объём диссертации. Диссертационная работа состоит из введения, четырех глав, заключения и списка литературы. Содержание изложено на 147 печатной странице, иллюстрировано 27 рисунками, 9 таблицами. Список литературы включает 113 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во введении отмечается, что в задачи геоинформатики входит изучение общих свойств геоинформации, закономерностей и методов ее получения, фиксации, накопления, обработки и использования, а также развитие теории, методологии и технологий создания геоинформационных систем с целью сбора, систематизации, хранения, анализа, преобразования, отображения и распространения пространственно-координированных данных. В то же время работы в области информационной безопасности в геоинформатике касаются в основном защиты информации и самой ГИС, но практически не затрагивают организацию информационной безопасности инфраструктуры ГИС. Обоснована актуальность выбранной темы, сформулированы основная цель и задачи исследований.

Первая глава посвящена, анализу объекта защиты (информационной инфраструктуры), среды, в которой находится объект защиты, и анализу угроз. Кроме того, в главе проводится моделирование факторов и характеристик, влияющих и определяющих информационную инфраструктуру. С этой целью проведен анализ информационных процессов, информационной среды и информационного взаимодействия. Исследован мобильный Интернет как часть информационной инфраструктуры современных информационных систем. Изучена современная статистика информационных угроз. Проанализированы вопросы нормализации и моделирования как основы исследования и организации информационных процессов, включая информационные процессы защиты информационных ресурсов. Рассмотрена информационная среда как совокупность информационных объектов, отношений между ними, информационных систем,

информационных ресурсов и информационных процессов, а также условий реализации процессов информационного взаимодействия.

В таблице 1 приведены десять уязвимостей программного обеспечения (ПО), обнаруженных на компьютерах пользователей. %ПОУ - Процент пользователей с обнаруженной уязвимостью.

Таблица 1. Статистика уязвимостей

	Название уязвимости ПО	Возможности, которые дает использование уязвимости злоумышленникам	%ПОУ
1	Microsoft Excel	получение доступа к системе и выполнение произвольного кода с привилегиями локального пользователя	49.70%
2	Microsoft Office Word	получение доступа к системе и выполнение произвольного кода с привилегиями локального пользователя	49.67%
3	Adobe Flash Player идентификатор SA35948	получение доступа к системе и выполнение произвольного кода с привилегиями локального пользователя раскрытие конфиденциальных данных обход системы безопасности	40.87%
4	Microsoft PowerPoint Outline	получение доступа к системе и выполнение произвольного кода с привилегиями локального пользователя	40.80%
5	Microsoft XML Core Services	получение доступа к системе и выполнение произвольного кода с привилегиями локального пользователя DoS-атака на уязвимую систему Cross-site scripting	35.15%
6	Microsoft Office OneNote	получение доступа к системе и выполнение произвольного кода с привилегиями локального пользователя	32.31%
7	Microsoft Outlook "mailto:"	получение доступа к системе и выполнение произвольного кода с привилегиями локального пользователя	31.79%
8	Adobe Flash Player идентификатор SA34012	получение доступа к системе и выполнение произвольного кода с привилегиями локального пользователя получение доступа к конфиденциальным	27.72%

		данным повышение привилегий обход системы безопасности	
9	Sun Java JDK / JRE	получение доступа к системе и выполнение произвольного кода с привилегиями локального пользователя DoS-атака на уязвимую систему обход системы безопасности	27.52%
10	Adobe Reader	получение доступа к системе и выполнение произвольного кода с привилегиями локального пользователя	24.52%

В таблице отмечены две уязвимости в Adobe Flash Player, которые имеют разные идентификаторы. Все эти программы устанавливают, как правило, на одном компьютере с ГИС и эти программы составляют инфраструктуру ГИС, поскольку в прямой или косвенной форме взаимодействуют с ней. Отсюда следует важный вывод: безопасность ГИС существенным образом зависит от ПО, входящего в инфраструктуру ГИС или функционирующего на одном компьютере с ГИС.

В настоящее время большой интерес представляет динамика уязвимостей по типам воздействия. На рисунке 1 приведены уязвимости по типам воздействия на систему.

Для анализа использованы статистические данные, публикуемые в печати и Интернет, например, фирмой Semantik, а также антивирусной сети Kaspersky Security Network (KSN). Как следует из рис.1 одной из основных угроз является получение доступа к системе. Эта угроза чаще реализуется эвристическими методами двухходовыми или многоходовыми атаками.

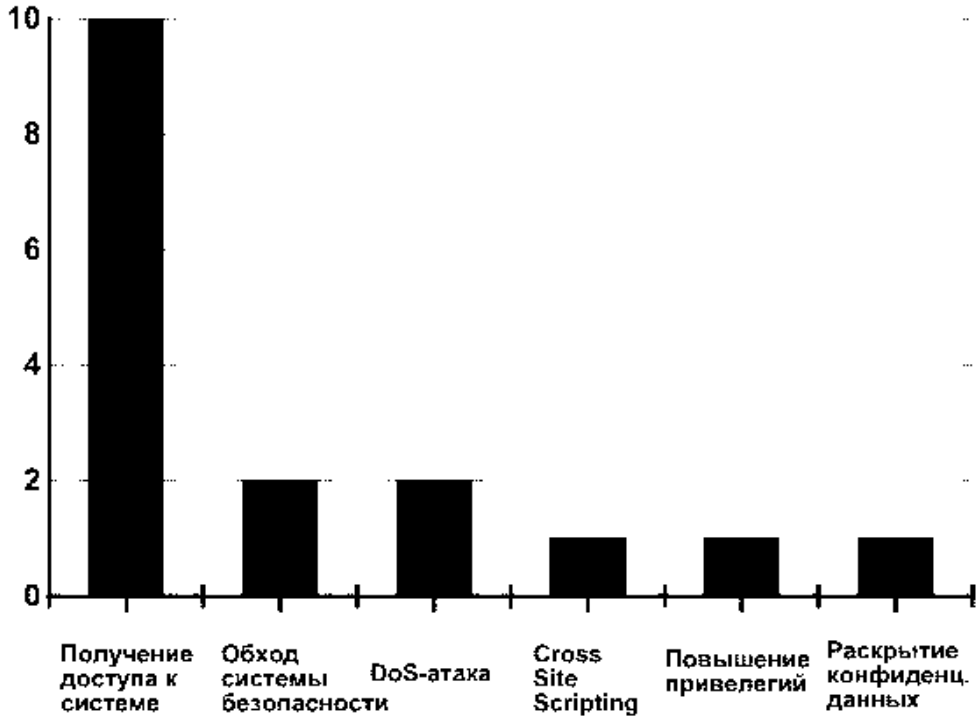

Рис.1. Статистика уязвимостей по типу воздействия на систему.

Как особый элемент инфраструктуры рассмотрена мобильная среда, которая все шире используется не только при коммуникациях, но и при создании мобильных информационных систем, включая мобильные ГИС. На основе проведенного анализа выявлено, что в современных условиях взаимодействие между информационными системами осуществляется в информационной среде при значительном участии инфраструктуры информационной системы. При переходе к локальным информационным системам, такой средой является компьютерная среда. Существуют информационные отношения между информационной системой, ее инфраструктурой и компьютерной средой, в которой они находятся. Наличие информационных отношений предопределяет взаимную связь и необходимость учета этих отношений при организации информационной безопасности.

В главе проведен многоаспектный анализ информационных угроз. Анализ показал, что в современных условиях подавляющее большинство атак направлено не на информационный объект (ИС, ПО), а на их инфраструктуру или обо-

лочку, или компьютерную среду. Поэтому методы защиты, ориентированные только на защиту ИС, потеряли эффективность. Основной информационной угрозой в настоящее время являются не прямые атаки на информационные системы, а эвристические методы проникновения в систему или методы обхода систем защиты. Для этой цели широко используют существующие социальные сети или имитации под известные сети. Современная информационная инфраструктура является важным дополнением к информационным системам и в ряде случаем без нее неэффективна работа ИС. Выявлено, что не существует нормативов на защищенность инфраструктур и сред, а существуют нормативы только на оценку защищенности ИС. Защите подлежат не отдельные информационные системы или программы, а их инфраструктура, тесно связанная с компьютерной средой. В рамках исследования первой главы были сформулированы общие задачи диссертационной работы.

Во второй главе проведены исследования и моделирование информационной инфраструктуры геоинформационной системы (ИИГИС) как объекта информационной защиты. Рассмотрены общие особенности инфраструктур информационных систем. Инфраструктура информационной системы (Information Infrastructure Systems - IIS) включает совокупность интерфейсов, систем обмена, информационных центров, систем связи и обеспечивает доступ потребителей к информационным ресурсам ИС. Дан системный подход к проектированию инфраструктуры информационной системы.

Рассмотрены особенности ГИС как информационной системы, что дало основание перейти к исследованию ИИГИС. Рассмотрено сходство и различие между интерфейсом ГИС и инфраструктурой ГИС. На основе функционального подхода построена модель компьютерной среды и информационной инфраструктуры ГИС (Рис.2). Компьютерная среда (КС) является основой функционирования ГИС. ГИС бывает связана с электронными таблицами (ЭТ), фотограмметрической станцией (ФС), системой обработки изображений (СОИ), САПР и другими информационными системами. Большинство информационных взаимодействий осуществляется через инфраструктуру ГИС.

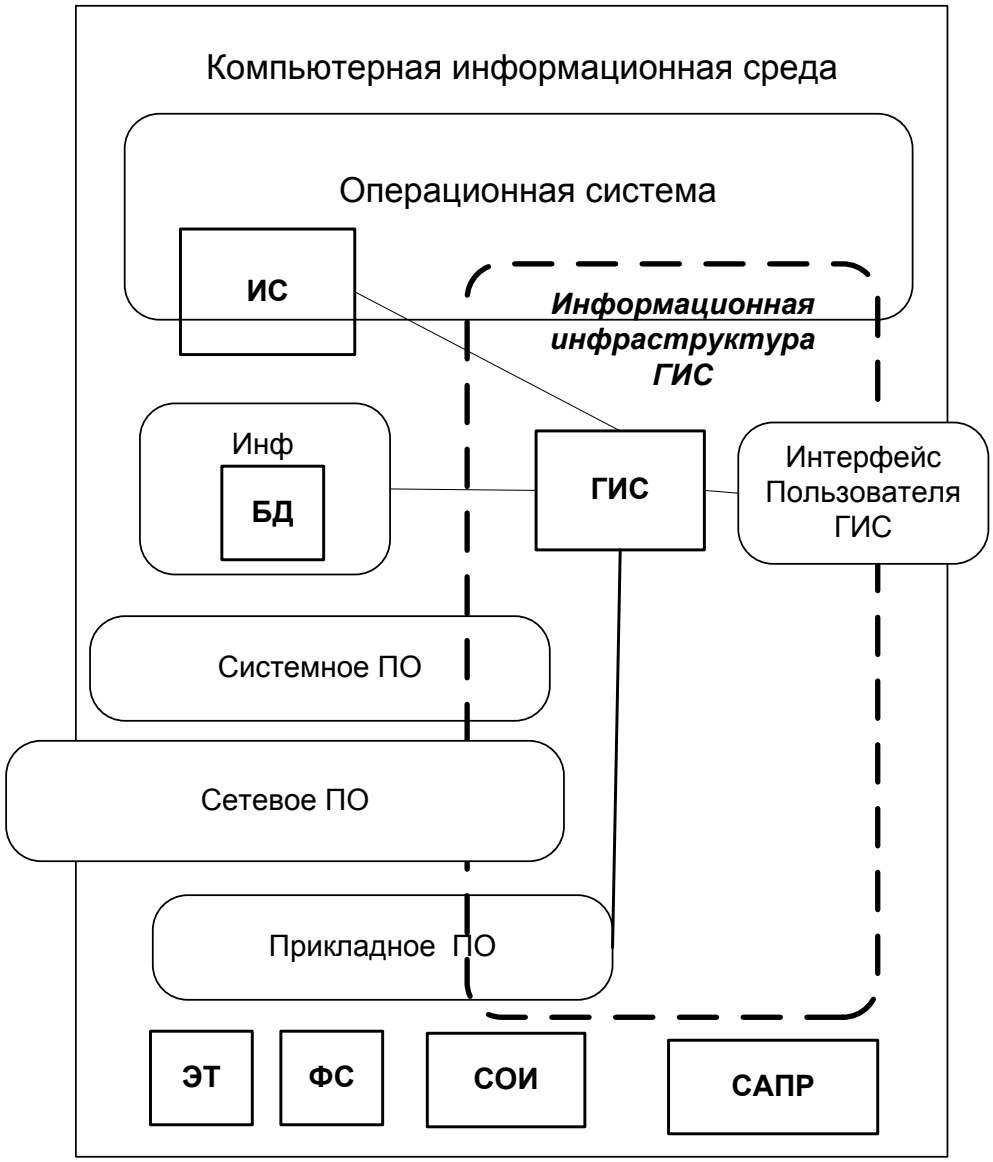

Рис.2. Компьютерная информационная среда и инфраструктура ГИС

Наибольшие уязвимости ИИГИС и компьютерной среды связаны с информационными сетевыми взаимодействиями и с работой пользователя.

В таблице 2 показаны основные угрозы, характерные для геоинформационной системы и ее инфраструктуры. Единица означает наличие угрозы, ноль отсутствие угрозы.

Таблица 2. Основные угрозы для ГИС и ее информационной инфраструктуры

	Вид угрозы	Объект воздействия	
		ГИС	ИИГИС
1	Неумышленные ошибочные действия собственных сотрудников	1	1
2	Сбои оборудования	1	1
3	Попытки внешнего несанкционированного доступа	0	1
4	Умышленные ошибочные действия собственных сотрудников	1	1
5	Атаки через сеть	0	1
6	Ошибочные исходные данные	1	0
7	Сбои программного обеспечения	1	1
8	Окончание жизненного цикла ТС и технологий	1	1
9	Нарушение согласования ГИС с внешней системой	0	1
10	Нарушение изменения режима секретности или доступа	0	1

Из таблицы 2 следует, что ИИГИС практически принимает все внешние угрозы на себя. Отсюда еще раз вытекает важность организации информационной безопасности ИИГИС, как первоочередной задачи информационной безопасности ГИС. Особая связь между ГИС и ее инфраструктурой приводит к тому, что интерфейс инфраструктуры должен обладать особым признаком, которое называют дружественный интерфейс. Даны рекомендации по организации профиля ИИГИС.

Выполнен системный анализ информационной безопасности инфраструктуры ГИС. Системный подход приводит к образованию трех видов структурного деления инфраструктуры ИС *(IIS)*: подсистем $PIIS_i$ i=1, n , компонент $KIIS_i$ i=1, p, и элементов $eIIS_l$ l=1, m

$$IIS = (PIIS_1 k_p PIIS_i ... PIIS_n);$$

$$IIS = (KIIS_1 k_k KIIS_i ... KIIS_p);$$

$$IIS = (eIIS_1 k_e eIIS_i ... eIIS_m).$$

Здесь k - критерии разбиения на k_p - подсистемы, k_k - компоненты, k_e - элементы. Разбиение дает возможность построить матрицы сопряжения по подсистемам, компонентам и элементам. Три специальные матрицы образуют базис системы в целом Msys(IIS). В матрицах определено соответствие между частями структурного деления системы сложной системы IIS и функциями. Элементная матрица будет диагональной. Вектор угроз VT воздействует на матрицу системы

$$Msys(IIS) \times VT = DR.$$

DR – результат деструктивного воздействия. Задачей информационной безопасности является минимизация DR.

Для анализа защищенности вводится понятие функции безопасности *SFO* и вероятность $P_i(t)$ безотказного выполнения этой функции. Для оценки этих величин используется формализм теории надежности:

$$P_i(t)=e^{(-t/Ti)},$$

где t – время безотказного выполнения *SFO*, T_i - оценка среднего времени безотказного выполнения *SFO*.

Выявлены основные угрозы Интернет, которые создают опасность для ГИС и ее инфраструктуры. Особенность этих угроз в том, что атакам подвергается не столько сама ГИС, сколько компьютерная среда того компьютера, на котором размещена ГИС. В работе обосновано положение о том, что для обеспечения защищенности ИИГИС и ГИС компьютерная среда должна иметь как минимум четыре уровня защиты. Это защита от сетевых атак, от спама, антивирусная защита, защита от компьютерных шпионов.

Третья глава посвящена исследованию и моделированию сетевых угроз IIS и технологическим решениям отражения этих угроз. Построена модель жизненного цикла сетевой атаки, приведенная на рис.3.

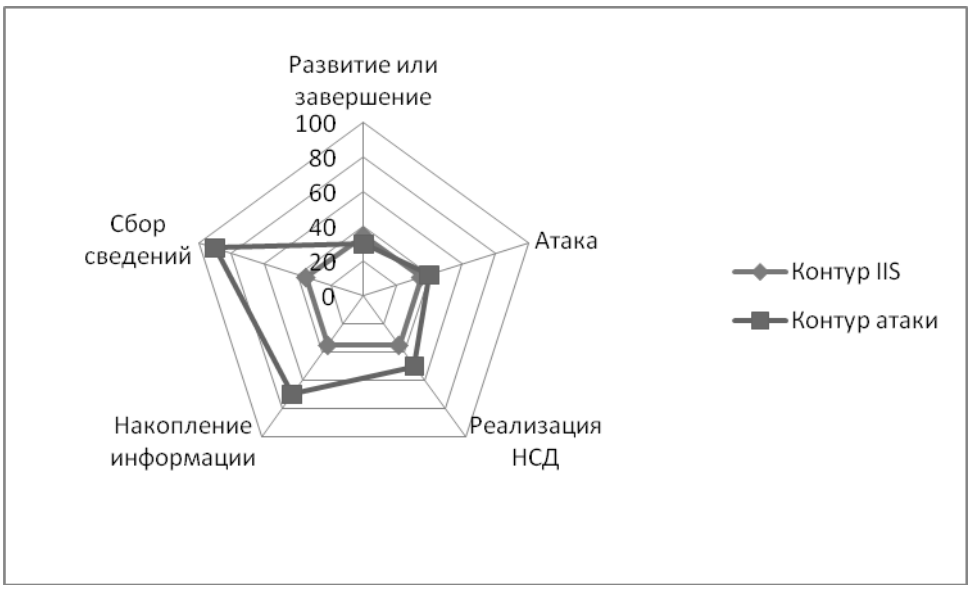

Рис.3. Жизненный цикл сетевой атаки

В условных баллах показана степень взаимодействия атаки и системы. Она включает следующие этапы: сбор сведений, накопление и анализ накопленной информации, осуществление несанкционированного доступа к ресурсам объекта атаки, проведение атаки, развитие или завершение атаки.

Сетевые угрозы представляют наибольшую внешнюю опасность для ИИГИС и КС. Проанализированы наиболее опасные для КС и ИИГИС сетевые атаки: сканирование; несанкционированный удаленный доступ; получение привилегированных прав; DoS – атаки. Анализ жизненного цикла атак позволил сформулировать основные правила для обеспечения безопасности. Детально рассмотрена одна из наиболее опасных атак DoS - атака Smurf. На основе анализа предложены контрмеры для ее отражения. При этом даны практические рекомендации для реализации контрмер в разных системах, таких как: *Solaris, Linux, FreeBSD, AIX, UNIX*.

В связи бурным ростом беспроводной Интернет и интеграцией мобильных технологий в третьей главе проанализированы растущие угрозы мобильной информационной среды для ИИГИС. Проанализированы следующие основные виды атак: атака деаутентификации, атака воспроизведением, фальсификация точки доступа, атаки на физический уровень и другие. На основе проведенного исследования даны рекомендации по организации архитектуры безопасной сети

WiMAX. В частности, даны технологии аутентификации устройств и пользователей, а также технология защиты радиоканала. Описана архитектура аутентификации в беспроводной Интернет . Описана процедура безопасного хэндовера. В целом предложенные технологии имеют широкое значение и могут использоваться для защиты ИИГИС и других информационных инфраструктур и систем.

В четвертой главе приводится описание мероприятий по защите, предложения по организации безопасности и модели защиты применительно к ИИГИС, разработанные автором. Для обеспечения полной безопасности ГИС необходима совместная защита ИИГИС и компьютерной среды по следующим категориям: физическая безопасность, информационная безопасность, компьютерная безопасность, экономическая безопасность, человеческая безопасность. На основе проведенных исследований автор применительно к ГИС и ее инфраструктуре предлагает *концептуальную модель информационной безопасности*, включающую следующие показатели безопасности: риск, угрозы, контрмеры, глубина или уровни защищенности, гарантия защищенности – показатель того, что система обеспечения безопасности будет вести себя как ожидалось. Эта концептуальная модель является основой политики безопасности ИИГИС и ГИС.

Автор обосновывает свою модель резервного копирования и показывает, что она является обязательным инструментом защиты геоинформации, например, кадастровой информации. Проанализированы разные стратегии резервного копирования. Показано, что резервное копирование принимает участие в отражении не мене семи опасных информационных угроз. Важным фактором является частота резервного копирования. На рисунке 4 приведен график затрат: *TE* – суммарные затраты на восстановление и на копирование; C_c — стоимость копирования информации за единицу времени; C_L – стоимость потерянной информации; K_V – коэффициент относительной стоимости создаваемой информации. На основе решения задачи оптимизации автор диссертации рассчитал оптимальное значение *Fo* частоты резервного копирования:

$$Fo = [(C_L \ K_V)/ C_C]^{1/2}.$$

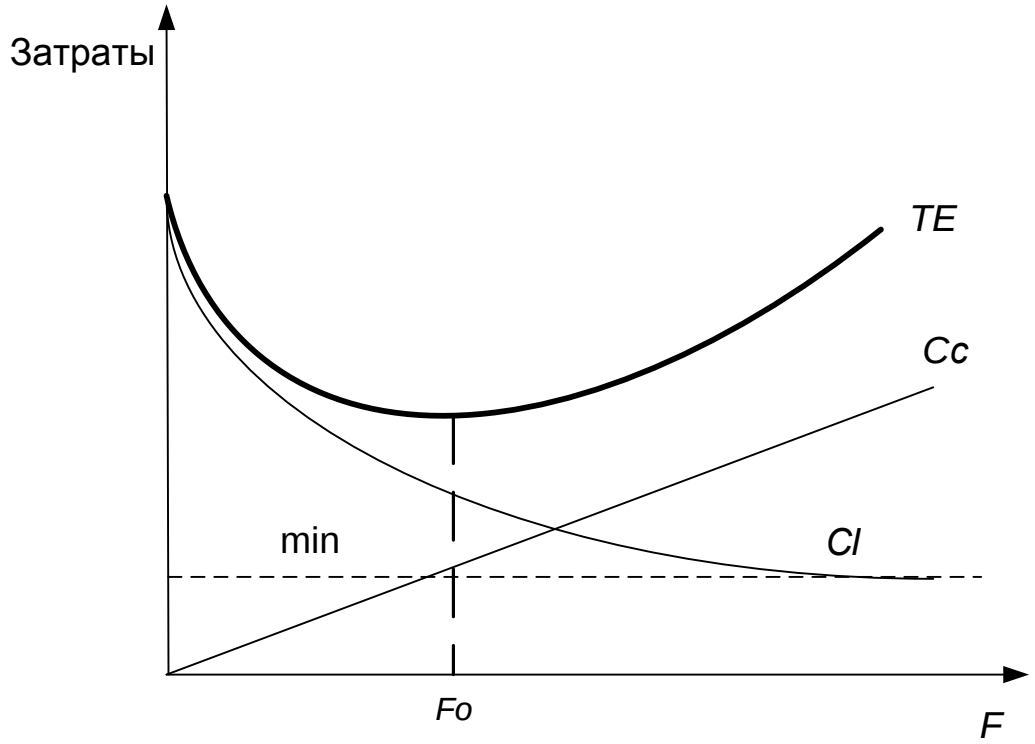

Рис.4 График затрат на резервное копирование и восстановление информации.

Для отражения внешних угроз и защиты информации применяют разные модели защит, которые отражают разные концепции, заложенные в этих моделях.

В дополнение к четырем основным существующим моделям информационной безопасности Биба, Гогена-Мезингера, Кларка-Вильсона и Сазерлендской модели автор предлагает свою модель, которую называет проектной (рис.5). Общий недостаток всех рассмотренных моделей – апостериорный подход. Они защищают информационные системы после их создания. В своей модели автор устраняет этот недостаток.

При построении этой модели защиты учитывается предположение о том, что понятие информационной безопасности *IIS* шире, чем понятие безопасности ИС. При построении модели защиты *IIS* учитывается предположение о том, что понятие информационной безопасности компьютерной среды шире, чем понятие безопасности *IIS*. Это приводит к необходимости включения в параметры защи-

ты *IIS* дополнительных параметров и показателей, отражающих защищенность компьютерной среды. К таковым относятся не только защищенность, но и качество проектирования, среды, надежность функционирования но и другие факторы.

Рис.5. Проектная модель защиты

Многие средства информационной безопасности в качестве цифрового метода защиты применяют технологию эвристического анализа. Эвристический ана-

лиз нередко используется совместно с сигнатурным сканированием для поиска сложных шифрующихся и полиморфных вирусов. Одним из побочных методов применения данного метода является цифровая защита авторских прав. Наряду со стеганографическими методами эвристический метод позволяет выявлять цифровые знаки авторского права. Это особенно важно для геоинформационных продуктов, которые имеют визуальные формы представления. В работе рассмотрено применение эвристического подхода для оценки защищенности ИИГИС.

Для оценки деструктивного воздействия автор рекомендует комплексный подход, включающий алгоритмическую оценку (АО), дополненную эвристической оценкой (ЭО). Задача ЭО – получение количественной оценки уровня информационного риска, возникающего в результате неполного выполнения функций безопасности. Алгоритм строится на основании следующих предположений:

имеется набор входных параметров Pi(t) $(i = 1, 2, ..., M)$, оценки которых получены в АО;

необходимо получить количественную оценку параметра r (текущий уровень информационного риска);

имеется набор лингвистических термов, характеризующих значения входных (α_k^i, $k \in [1, N_i]$, где N_i - количество термов параметра y_i) и выходного (δ_j, $j \in [1, N]$, где N – количество термов параметра r) параметров.

Для решения задачи ЭО применяются методы теории предпочтений и нечеткой логики.

В работе рассмотрена информационная угроза спам - одна из основных угроз работы в сети Интернет. Эффективных способов борьбы мало и количество спам-сообщений увеличивается с каждым днем. Автор показывает, что применительно к геоинформации опасность спама возрастает, поскольку он приводит к нарушению полноты и, что особенно важно для геоданных, нарушению целостности геоданных. Рекомендованы организационные меры отражения

данной угрозы. Используя оценку К.Э. Шеннона для оценки пропускной способности канала передачи автор показывает, что наличие спама эквивалентно снижению пропускной способности канала на порядки. В работе даются эвристические меры по отражению данной угрозы. В качестве эффективной меры борьбы со спамом автор рекомендует нейросетевой фильтр и базу знаний.

В главе дается анализ угрозы spyware-модулей и рекомендации по отражению этой угрозы.

В заключении даны результаты проведённого анализа, теоретических и экспериментальных исследований. Получены следующие выводы и основные результаты: исследование информационных процессов, протекающих в компьютерных средах, мобильных системах, геоинформационных системах и сетях, а также анализ научных публикаций по теме исследования показало, что многие опубликованные и практикуемые методы не учитывают особенности инфраструктуры ГИС, не рассматривают ее как объект первоочередной защиты, не предлагают комплексных решений по организации защиты в системе ГИС+инфраструктура.

Основные результаты диссертационной работы заключаются в следующем:

1. Систематизированы современные информационные угрозы применительно к ГИС, ее информационной инфраструктуре и компьютерной среде, в которой они находятся, и определены основные тенденции развития угроз;

2. Построена модель информационной инфраструктуры ГИС (ИИГИС) с позиций информационной защищенности. Сформулированы основные характеристики ИИГИС;

3. Построена модель взаимосвязи ГИС, ИИГИС и компьютерной среды, в которой они находятся, в аспекте информационной безопасности. Обоснована необходимость организации единой защиты для всех трех систем;

4. Исследованы модели сетевых угроз для ИС и ИИГИС, в частности, новые угрозы, создаваемые беспроводными технологиями и мобильной средой;

5. Разработан ряд организационных и технических мероприятий защите ГИС и ИИГИС, которые включают:

5.1. Концептуальную модель информационной безопасности ИИГИС, которая служит основой политики безопасности;

5.2. Проектную модель информационной защиты ИИГИС, которая включает управление конфигурациями данных и ПО, разделение дискового пространства и регламентацию работ;

5.3. Математическую модель определения оптимальной частоты резервного копирования в зависимости от ценности создаваемой информации и затрат при копировании и восстановлении;

5.4. Эвристический метод анализа деструктивных воздействий на ИИГИС, который является инструментом резервирования и тем самым повышает надежность и защищенность системы безопасности;

5.5. Рекомендации по повышению защищенности ГИС и ИИГИС при организации Веб-ГИС технологий;

5.6. Рекомендации, повышающие информационную безопасность ГИС и работы с ГИС, такие как борьба со спамом и компьютерными шпионами.

Сформулированная цель диссертационной работы достигалась решением основной научной задачи, которая состояла в разработке комплексной методики обнаружения уязвимостей и повышения защищенности ГИС и инфраструктуры ГИС.

Список опубликованных работ по теме диссертации.

1. Цветков В.Я., Булгаков С.В. Что такое Спам и как с ним бороться // ЭЖ - Интернет образование -№19 - 2004. .http://vio.fio.ru/vio_19.
2. Цветков В.Я., Булгаков С.В. Информационная безопасность в геоинформатике: компьютерные шпионы // Геодезия и аэрофотосъемка, - 2004. - №4 - с. 99- 108.
3. Цветков В.Я., Булгаков С.В. Информационная угроза - спам // Геодезия и аэрофотосъемка. - 2004. - №5. - с. 116-128.
4. Цветков В.Я., Булгаков С.В. Информационная угроза: компьютерные шпионы // Информационные технологии. - 2004. - , №9. - с. 2-4.
5. Коростелев Ю.А., Булгаков С.В Информационные объекты // Методы управления и моделирования. — Вып.4.**:** Сборник научных трудов. – М.:

МАКС Пресс, 2004—с3-4.

6. Булгаков С.В. Мобильный Интернет как информационная инфраструктура // Методы управления и моделирования— Вып. 5**:** Сборник научных трудов. – М.: МАКС Пресс, 2005. — с.30-43.
7. Булгаков С.В. Информационная инфраструктура ГИС.// Исследование процессов и явлений методами геоинформатики - вып.10. Сборник научных трудов. – М.: МАКС Пресс, 2006 —с.29-32.
8. Цветков В. Я., Булгаков С.В. Информационная инфраструктура. М.: МИИГАиК, «Госинформобр». 2006. - 84 с.
9. Булгаков С.В., Ковальчук А.В., Цветков В.Я., Шайтура С.В. Защита информации в ГИС. - М.: МГТУ им. Баумана, 2007 - 183 с
10. Булгаков С.В., Ковальчук А.В., Цветков В.Я., Шайтура С.В. Интегрированные геоинформационные системы. - М.: МГТУ им. Баумана, 2007 - 113 с.
11. Цветков В. Я., Булгаков С.В. Дружественный интерфейс как характеристика информационной инфраструктуры // Современные наукоемкие технологии. - 2010. - №1. - с 44-45.
12. Цветков В. Я., Булгаков С.В. Анализ инфраструктуры информационной системы // Успехи современного естествознания. – 2010. - №3. С 44-45.
13. Цветков В. Я., Булгаков С.В. Эвристический анализ как инструмент информационной безопасности // Успехи современного естествознания. – 2010. - №3. С 45-46.
14. Булгаков С.В., Корнаков А.Н., Пушкарева К.А., Цветков В.Я. Информационные модели в управлении// Вестник Московского государственного областного педагогического университета. -2010. - № 1. - с.45-48.
15. Булгаков С.В., Корнаков С.А. Функциональная модель информационного управления // Вестник Московского государственного областного педагогического университета. -2010. - № 2. - с.179- 181.
16. Розенберг И.Н., Булгаков С.В. Проектная модель информационной безопасности ГИС // Вестник Московского государственного областного педагогического университета. -2010. - № 2. - с.110 – 113.

Подп. к печати Формат 60х90/16
Бумага офсетная Печ. л. 1,5 Уч. – изд. л. 1,5
Тираж экз. 80 Заказ № Цена договорная

МИИГАиК
105, Москва К-64, Гороховский пер., 4