Оглавление

ПРИНЯТЫЕ СОКРАЩЕНИЯ

АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
БД	–	база данных
ГИС	–	геоинформационная система
ИВК	–	информационно-вычислительный комплекс
ИВП	–	информационно-вычислительный процесс
КВИС	–	критически важная информационная система
ЛВС	–	локальная вычислительная сеть
МЭ	–	межсетевой экран
НДВ	–	недекларированные возможности
НСД	–	несанкционированный доступ
ОПО	–	общее программное обеспечение
ОС	–	операционная система
ПО	–	программное обеспечение
ППД	–	протокол передачи данных
ПУ	–	пункт управления
СВТ	–	средства вычислительной техники
СЗИ	–	средства защиты информации
СПО	–	специальное программное обеспечение
СПКА	–	средства противодействия компьютерным атакам
ССД	–	сервер сбора данных
ССД-А	–	сервер сбора данных абонента
ССИ-П	–	сервер сбора данных пункта
ССИ-Ц	–	сервер сбора данных центра
СУБД	–	система управления базами данных
СЭП	–	сервер электронной почты
ТЦУ	–	технологический цикл управления
ЦКО	–	цифровое коммуникационное оборудование
ЦУ	–	центр управления

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины	Определения
Критически важная информационная система (КВИС)	Информационно-телекоммуникационные средства, на которых осуществляются сбор, обработка и передача информации, выход параметров которых за допустимые пределы может привести к нарушению функционирования (функциональному поражению) КВИС
Компьютерная атака	Целенаправленное программно-аппаратное воздействие на информационно-телекоммуникационные средства, приводящее к нарушению или снижению эффективности выполнения технологических циклов управления в КВИС
Уязвимые места КВИС	Точки санкционированного и несанкционированного доступа через которые могут быть реализованы компьютерные атаки.
Сценарий компьютерной атаки	Комплекс действий, проводимых с целью нарушения устойчивости функционирования КВИС
Устойчивость функционирования КВИС	Способность КВИС обеспечивать установленные регламенты выполнения технологических циклов управления в условиях компьютерных атак
Технология противодействия компьютерным атакам на КВИС	Совокупность взаимосвязанных процедур прогнозирования сценариев и классификации компьютерных атак нарушителя, анализа уязвимых мест и технологических циклов управления КВИС, применения методов и моделей противодействия атакам и оценки устойчивости функционирования КВИС в условиях компьютерных атак

1 Особенности выполнения технологических циклов управления в критически важных информационных системах

Критически важные информационные системы (КВИС) сбора, обработки, передачи, хранения и отображения информации обеспечивают выполнение технологических циклов управления объектами (пунктами и центрами управления) различного целевого назначения.

Структура КВИС и средств защиты информации в условиях компьютерных атак приведена на рисунке 1.

Технологический цикл управления (ТЦУ), реализуемый КВИС, определяется объемом технологических операций по сбору, передаче, обработке информации и выдаче управляющих воздействий, которые необходимо выполнить на заданном интервале времени (например, суточном интервале). Интенсивность выполнения ТЦУ определяется, прежде всего, параметрами объекта управления.

Нарушение ТЦУ путем реализации компьютерной атаки приводит к снижению эффективности объекта управления (нештатному функционированию или полному интеллектуальному выводу из строя). Результатом компьютерной атаки могут быть события: искажения информации; выдачи ложной информации; несвоевременной обработки данных и выдачи информации абонентам в критические интервалы времени, сбора информации о состоянии систем и другие нарушения целостности и доступности информации в КВИС.

К числу основных задач типовых КВИС относятся [2, 25, 32, 46, 65, 67-69]:

- передача и прием исходных данных для проведения расчетов;
- сбор, хранение и доставка информации на пункте управления;
- доставка, сбор и выдача управляющей информации абонентам центров управления;
- обмен информацией между абонентами пунктов и центров управления;
- организация оперативного взаимодействия и управления между КВИС по каналам связи.

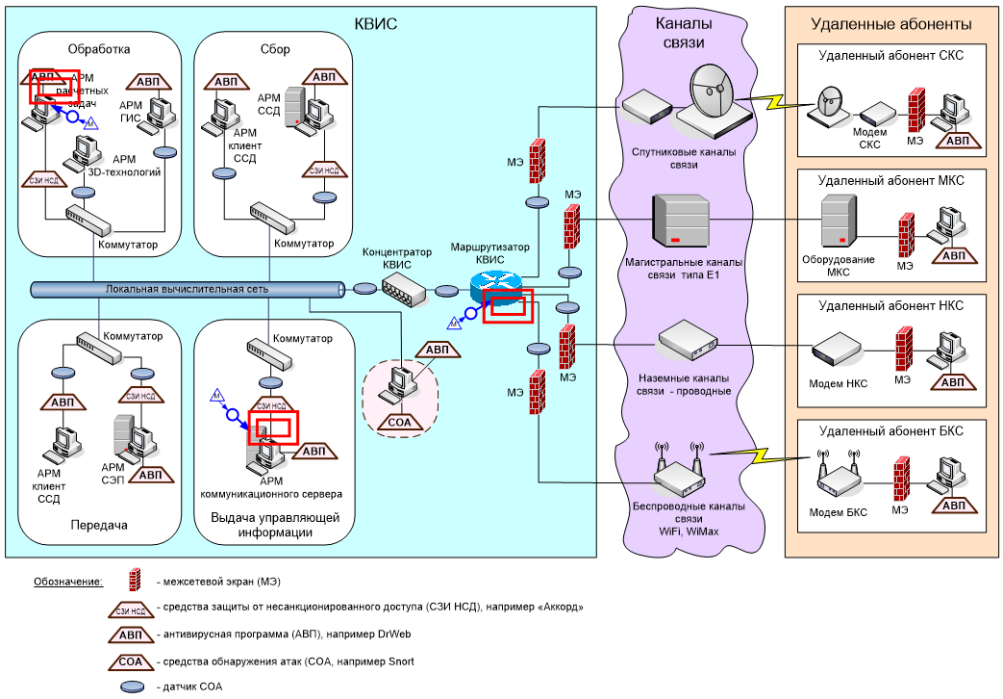


Рисунок 1 – Структура КВИС и средств защиты информации в условиях компьютерных атак

Топология, состав и функции КВИС формируется на основе унифицированных информационно-телекоммуникационных средств в соответствии с требованиями к объектам управления. Способы и протоколы информационного взаимодействия абонентов КВИС для каждого конкретного объекта управления реализуются в схеме организации связи с абонентами, объединяющими средства измерений, сбора, обработки и передачи информации. В каждом конкретном КВИС могут использоваться дополнительные коммуникационные средства, учитывающие специфику технического и программного обеспечения.

Современные КВИС функционируют на базе защищенного коммуникационного оборудования, межсетевых экранов и стеков протоколов передачи данных TCP/IP. Перспективные информационно-телекоммуникационные средства КВИС построены как единая система приема, передачи, сбора, обработки и доставки информации. Такой подход позволяет унифицировать аппаратные средства и программное обеспечение, а, следовательно, сократить расходы на их создание и эксплуатацию [2, 25, 32, 46, 47, 65, 67-69].

Однако при модернизации и развитии КВИС на основе применения новых информационных технологий возникает противоречие, заключающееся в том, что

сетевая архитектура КВИС и цифровое коммуникационное оборудование необходимые для повышения надежности информационно-вычислительного процесса и оперативности передачи данных, является весьма уязвимой при воздействии компьютерных атак.

Находящиеся в эксплуатации средства защиты от несанкционированного доступа ПЭВМ и локальных вычислительных сетей КВИС, антивирусные средства не имеют функции противодействия компьютерным атакам [5-10, 21, 22, 28-30, 33, 35, 40, 44, 48, 52, 56, 58-60, 64, 68, 69]. Поэтому, при внедрении в КВИС перспективных информационных технологий необходимо обеспечить требования по противодействию компьютерным атакам для обеспечения устойчивости функционирования при выполнении регламентов сбора, доставки и обработки информации.

Системный анализ особенностей выполнения технологических циклов управления в КВИС в условиях компьютерных атак осуществляется по технологическим схемам сбора данных, обмена формами информации и доставки информации, представленных на рисунках 2, 3.

Условия воздействия компьютерных атак формализуются в виде графов состояний и событий реализации компьютерных атак:

1. Ввод ложных исходных данных.
2. Нарушение информационного взаимодействия между абонентами КВИС.
3. Отказ в выдаче, доставке данных и обмене информацией.
4. Инициализация ложных событий реконфигурации КВИС (перезагрузки ПЭВМ абонента).
5. Ввод ложных расчетных данных.
6. Ввод ложных результатов обработки информации.
7. Перегрузка абонентов КВИС «спамом» технологических результатов обработки информации.

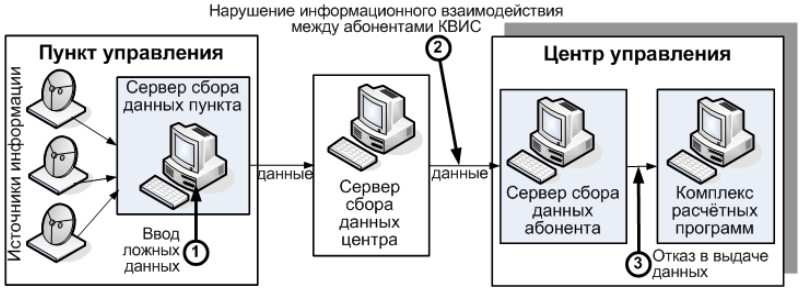


Рисунок 2 – Технологическая схема сбора данных в КВИС при воздействии компьютерных атак

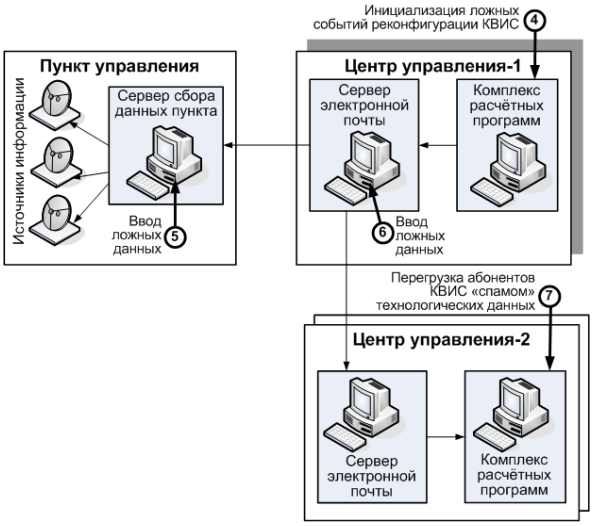
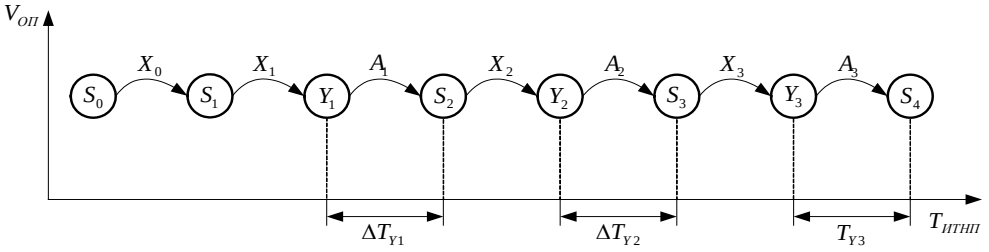


Рисунок 3 – Технологическая схема обмена информацией при воздействии компьютерных атак

Представление технологической схемы сбора, доставки данных и обмена информацией в виде графов соответствующих состояний и событий выполнения ТЦУ в КВИС и наиболее вероятных событий и состояний реализации компьютерных атак приведено на рисунках 4-6.



Периоды времени действия атак Y_1, Y_2, Y_3

Рисунок 4 – Представление технологической схемы сбора данных состояниями и событиями выполнения ТЦУ в КВИС и реализации компьютерных атак

На рисунке 4 приняты обозначения:

Состояния выполнения ТЦУ в КВИС:

S_0 – ожидание исходных данных;

S_1 – сбор данных от источников информации;

S_2 – передача данных из пункта управления в центр управления-1, прием и маршрутизация данных в центре управления-1;

S_3 – передача данных из центра управления-1, прием и архивация данных в сервере электронной почты центра управления-2;

S_4 – передача данных в комплекс расчетных программ.

Состояния реализации компьютерных атак:

Y_1 – ввод ложных данных;

Y_2 – нарушение информационного взаимодействия между абонентами КВИС;

Y_3 – отказ в выдаче данных.

События выполнения ТЦУ в КВИС:

X_0 – начало сеанса приема исходных данных;

X_1 – тракт информационного взаимодействия пункта управления с центром управления-1 установлен;

X_2 – тракт информационного взаимодействия центром управления-1 с центром управления-2 установлен;

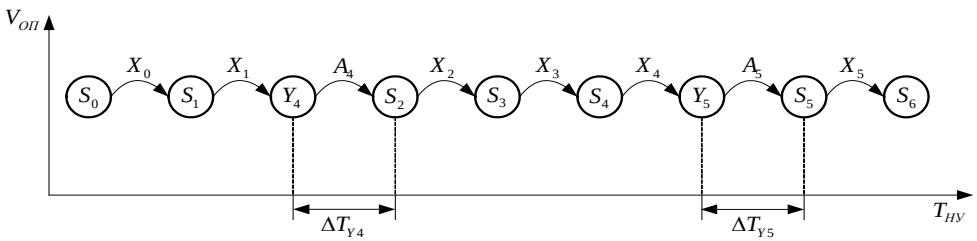
X_3 – запрос от комплекса расчетных программ к серверу сбора данных поступил.

События реализации компьютерных атак:

A_1 – ложные данные введены;

A_2 – задержка информационного взаимодействия между центрами управления реализована;

A_3 – запрос от комплекса расчетных программ к серверу сбора данных о выдаче информации отклонен.



Периоды времени действия атак Y_4, Y_5

Рисунок 5 – Представление технологической схемы передачи данных между пунктом и центрами управления состояниями и событиями выполнения ТЦУ в КВИС и реализации компьютерных атак

На рисунке 5 приняты обозначения:

Состояния выполнения ТЦУ в КВИС:

S_0 – ожидание данных от комплекса расчетных программ;

S_1 – прием и маршрутизация данных сервером электронной почты центром управления;

S_2 – передача данных на пункт управления;

S_3 – передача данных в информационно-вычислительный комплекс (ИВК) пункта управления;

S_4 – ожидание результатов расчета от ИВК пункта управления;

S_5 – прием и маршрутизация данных сервером электронной почты;

S_6 – передача данных на объект управления.

Состояния реализации компьютерных атак:

Y_4 – инициализация ложных событий реконфигурации КВИС;

Y_5 – ввод ложных данных.

События выполнения ТЦУ в КВИС:

X_0 – информационно-логическое соединение сервера электронной почты (СЭП) с комплексом расчетных программ центра управления установлено;

X_1 – тракт информационного взаимодействия СЭП с ИВК установлен;

X_2 – информационно-логическое соединение СЭП с ИВК пункта управления установлено;

X_3 – передача данных из СЭП в ИВК пункта управления завершена;

X_4 – информационно-логическое соединение СЭП с ИВК пункта управления установлено;

X_5 – информационно-логическое соединение СЭП с источником информации пункта управления установлено;

События реализации компьютерных атак:

A_4 – произошла нештатная перезагрузка ПЭВМ абонента;

A_5 – реализован ввод ложных данных.

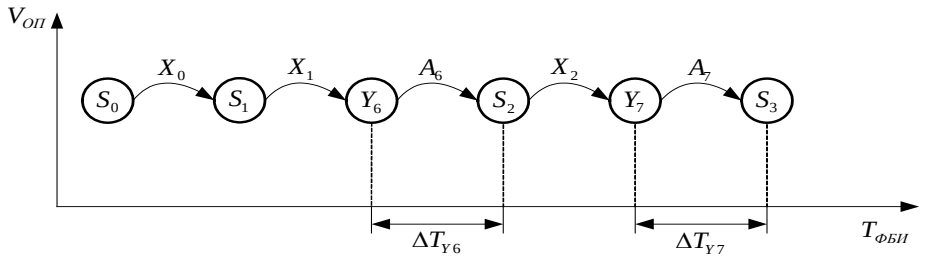


Рисунок 6 – Представление технологической схемы передачи форм информации между центрами управления состояниями и событиями выполнения ТЦУ и реализации компьютерных атак

На рисунке 6 приняты обозначения:

Состояния выполнения ТЦУ в КВИС:

S_0 – ожидание форм информации от комплекса расчетных программ;

S_1 – прием и маршрутизация форм информации сервером электронной почты центра управления;

S_2 – передача форм информации в центр управления;

S_3 – прием форм информации абонентом центра управления.

Состояния реализации компьютерных атак:

Y_6 – ввод ложных данных;

Y_7 – перегрузка абонентов КВИС «спамом» технологических форм информации.

События выполнения ТЦУ в КВИС:

X_0 – информационно-логическое соединение СЭП центра управления с комплексом расчетных программ установлено;

X_1 – тракт информационного взаимодействия между СЭП центров управления установлен;

X_2 – прием форм информации абонентом центра управления завершен.

События реализации компьютерных атак:

A_6 – реализован ввод ложных данных;

A_7 – произошла перегрузка абонентов КВИС «спамом» технологических форм информации.

Системный анализ приведенных графов (соответствующих событий и состояний выполнения ТЦУ в КВИС и реализации компьютерных атак) и их формализация математическими моделями позволит при использовании соответствующих методов противодействия компьютерным атакам обеспечить устойчивость функционирования КВИС при реализации технологических циклов управления в условиях воздействия компьютерных атак.

2 Способы реализации компьютерных атак и обобщённый сценарий противодействия им

Анализ реализованных компьютерных атак в сфере высоких технологий показывает, что они осуществляются при наличии точек несанкционированного доступа или внутреннего нарушителя с полномочиями штатного оператора КВИС [1, 3, 31, 37-39, 41-43, 51, 54].

Модель уязвимых мест КВИС на базе эталонной модели взаимодействия открытых систем (ЭМ ВОС) представлена на рисунке 7.

Данная модель уязвимых мест, позволяет взаимоувязать уровни ЭМ ВОС и возможности по доступу нарушителя к сетевым сервисам, которые, по сути, и создают уязвимые места (точки несанкционированного доступа) для реализации компьютерных атак.

Для выявления уязвимых мест КВИС необходимо наличие информации о реализованных в них средствах защиты информации (СЗИ). При наличии данной информации есть возможность спрогнозировать компьютерные атаки на уязвимости КВИС. На практике идеальное построение КВИС не гарантирует полное устранение уязвимых мест, что обусловлено необходимостью использования открытых портов для взаимодействия в вычислительной сети и наличие человеческого фактора (качество настройки СЗИ зависит от квалификации обслуживающего персонала и знания им специфики функционирования КВИС).

При поиске уязвимых мест программно-алгоритмического обеспечения необходимо знать формальное описание программ, эксплуатационную документацию и реальный код в виде исходных текстов, для их сопоставления. Такое сопоставление позволяет выявить уязвимые места общего и специального программного обеспечения КВИС, программного обеспечения цифрового коммуникационного оборудования (ЦКО) и СЗИ, используемых в КВИС.

В качестве точек несанкционированного доступа могут выступать свободные порты в коммуникационном оборудовании, сетевые проводные и беспроводные интерфейсы, незащищенные стеки протоколов передачи данных, ошибочно реализованные функции общего и специального программного обеспечения и другие нарушения, не устраненные администратором информационной безопасности КВИС. В

современных условиях применения КВИС в роли внутреннего нарушителя выступают субъекты доступа, выполняющие несанкционированные воздействия, которые легендируются под штатные процессы эксплуатации КВИС [7, 8, 18, 21, 22, 50-52, 54].

Рисунок 7 – Модель уязвимых мест КВИС на базе ЭМ ВОС

Совокупность уязвимостей в КВИС, через которые осуществлены точки несанкционированного доступа (подключения), средства осуществления компьютерных атак и реализованный комплекс несанкционированных воздействий на элементы КВИС по сценарию нарушителя в и образуют основу компьютерных атак на КВИС.

Возможные сценарии реализации компьютерных атак нарушителем приведены на рисунке 8.

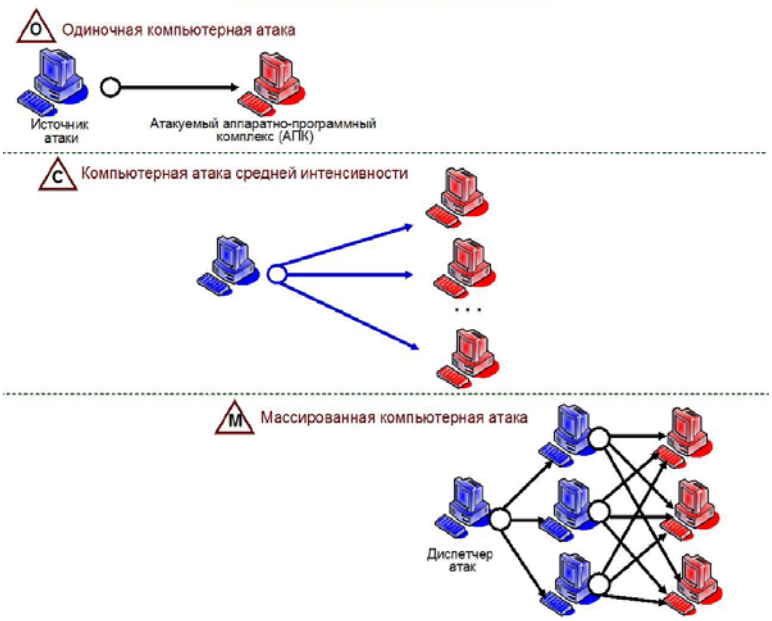


Рисунок 8 – Возможные сценарии реализации компьютерных атак

Анализ статистики, способов и форм реализации компьютерных атак [50-52, 54, 66] в локальных и региональных вычислительных сетях, глобальной сети Интернет обобщен в виде таблицы 1.

В настоящее время основные данные для статистики о компьютерных атаках (более 4000000 в 2012 году по статистике, собранной антивирусными средствами лаборатории Касперского) дают базы данных компьютерных атак, размещенные в сети Интернет и поддерживаемые крупными организациями разработчиками систем обнаружения компьютерных атак, общего программного обеспечения и исследовательскими центрами [31, 38, 54, 63].

Следует отметить, что данные по анализу компьютерных атак в таблице 1 и в других публикациях, как правило, относятся к сети Интернет. По сути, глобальную сеть Интернет условно можно считать сложившимся макрополигоном для отработки базовых технологий противодействия компьютерным атакам на КВИС.

Таблица 1 – Основные способы реализации компьютерных атак

№ п/п	Наименование компьютерной атаки	Способы реализации компьютерных атак	Область применения и пример реализации
1.	«Ложная информация»	логическая подмена сервера – реализация атаки по перенаправлению запросов штатных программ к ложному серверу путем	Интернет-сети; программы формирования ложных DNS и ARP серверов,

		искажения таблицы соответствия между IP-адресацией и DNS-адресацией с целью выдачи потребителю ложной или ненужной для его работы информации;	подмены Web-узлов, искажения системных журналов.
		введение ложной информации (дезинформации) – организация атаки по проникновению в базы и хранилища данных специальной информации, Web-серверы и размещение (тиражирование) заведомо ложной информации.	Интернет-сети и сети TCP/IP различных приложений; программы взлома Web-серверов; запись ложной информации в базы данных.
2.	«Функциональное поражение»	локальный «отказ в обслуживании» – проведение атаки по нарушению функционирования КВИС, «зависание» и (или) перезагрузка ПЭВМ, на которой выполняется атака или находящейся в составе ЛВС;	сети TCP/IP различных приложений; в структуре ЛВС на базе ОС Windows 2000 (XP, 7);
		удаленный «отказ в обслуживании» – организация атаки по нарушению функционирования КВИС «зависание» и (или) и перезагрузка ПЭВМ в режиме удаленного доступа;	Интернет-сети; teardrop;
		сканирование сети и её уязвимостей – реализация атаки по несанкционированному анализу топологии сети, открытых портов абонентов, выявление уязвимостей, адресов серверов и доступных сервисов, которые могут быть использованы для атаки;	сети TCP/IP различных приложений; комплексы программ SATAN, Shadow, nmap
		сканирование протоколов передачи данных сети – осуществление атаки по несанкционированному анализу сетевого трафика с целью оценки загрузки трафика, добывания сведений об идентификации, аутентификации операторов КВИС;	сети TCP/IP различных приложений; различные версии программ – snifferrs;
		«взламывание» паролей – реализация атаки по генерации и подбору	сети TCP/IP различных приложений; комплексы

		паролей операторов и администраторов сети для подключения к информационным ресурсам КВИС от лица штатного субъекта доступа;	программ L0phtCrack, John the Ripper;
		локальное проникновение в КВИС – выполнение атаки по несанкционированному доступу к информационным ресурсам ПЭВМ (серверу сети), на которых выполняется программа атаки, в интересах нарушения порядка администрирования сети;	Интернет-сети; программа Getadmin;
		удаленное проникновение в КВИС – реализация атаки по несанкционированному доступу к информационным ресурсам ПЭВМ (серверу сети) с целью захвата управления ими в режиме удаленного доступа и манипулирования системными функциями;	Интернет-сети и сети TCP/IP различных приложений; программа SubSeven, BackOrifice;
		разрушение информации и программ – осуществление атаки с целью нанесения ущерба информационным ресурсам нарушителя.	Интернет-сети и сети TCP/IP различных приложений; массовые взломы сайтов информационных агентств и государственных учреждений, компьютерные преступления в финансовой сфере
3.	«Разрыв соединения»	логическое отключение абонентов – выполнение атаки по отключению информационно-логического взаимодействия абонентов в сети при использовании технологии «клиент – сервер»;	сети TCP/IP различных приложений;

		перенаправление пакетов данных – реализация атаки на основе получения доступа к цифровому коммуникационному оборудованию с программным управлением с целью искажения порядка маршрутизации пакетов передачи данных в сети (перехвата управления сетью).	сети TCP/IP различных приложений
4.	«Спам»	«спам» – выполнение атаки в форме рассылки в сети значительного количества пакетов передачи данных с неактуальной информацией и с электронной почтой, в которой скрыты различные компьютерные атаки (создаются условия для критической нагрузки на сеть).	Интернет-сети; от 30 до 90 % электронной почты в сети Интернет является «спамом»

Тем не менее, современные КВИС строятся, как и сети Интернет, на базе стандартных протоколов (стеков протоколов) TCP/IP. Поэтому, опыт отработки компьютерных атак в сети Интернет может быть успешно адаптирован для КВИС замкнутых сетей передачи данных специального назначения при наличии внутреннего нарушителя.

Обобщенный сценарий противодействия компьютерным атакам представлен на рисунке 9.

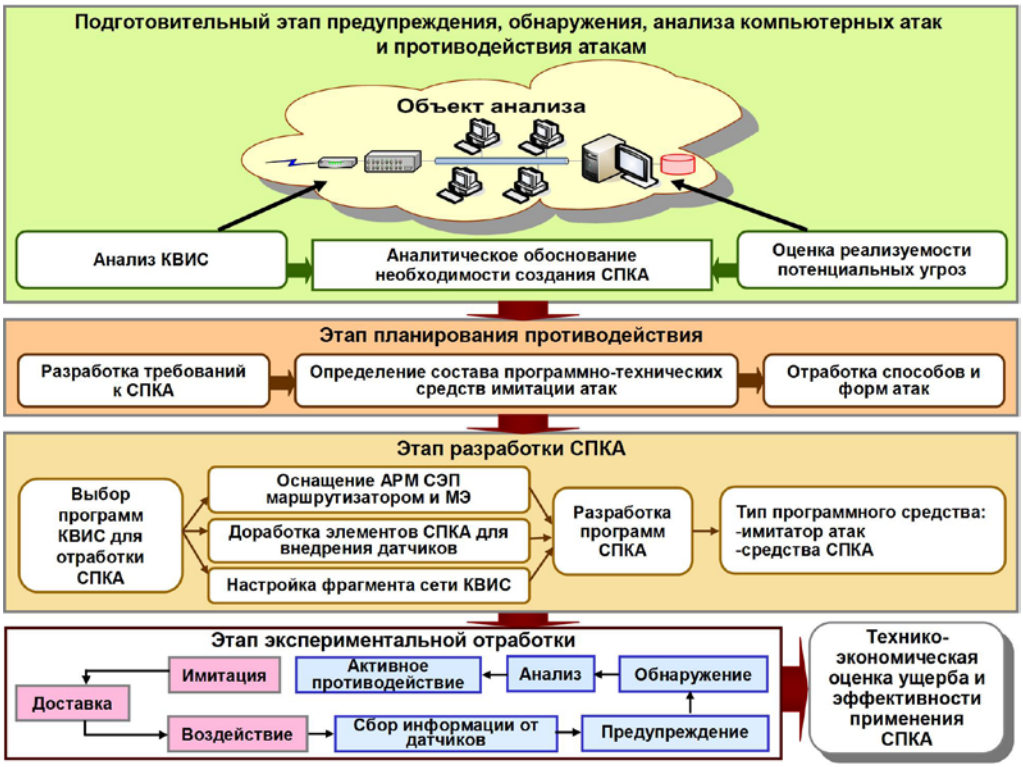


Рисунок 9 – Обобщенный сценарий противодействия компьютерным атакам

Порядок реализации обобщенного сценария включает в свой состав четыре этапа:

- подготовительный этап предупреждения, обнаружения и анализа компьютерных атак, который заканчивается аналитическим обоснованием характеристик объекта защиты (КВИС) и средств СПКА;
- этап планирования, в основном заключающийся в разработке требований к составу и функциям СПКА;
- этап разработки средств СПКА, состоящий в том, что в узлы КВИС внедряются датчики и производится настройка сети анализируемого объекта;
- этап экспериментальной оценки позволяет отработать сценарий применения СПКА: имитация воздействия атак (имитация, доставка, воздействие), противодействие атакам (сбор информации от датчиков, обнаружение, анализ, визуализация, активное противодействие).

3 Классификация компьютерных атак на критически важные информационные системы

Средства реализации компьютерных атак на КВИС представляют собой совокупность программных или программно-аппаратных средств, предназначенных для нарушения (искажения) информационно-вычислительного процесса, заданной технологии и регламентов сбора, обработки и передачи информации и целенаправленного срыва ТЦУ.

Совокупность компьютерных атак по видам воздействия декомпозируются на:

- информационно-коммуникационные, которые состоят в искажении, нарушении, подмене данных, находящихся на каком-либо накопителе информации, в процессе сбора, обработки, хранения или передачи с использованием телекоммуникационных средств;
- функциональные, заключающиеся в изменении, задержке выполнения (искусственном замедлении), блокировании, нарушении штатных функций, установленных в эксплуатационной документации на КВИС;
- информационно-психологические, определенные как программно-технические воздействия текстовой, графической и звуковой информацией (дезинформацией) на оператора, приводящие к нарушению его функциональных обязанностей (в монографии не рассматриваются).

В настоящее время в компьютерной литературе предложены классификации компьютерных атак [37, 38, 42, 43, 54, 63, 66, 68], которые могут служить основой для исследования свойств атак и средств противодействия им. Однако известные классификации обобщают атаки для сетей общего пользования типа Интернет, не имеют классификационных признаков систематизации данных, недостаточно информативны, носят частный характер обобщения отдельных атак хакеров на конкретные операционные системы, и не являются строго научной классификацией компьютерных атак.

В предложенной классификации компьютерных атак установлено соответствие между основными характеристиками элементов КВИС, спецификой их применения и особенностями реализации атак по принятым классификационным признакам.

Разработка классификации компьютерных атак основана на материалах ГОСТ Р 51275-99 «Объект информатизации. Факторы, воздействующие на информацию», руководящих документах ФСТЭК России, опыте разработки и научно-методического сопровождения КВИС и результатах исследований в области противодействия компьютерным атакам [42, 43, 54, 63].

Действующие нормативные документы определяют лишь виды программно-аппаратных воздействий и не в полной мере позволяют классифицировать компьютерные атаки на КВИС. При разработке классификатора компьютерных атак были использованы общие подходы к классификации объектов в области информационных технологий и существующие научные методы классификации угроз безопасности информации [5-24, 26-30, 40-44, 57].

Для пояснения сущности построения автоматизированных систем в защищенном исполнении при учете угроз несанкционированных воздействий (по мнению автора, понятие близкое к компьютерной атаке) используются ГОСТ Р 51624-2000, ГОСТ 51583-2000.

Классификация компьютерных атак, направленных на нарушение устойчивости функционирования КВИС, представлена в таблице 2.

Классификация компьютерных атак представляет собой систематический перечень классификаторов, обобщенных в виде таблиц и позволяющих определить для каждой из них место на множестве различных атак. Индекс классификатора в таблице 2 определяет один из 17 классификационных признаков компьютерных атак. Набор индексов позволяет в полном объеме дать характеристику свойствам атаки и особенностям ее реализации.

На основе классификации и системного анализа компьютерных атак, направленных на нарушение динамических процессов выполнения ТЦУ, в диссертации разработаны методы, модели и алгоритмы противодействия наиболее характерным для КВИС атакам.

Множество классов компьютерных атак, образуемое объединением классификаторов Y_{ij}, позволяет выявить совокупность неблагоприятных факторов КВИС, связанных с особенностями их применения. Классификатор $Y_{4.5}$ – «нарушение протоколов передачи данных или искажение информации в каналах связи» характеризует уровни эталонной модели взаимодействия открытых систем ISO/OSI (стандарт ISO 7498), на которые осуществляется воздействие компьютерными атаками.

Следует отметить, что классификатор компьютерных атак на протоколы передачи данных целесообразно поставить в соответствие с классификацией сетевого общего и специального программного обеспечения КВИС согласно модели ISO/OSI.

Таблица 2 – Классификация компьютерных атак на КВИС

№ п/п	Классификационный признак компьютерной атаки	Индекс классификатора (Y_{ij})	Содержание классификатора
1.	По источнику атаки	Y11 Y12	Внешние Внутренние
2.	По цели воздействия	Y21 Y22 Y23	Нарушение целостности Нарушение доступности Нарушение штатного режима функционирования
3.	По принципу воздействия	Y31 Y32 Y33	Использование существующих (штатных) каналов доступа Использование скрытых каналов доступа Формирование новых каналов доступа
4.	По способам воздействия	Y41 Y42 Y43 Y44 Y45 Y46	Нарушение структур данных Нарушение текстовых файлов, объектных и загрузочных кодов программ Нарушение функций общего ПО КВИС (операционной системы, системы управления базами данных и других программ) Нарушение функций специального ПО КВИС Нарушение сети (протоколов) передачи данных Искажение программ и информации в цифровом коммуникационном оборудовании
5.	По характеру воздействия	Y51 Y52 Y53 Y54	Активное воздействие (нарушение, разрушение, искажение) Пассивное воздействие (сбор информации, наблюдение, анализ) Интерактивный режим нарушителя с объектом (субъектом) доступа Воздействие при выполнении ТЦУ (осуществлении информационно-вычислительного процесса обработки данных)
6.	По объектам и субъектам воздействия	Y61 Y62 Y63	Пункты управления Мобильные пункты управления Центры управления

№ п/п	Классификационный признак компьютерной атаки	Индекс классификатора (Y_{ij})	Содержание классификатора
		Y64 Y65	Операторы Лица, принимающие решения
7.	По средствам воздействия	Y71 Y711 Y712 Y72 Y721 Y722 Y723 Y724 Y725 Y726 Y73 Y731 Y732 Y74	«Ложная информация»: – искажения информации; – введение дезинформации «Функциональное поражение»: – нарушение режимов функционирования; – блокирование информации («отказ в обслуживании»); – разрушение (стирание информации); – перехват информации; – разглашение (утечка) информации; – хищение информации. «Разрыв соединения»: – логическое отключение абонентов; – перенаправление пакетов данных (искажение порядка маршрутизации). «Спам»
8.	По используемой ошибке	Y81	Ошибки в работе администратора локальной вычислительной сети и администратора безопасности информации
9.	По состоянию нарушаемых технологических операций	Y91 Y92 Y93	Сбор, прием, передача данных, обмен информацией Осуществление информационно-вычислительного процесса Запись, считывание, хранение информации в базе данных
10.	По уровню эталонной модели взаимодействия открытых систем (ЭМВОС)	Y10 1 Y10 2 Y10 3 Y10 4 Y10 5 Y10 6 Y10 7	Физический Канальный Сетевой Транспортный Сеансовый Представительский Прикладной
11.	По типу воздействия	Y11.1 Y11.2	Программное Программно-техническое
12.	По потенциальному	Y12.1	Низкий ущерб (несущественный, на уровне административных решений)

№ п/п	Классификационный признак компьютерной атаки	Индекс классификатора (Y_{ij})	Содержание классификатора
	ущербу	Y12.2 Y12.3 Y12.4	Средний ущерб (требует материальных затрат) Высокий ущерб (значительный материальный ущерб) Катастрофический ущерб (ущерб на уровне затрат, приводящих к корректировке расходования бюджетных средств государства)
13.	По соответствию требованиям к средствам защиты информации	Y13.1 Y13.2 Y13.3 Y13.4 Y13.5	Класс защищенности для АС Класс защищенности для СВТ Класс защищенности для межсетевых экранов Класс защищенности для антивирусных средств Класс по контролю отсутствия недекларированных возможностей
14.	По сценариям воздействия субъекта доступа	Y14.1 Y14.2 Y14.3 Y14.4 Y14.5 Y14.6 Y14.7	Внешний злоумышленник (вероятный противник) Санкционированный оператор Санкционированный абонент удаленного доступа Зарегистрированный оператор внешней системы Администратор КВИС Администратор безопасности информации Программист – разработчик
15.	По этапам жизненного цикла системы	Y15.1 Y15.2	Технологические воздействия Эксплуатационные воздействия
16.	По характеру возникновения	Y16.1 Y16.2	Преднамеренные воздействия Непреднамеренные воздействия
17.	По виду совершенного компьютерного преступления	Y17.1 Y17.2 Y17.3	Неправомерный доступ к компьютерной информации Создание, использование и распространение вредоносных программ Нарушение правил эксплуатации средств вычислительной техники и программного обеспечения
Примечание: Приняты обозначения классификатора Y_{ij}: i – группа классификатора, j – номер классификатора в группе.			

Сертифицированные средства защиты удаленного доступа – межсетевые экраны – в настоящее время обеспечивают защиту на физическом, канальном, сетевом, транспортном уровнях. Противодействие компьютерным атакам функциями межсетевого экрана на сеансовом, представительном и прикладном уровнях не предусматривается, что представляет существенную опасность нарушения устойчивости функционирования КВИС. Поэтому, при построении системы комплексного противодействия компьютерным атакам необходимо предусмотреть меры защиты сетевых программ и протоколов передачи данных на всех уровнях модели ISO/OSI согласно стандарту ISO 7498 [17].

Классификатор $Y_{6.j}$ – «по объектам и субъектам воздействия» характеризует базовые объекты КВИС – пункты и центры управления.

Классификатор $Y_{7.j}$ – «по средствам воздействия» должен быть ключевым при регистрации атаки и определении способа и формы ее реализации.

Классификатор $Y_{13.j}$ – (по соответствию требованиям к классу защищенности автоматизированных систем и средств вычислительной техники) отражает соответствие характеристик компонентов КВИС и уровня конфиденциальности защищаемой информации руководящим документам ФСТЭК России.

Классификатор $Y_{15.j}$ – «по этапам жизненного цикла системы» определяет период времени воздействия компьютерной атаки на КВИС: технологические воздействия – на этапах проектирования, разработки и внедрения КВИС, эксплуатационные воздействия – на этапах эксплуатации и модернизации КВИС.

Классификатор $Y_{16.2}$ «непреднамеренные воздействия» определяет события в работе КВИС, при которых происходят случайные (незлонамеренные) нарушения устойчивости её функционирования (надежности, оперативности и т.д.), в части программных средств, оценка характеристик качества производится по ГОСТ 28195-89.

Классификаторы $Y_{17.1} – Y_{17.3}$ определены в соответствии с главой 28 «Преступления в сфере компьютерной информации», статьями 272 - 274 Уголовного Кодекса Российской Федерации.

Анализ предложенной классификации компьютерных атак показывает, что значительная часть воздействий ($Y_{7.j}$) связана с преднамеренным нарушением программ и информации, используемых в цифровом виде. Осуществление информационно-вычислительного процесса в КВИС при выполнении требований к объемам обрабатываемой информации, точности вычислений и временных

ограничениях на выполнение ТЦУ обуславливает актуальность разработки методов, моделей и алгоритмов противодействия компьютерным атакам на КВИС. Разработанная классификация компьютерных атак на КВИС реализована в имитаторе атак, который позволил провести исследования и получить оценки эффективности применения методов, моделей и алгоритмов противодействия атакам с обеспечением устойчивости функционирования КВИС в рамках экспериментов (п. 6) на стендовом полигоне.

4 Роль и место противодействия компьютерным атакам в обеспечении устойчивости функционирования критически важных информационных систем

Роль и место противодействия компьютерным атакам в обеспечении устойчивости функционирования КВИС определяется следующими факторами:

- особенностями применения КВИС в условиях воздействия компьютерных атак (прежде всего, временными ограничениями на выполнение ТЦУ);
- возможными последствиями нарушения устойчивости функционирования КВИС;
- вкладом в эффективность выполнения ТЦУ в КВИС.

Модель нарушения устойчивости функционирования КВИС в условиях компьютерных атак приведена на рисунке 10.

В условиях воздействия компьютерных атак на КВИС без применения средств противодействия компьютерным атакам (СПКА) существует потенциальная опасность невыполнения ТЦУ и потери его управляемости элементов КВИС. Следствием подобных воздействий будет срыв (некачественное выполнение) установленного порядка доведения информации до потребителей.

Анализ КВИС показывает, что средства противодействия компьютерным атакам должны иметь распределенную структуру компонентов внедренных в виде датчиков в программное и информационное обеспечение, позволяющих проводить мониторинг компьютерных атак в процессе выполнения ТЦУ и предупредить их на ранней стадии информационной акции нарушителя. Нейтрализация и блокирование атак, нарушающих устойчивость функционирования КВИС, должна осуществляться методами обнаружения и анализа (сигнатурного и функционального) и анализа аномальных событий. В комплексе средств автоматизации КВИС, находящемся в эксплуатации, отклонение от ТЦУ (взаимосвязанных во времени процессов сбора, передачи и обработки заданных объемов информации и соответствующих им функций специального программного обеспечения, зафиксированных в эксплуатационной документации) является аномальным и анализируется как возможное воздействие компьютерной атаки.

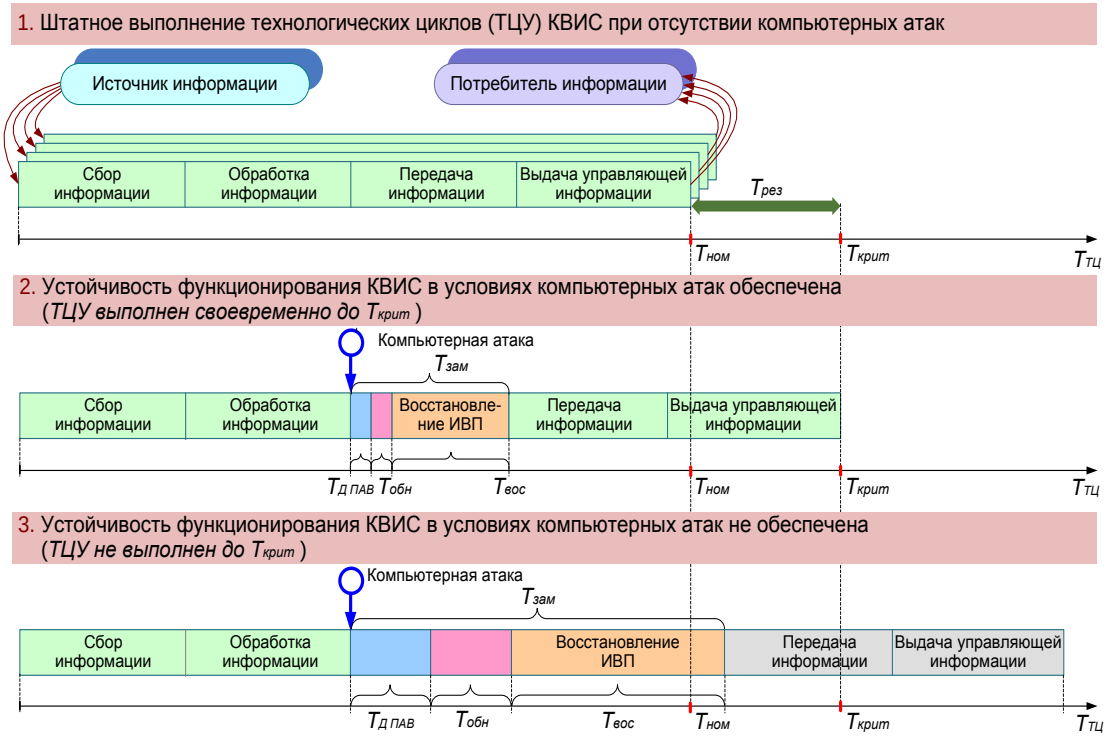


Рисунок 10 – Модель нарушения устойчивости функционирования КВИС в условиях компьютерных атак

Противодействие компьютерным атакам осуществляется методами и средствами блокирования источника атаки, логического отключения абонента администратором КВИС, файла выявления и уничтожения программного кода и данных атаки, реконфигурацией КВИС на защищенные фрагменты и динамическим восстановлением информационно-вычислительного процесса по контрольным точкам. Эффективное функционирование СПКА возможно лишь при комплексном и взаимосвязанном применении средств защиты от несанкционированного доступа, антивирусных средств и межсетевых экранов.

Результаты работы этих средств (системные журналы) будут наряду с датчиками источником информации для выявления атак. Особенно важна согласованность работы СПКА с администраторами вычислительной сети и безопасности информации. В конечном итоге СПКА развивает и дополняет функциональные возможности администратора безопасности по противодействию новой угрозе снижения устойчивости функционирования и возможного интеллектуального поражения КВИС в результате воздействия компьютерной атаки.

Возможные последствия нарушения устойчивости функционирования КВИС в результате реализации взаимосвязанной совокупности угроз информационной безопасности и компьютерных атак представлены в таблице 3.

Таблица 3 – Возможные последствия нарушения устойчивости функционирования КВИС в результате реализации совокупности угроз информационной безопасности и компьютерных атак

Объекты воздействия	Возможные последствия нарушения устойчивости функционирования КВИС			
	компьютерные атаки	несанкционированный доступ (НСД) к информации	компьютерные вирусные воздействия	проявление недекларированных возможностей (НДВ)
Пункты управления	Последствия: нарушение выполнения (снижение качества выполнения) планов работ по объектам управления. Способы воздействия: программно-аппаратные воздействия на средства ЛВС, разрабатываемые по технологии «Intranet» и IP-телефонии; ввод ложных данных; сбор некачественной (ложной) информации; несанкционированные подключения внешних абонентов к серверам баз данных; воздействия компьютерных вирусов; проявления НДВ и НСД к информации.			
Центры (сектора) управления	Последствия: комплексное нарушение процессов управления и нештатное функционирование КВИС, потеря актуальной управляющей информации. Способы воздействия: программно-аппаратные воздействия на ЛВС, искажение данных, несанкционированные подключения внешних абонентов к пунктам управления, разрыв соединений между абонентами, воздействия компьютерных вирусов, проявления НДВ и НСД к информации.			
Потребители информации	Последствия: не выполняются целевые задачи информационного обеспечения и вследствие этого снижение эффективности управления. Способы воздействия: косвенные воздействия на КВИС. В случае несанкционированного подключения к средствам обработки информации создаются дополнительные предпосылки для реализации компьютерных атак, воздействия компьютерных вирусов, проявления НДВ и НСД к информации.			

<table>
<tr><td rowspan="2">Объекты воздействия</td><td colspan="4">Возможные последствия нарушения устойчивости функционирования КВИС</td></tr>
<tr><td>компьютерные атаки</td><td>несанкционированный доступ (НСД) к информации</td><td>компьютерные вирусные воздействия</td><td>проявление недекларированных возможностей (НДВ)</td></tr>
<tr><td>Территориально-распределенные вычислительные сети, локальные вычислительные сети (ЛВС)</td><td colspan="4">Последствия: нарушение информационно-логического взаимодействия абонентов, функций мониторинга сети, электронной почты и протоколов передачи данных.
Способы воздействия: искажение, блокирование, уничтожение пакетов данных, нарушение адресации и порядка администрирования сети, настройка ложной маршрутизации пакетов данных при недостаточной защите удаленного доступа межсетевыми экранами, отсутствии средств предупреждения и обнаружения компьютерных атак, возможностях НСД к информации и проявлении НДВ, проникновении компьютерных вирусов.</td></tr>
<tr><td>Сетевые операционные системы (ОС)</td><td colspan="4">Последствия: нарушение информационно-вычислительного процесса в КВИС и прав доступа к информационным ресурсам ОС.
Способы воздействия: программно-аппаратные воздействия на системные файлы и регистры ОС, несанкционированный перезапуск и «зависание» ОС, взлом программ разграничения доступа операторов к информации при недостаточно эффективной работе встроенных средств защиты от НСД и администрирования ОС, программного межсетевого экрана, антивирусных средств, проявлении НДВ, (датчика ОС – при установке СПКА).</td></tr>
<tr><td>Система управления базами данных (СУБД) и базы данных (БД)</td><td colspan="4">Последствия: нарушение целостности и доступности данных в результате искажения информационных таблиц и прав доступа к информационным ресурсам СУБД.
Способы воздействия: ввод ложных данных, искажение алгоритмов обработки транзакций, нарушение структуры интерфейсов и целостности БД, создание условий для противоречивости предоставляемых данных вследствие воздействия атак, НСД к информации, наличия уязвимых мест в средствах защиты СУБД, БД и НДВ в ее программах при отсутствии средств противодействия компьютерным атакам в серверах сбора информации.</td></tr>
</table>

Объекты воздействия	Возможные последствия нарушения устойчивости функционирования КВИС			
	компьютерные атаки	несанкционированный доступ (НСД) к информации	компьютерные вирусные воздействия	проявление недекларированных возможностей (НДВ)
Специальное программное обеспечение, комплексы расчетных программ	Последствия: нарушение точности и достоверности данных, необходимых для качественного выполнения ТЦУ и прав доступа к СПО; невыполнение (несвоевременное выполнение) требуемого объема вычислительных технологических операций. Способы воздействия: ввод ложных данных, блокирование, останов выполнения программ, искажение входных данных и результатов расчета, инициализация ложных событий реконфигурации КВИС при наличии в программном обеспечении ошибок и недекларированных возможностей.			

Анализ таблицы 3 показывает, что для обеспечения устойчивости функционирования КВИС необходимо предусмотреть разработку методов и средств противодействия компьютерным атакам в процессе внедрения новых информационно-телекоммуникационных технологий в территориально-распределенных и локальных вычислительных сетях, базах данных, специальном программном обеспечении (СПО) КВИС.

Под противодействием компьютерным атакам на КВИС понимаются взаимосвязанные процессы предупреждения о фактах угроз подготовки к реализации компьютерных атак, обнаружения признаков атак, анализа параметров атак и активного противодействия источникам атаки, а также комплексная защита КВИС от подобных воздействий.

По результатам моделирования компьютерных атак, опыта научно-методического сопровождения КВИС и экспертной оценки вклад средств противодействия компьютерным атакам в обеспечение устойчивости функционирования КВИС для общего случая иллюстрируется рисунками 11 и 12 [49, 55, 70].

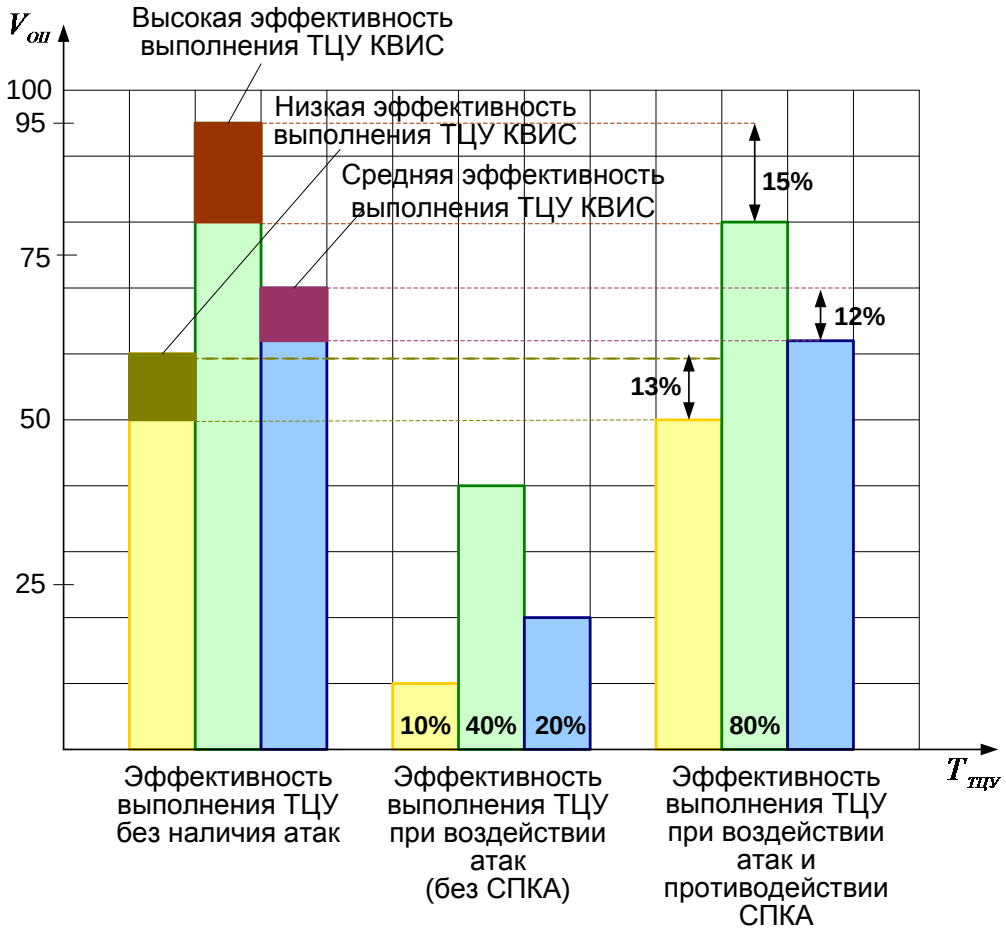


Рисунок 11 – Зависимость объема технологических операций (в процентах от общего объема) от времени выполнения ТЦУ КВИС

Устойчивость функционирования КВИС в условиях воздействия компьютерных атак – свойство КВИС выполнить заданный объем технологических операций за установленный период времени при воздействии компьютерных атак. Показателем устойчивости функционирования КВИС является вероятность устойчивости функционирования, требуемое значение которой для большинства современных КВИС определяется значением $P_{уф\ тр} = 0.95$.

Эффективность выполнения ТЦУ характеризуется полнотой объема (процент от общего числа необходимых операций) выполненных технологических операций на временном интервале ТЦУ.

Гистограмма на рисунке 11 показывает, что воздействие компьютерных атак на КВИС при начальной высокой эффективности выполнения ТЦУ $V_{ОП}$ = 95% (за счет оперативности вычислений и обмена данными, высокой надежности программно-аппаратных средств) снижает устойчивость функционирования приблизительно до

величины $V_{ОП}$ = 40%. А при низкой эффективности выполнения ТЦУ приводит фактически к полному нарушению информационно-вычислительного процесса $V_{ОП}$ = 10%.

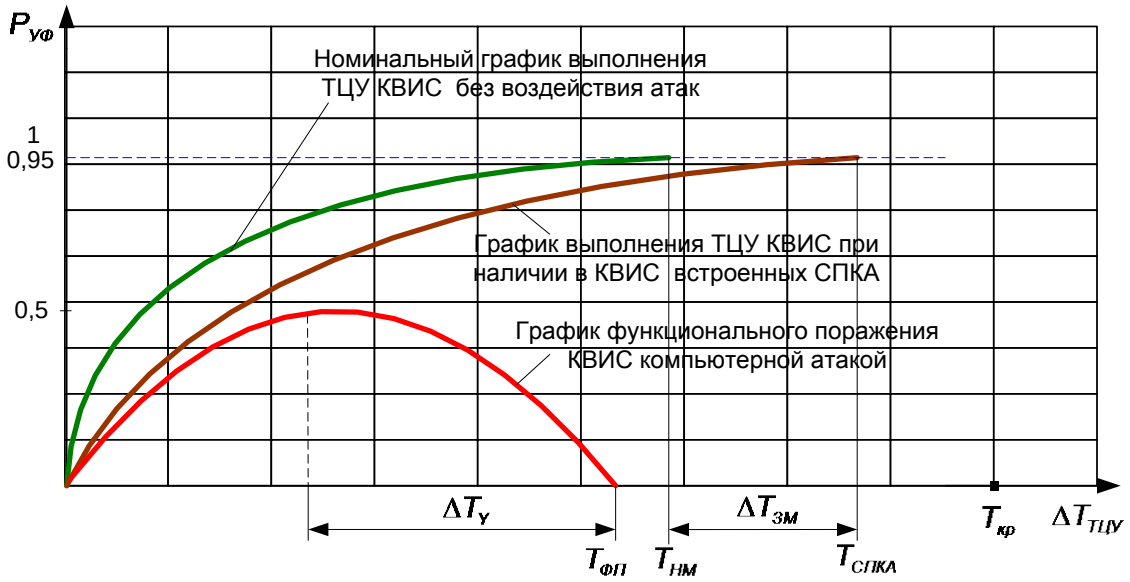


Рисунок 12 – Зависимость вероятности устойчивости функционирования КВИС от времени выполнения ТЦУ КВИС

Использование средств противодействия компьютерным атакам несколько снижает эффективность выполнения ТЦУ за счет дополнительной загрузки трафика сети и использования вычислительных ресурсов КВИС, но в конечном итоге позволяет выполнить целевую задачу по обеспечению устойчивости функционирования КВИС ($V_{ОП}$ = 80%).

Иллюстративные графические зависимости на рисунке 12 наглядно демонстрируют опасность функционального поражения КВИС без встроенной СПКА от начала действия атаки до момента времени функционального поражения $T_{ФП}$ ($\Delta T_У$ – время действия компьютерной атаки). При использовании СПКА происходит «замедление» процесса выполнения ТЦУ на время $\Delta T_{ЗМ}$ и за большее время достигается требуемое значение вероятности устойчивости функционирования КВИС ($T_{СПКА}$ – время завершения ТЦУ при использовании СПКА). Тем не менее, наличие временной избыточности на выполнение ТЦУ в КВИС дает возможность после момента наступления номинального времени $T_{НМ}$, но до времени $T_{кр}$ выполнить ТЦУ в установленный срок с приемлемым качеством.

Как видно из анализа рисунков 11 и 12 при разработке методов и моделей противодействия компьютерным атакам необходимо разрешить противоречие между требуемой оперативностью выполнения технологических операций и задержками времени, связанными с дополнительной загрузкой сетевого трафика и использованием вычислительного ресурса на работу средств противодействия компьютерным атакам. Методы противодействия компьютерным атакам должны не только позволять оперативно обнаружить атаки, но и обеспечить устойчивость функционирования КВИС в квазиреальном масштабе времени, а также предусматривать активное противодействие компьютерным атакам с целью недопущения их усиления и полного блокирования источника возникновения этих атак.

5 Анализ средств противодействия компьютерным атакам

Осуществление хакерами все более изощренных атак в сетях общего пользования (аналогичных по принципам построения закрытым сетям) показывает, что уязвимости протоколов передачи данных и операционных систем, потенциальные ошибки в специальном программном обеспечении [1, 3, 4, 22, 34, 37-39, 41-44, 54, 55] обуславливают необходимость создания самостоятельных средств противодействия компьютерным атакам. Современные средства защиты информации от несанкционированного доступа (НСД) в локальных вычислительных сетях и средства защиты удаленного доступа к информации – межсетевые экраны не обеспечивают противодействие компьютерным атакам в КВИС.

Причиной этого является отсутствие факторов угроз воздействия компьютерных атак с целью преднамеренного нарушения функционирования (интеллектуального вывода из строя) информационно-телекоммуникационных средств в традиционной модели угроз (нарушения конфиденциальности, целостности и доступности информации) и модели нарушителя [16, 22, 28-30, 61-64]. Следует отметить, процессы нарушения целостности и доступности информации входят в состав возможных программно-аппаратных воздействий на основе сценариев реализации компьютерных атак.

Межсетевые экраны, как правило, обеспечивают защиту информации в режиме удаленного доступа от физического до транспортного уровня ЭМВОС на основе контроля возможных IP - адресов абонентов сети. При этом межсетевые экраны являются лишь источником и средством сбора исходных данных для интеллектуального выявления и противодействия атак. В межсетевых экранах не предусматривается набор интеллектуальных датчиков, контролирующих информационно-вычислительный процесс в СПО, ОС, СУБД и коммуникационном оборудовании, а также подготовки принятия решения для активного противодействия нарушителю.

Обобщенный анализ характеристик средств противодействия компьютерным атакам на основе оценки публикаций по разработанным средствам обнаружения атак [1, 3, 4, 22, 34, 37-39, 41-44, 54, 55], приведен в таблице 4.

Разработанные СПКА позволяют осуществлять дополнительные к известным средствам защиты от НСД механизмы разграничения доступа в сети путем нарушения сетевого трафика, обхода средств защиты, использования их уязвимостей. Однако коммерческие СПКА существенно снижают оперативность передачи данных в сети в виду значительной дополнительной загрузки трафика (30-50% от общего объема) и настройки на обнаружение избыточного числа возможных атак (Real Secure около 700 атак и Dragon более 3000 атак). В отличие от сети Интернет в замкнутой сети КВИС с конкретным числом IP-адресов источников и потребителей информации и ввиду наличия технологических ограничений на эксплуатацию ОПО, СПО, СУБД, коммуникационного оборудования возможных типов атак не более 20.

Общим недостатком приведенных в таблице средств является слабо развитые возможности функционального анализа регламентов обработки информации СПО, контроля специфики технологических процессов КВИС и выявления неизвестных атак. Кроме того, массированные атаки в форме спама сообщений может приводить к переполнению системных журналов, таблицы маршрутизации, системной памяти и «отказу в обслуживании» самих средств обнаружения компьютерных атак.

Таблица 4 – Анализ характеристик средств противодействия компьютерным атакам

№ п/п	Наименование средства	Реализованный метод обнаружения атак	Принцип действия	Основные функции
1.	Real Secure (разработчик – Internet Security Systems)	Сигнатурный анализ и анализ аномалий в сети	Сравнительный анализ результатов оценки сетевого трафика от сенсоров с базой данных сигнатур атак (обнаруживает около 700 атак в сети Интернет)	– выявление потенциально опасных (неправомерных) действий по шаблону фильтрации трафика сети, – обнаружение несанкционированного доступа к ресурсам сети по фильтрации протоколов Telnet, FTP, SMTP, NNTP, – идентификация злоумышленников в сети по портам и IP-адресам абонентов, – реагирование на атаки

№ п/п	Наименование средства	Реализованный метод обнаружения атак	Принцип действия	Основные функции
				путем реконфигурации отдельного коммуникационного оборудования, – взаимодействие со средствами администратора безопасности сети, – возможность создания собственных шаблонов атак, – запись и воспроизведение атаки, – использование ОС ряда Windows.
2.	Dragon (разработчик – Enterasys Networks)	Сигнатурный анализ и анализ аномалий в сети	Выявление атак по результатам мониторинга сети, включая анализ сигнатур в протоколах передачи данных и идентификацию несанкционированных действий в сети	– мониторинг безопасности сети в реальном масштабе времени, – обнаружение злонамеренных действий по искажению сетевых настроек, – анализ системных журналов межсетевых экранов, – проверка целостности системных файлов, контроль доступа к ресурсам сети – управление сенсорами и контроль потоков событий от датчиков, – определение потенциальных вторжений только для известных сигнатур, – поддержка базой данных сигнатур более 3000 сигнатур атак, – использование сервером и сетевым сенсором Dragon ОС Solaris, Linux, FreeBSD.

№ п/п	Наименование средства	Реализованный метод обнаружения атак	Принцип действия	Основные функции
3.	TriSentry (разработчик – Psionic Technologies)	Анализ аномалий в сети	Интеллектуальный контроль доступа к сети детектором сканирования в реальном масштабе времени	– выявление фактов сканирования портов сервера, – контроль протокола по настройкам файла конфигурации, – предотвращение доступа от сканируемого сервера к клиентам сети, – возможность описания сигнатур атак, – анализ состояния безопасности сети по базовой таблице IP-адресов, – использование ОС ряда Unix.
4.	IDS/9000 (разработчик – Hewlett-Packard)	Анализ аномалий в сети	Мониторинг системных событий, файлов и протоколов передачи данных на основе использования программ «агентов» с целью обнаружения компьютерных атак	– идентификация атак по IP-адресу или логическому имени абонента, – обнаружение изменений прав доступа, – выявление фактов использования прав администратора, – обнаружение нестандартных процессов в операционной системе, – контроль процессов регистрации операторов и назначения полномочий администратора, – обнаружение попыток модификации файлов.
5.	Snort (Snort Wireless) – разработчик Source Fire	Сигнатурный анализ в сети	Анализ сетевого трафика в реальном масштабе времени и регистрацию	– выявление потенциальных атак по сигнатурам (база данных содержит более 1500 сигнатур), – фильтрация сетевого трафика в заданном

№ п/п	Наименование средства	Реализованный метод обнаружения атак	Принцип действия	Основные функции
			событий информационной безопасности в распределенной вычислительной сети (проводной и беспроводной).	диапазоне IP-адресов абонентов, – предупреждение администратора информационной безопасности об обнаруженных атаках в реальном масштабе времени на основе централизованной системы мониторинга и обработки событий, – тестирование Web-узлов, – возможность использования модулей расширений для применения дополнительных способов выявления атак, – протоколирование подозрительных событий в сетевом трафике, – использование ОС ряда Windows и Unix.

В настоящее время известно более двадцати средств обнаружения компьютерных атак на основе методов анализа сигнатур, выявления аномалий или комбинированного применения этих методов [37, 38, 41-43]. Главным образом они ориентированы на обнаружение атак в сети Интернет и соответствующие сетевые сервисы.

Общей характеристикой этих систем является наличие датчиков, которые извещают о возможных событиях вторжений атак в КВИС как на программном, так и аппаратном уровне. Многие из систем обнаружения атак используются совместно с межсетевыми экранами и обладают функциями взаимодействия с операционной системой.

В дальнейшем прогнозируется развитие средств обнаружения атак в направлении создания иерархической сети интеллектуальных датчиков, разработки совершенных алгоритмов распознавания неизвестных атак в реальном масштабе

времени и реализации специализированных средств, обеспечивающих эффективное противодействие компьютерным атакам с учетом специфики применения конкретных информационно-телекоммуникационных средств.

Таким образом, анализ средств противодействия компьютерным атакам показывает, что в них используется комплексный подход к обнаружению признаков атак на основе обработки данных от системы датчиков, но при этом не реализованы взаимосвязанные со СПКА функции сохранения устойчивости функционирования КВИС в условиях воздействия атак.

6 ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ НА КРИТИЧЕСКИ ВАЖНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Стратегия противодействия компьютерным атакам на КВИС представлена на рисунке 13. Она позволяет осуществлять многоуровневое противодействие компьютерным атакам по четырем уровням:

1. Предупреждение атак – определение потенциальных угроз компьютерных атак на основе аналитической информации и мониторинга КВИС.
2. Обнаружение атак – выявление признаков атак в информации, программах КВИС и в циркулирующих потоках данных.
3. Анализ атак – распознавание и каталогизация компьютерных атак в соответствии с принятой их классификацией.
4. Активное противодействие атакам и обеспечение устойчивости функционирования КВИС – блокирование или нейтрализация деструктивных воздействий.

На указанных уровнях противодействия компьютерным атакам на КВИС осуществляется определение признаков атак в соответствии с заданным алгоритмом распознавания СПКА. Алгоритм позволяет провести анализ априорной информации о потенциальных угрозах компьютерных атак, сбор сведений от датчиков, оценку полученной апостериорной информации и выработать системное решение по обнаружению этих атак на соответствующих уровнях иерархии КВИС.

Особенностью комплексного противодействия компьютерным атакам при сохранении устойчивости функционирования КВИС является формирование множества признаков атак не только по цифровым сигналам датчиков, но и по аналитической информации признаков подготовки атак нарушителем, фактам обнаружения аномалий в КВИС и нарушений функций системы по данным системных журналов СПКА и средств мониторинга.

Достоверность распознавания признаков компьютерных атак является необходимым условием для работы СПКА.

Полнота функций СПКА для противодействия известным и неизвестным атакам является достаточным условием для достижения эффективности применения СПКА.

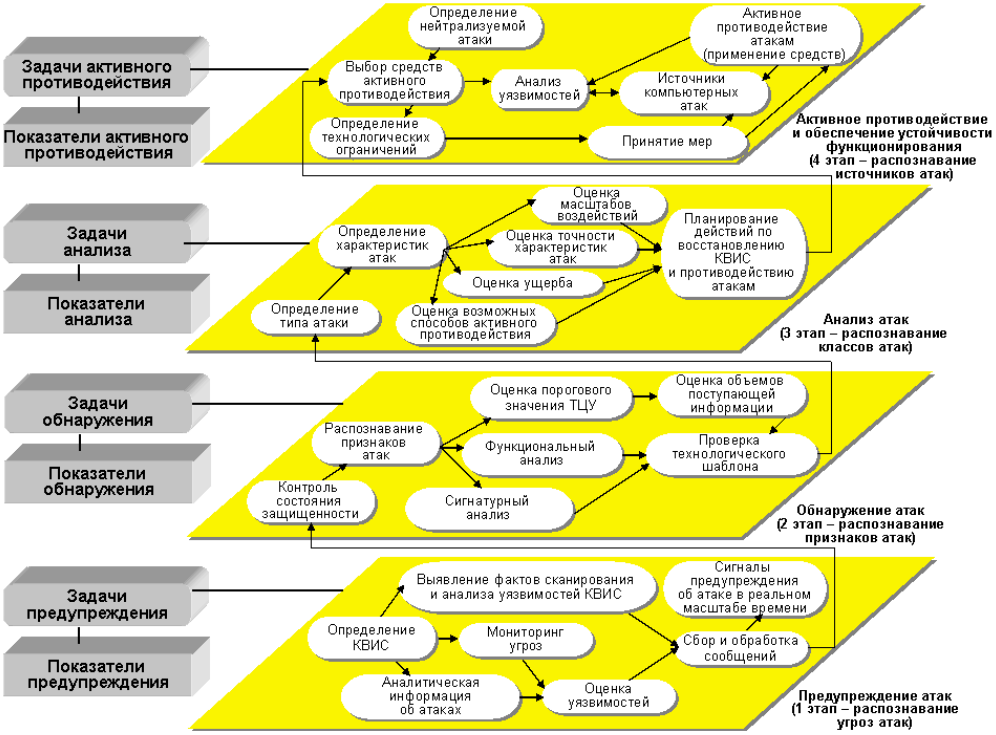


Рисунок 13 – Стратегия противодействия компьютерным атакам на КВИС

Стратегия противодействия компьютерным атакам на КВИС состоит в следующем:

1. В формировании единого пространства параметров противодействия компьютерным атакам (параметров состояния КВИС и СЗИ, признаков атак, параметров СПКА и устойчивости функционирования КВИС).

2. В учете разнородных факторов противодействия компьютерным атакам на КВИС:

– в выявлении (распознавании в структуре параметров информационно-вычислительного процесса) известных и неизвестных атак;

– необходимости выполнения заданного ТЦУ;

– в сохранении устойчивости функционирования КВИС в условиях воздействия компьютерных атак.

3. Разработке алгоритма противодействия компьютерным атакам.

4. Разработке причинно-следственных математических соотношений, определяющих конкретную логику и ограничения на решение проблемы противодействия компьютерным атакам.

5. Разработке шкалы показателей противодействия компьютерным атакам.

6. Разработке обобщенного метода противодействия компьютерным атакам на основе теории распознавания образов.

7. Реализации активного противодействия атакам и обеспечении устойчивости функционирования КВИС.

Под технологией противодействия компьютерным атакам на КВИС понимается совокупность взаимосвязанных процедур прогнозирования сценариев и классификации компьютерных атак нарушителя, анализа уязвимых мест и технологических циклов управления КВИС, применения методов и моделей противодействия атакам и оценки устойчивости функционирования КВИС в условиях воздействия компьютерных атак.

Технология организации противодействия компьютерным атакам на КВИС представлена на рисунке 14 и включает в свой состав:

1. Оценку нарушителя, которая предполагает работы по прогнозированию возможных сценариев компьютерных атак нарушителя и классификацию компьютерных атак.

2. Идентификацию состояния КВИС, основанную на анализе потенциальных уязвимых мест и анализе состояний компонентов КВИС при выполнении ТЦУ.

3. Разработку методов и моделей противодействия компьютерным атакам: предупреждения, обнаружения, анализа компьютерных атак и активного противодействия атакам.

4. Оценку устойчивости функционирования КВИС, заключающуюся в получении необходимой совокупности параметров структурно-функционального построения СПКА и КВИС для сохранения устойчивости функционирования в условиях воздействия компьютерных атак.

Отличительной особенностью технологии противодействия компьютерным атакам на КВИС является то, что достоверность получаемых с её помощью результатов и качество применения методов, моделей и средств противодействия атакам обеспечивается гибким сочетанием математического, имитационного и натурного моделирования и априорной экспериментальной оценки эффективности средств противодействия компьютерным атакам на стендовом полигоне.

Применение технологии противодействия компьютерным атакам предполагает достаточно сложный динамический мониторинг и анализ состояний КВИС, трафика входных и выходных данных, раннего выявления признаков атак как исходя из сигнатурного анализа программного и информационного обеспечения, так и по

обнаружению аномального поведения системы и отклонений при выполнении технологических циклов управления.

Для эффективного применения технологии противодействия компьютерным атакам на КВИС и минимизации вычислительных ресурсов при её применении необходимо разработать языки описания компьютерных атак и уязвимостей, типовые шаблоны (паспорта) для технического описания характеристик атак и технологических циклов управления в КВИС, а также защищенный протокол передачи данных между элементами средств противодействия компьютерным атакам.

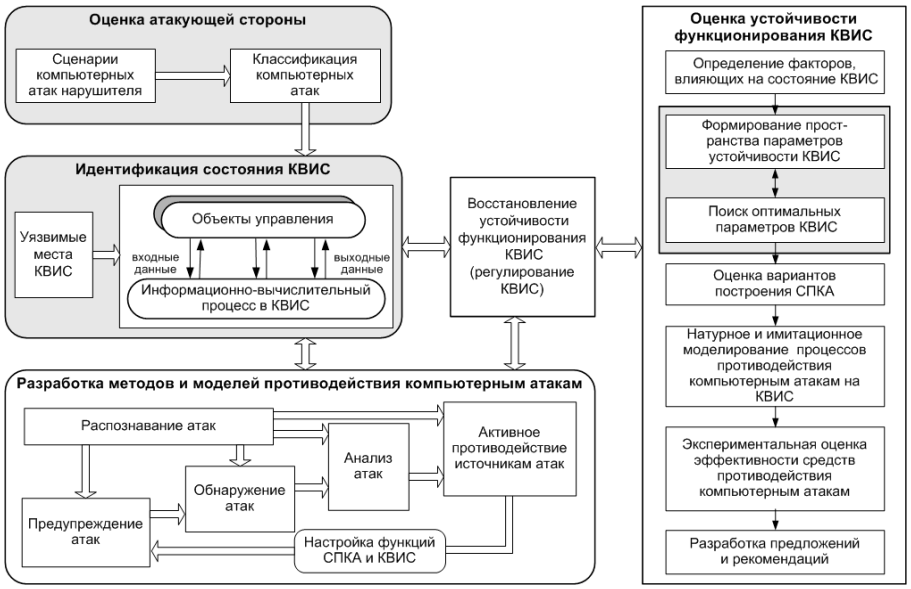


Рисунок 14 – Технология организации противодействия компьютерным атакам на КВИС

На рисунке 15 представлен алгоритм противодействия компьютерным атакам на основе многодатчиковых систем.

Первоначальным источником информации для выполнения мониторинга состояния устойчивости функционирования КВИС и применения средств противодействия компьютерным атакам являются интеллектуальные датчики (программные или программно-аппаратные средства) выявления (регистрации) атак и сбора информации о них. Датчики включаются в общее и специальное программное обеспечение, системы управления базами данных и базы данных, цифровое коммуникационное оборудование КВИС, средства защиты информации и сами средства противодействия.

Сбор, обработку и выявление признаков атак от совокупности датчиков осуществляют их управляющие программы. Они производят протоколирование событий при использовании коммуникационных ресурсов (контроль и ведение протокола событий в сети, мониторинг сетевого трафика, сбор статистики по загрузке, оперативности и надежности сети КВИС) и осуществлении доступа к информационным ресурсам (разграничение и контроль доступа к данным, резервирование эталонных данных, выявление ложных данных, сохранение целостности структур данных).

Управляющие программы датчиков производят протоколирование событий при использовании коммуникационных ресурсов (контроль и ведение протокола событий в сети, мониторинг сетевого трафика, сбор статистики по загрузке, оперативности и надежности сети КВИС) и доступе к информационным ресурсам (разграничение и контроль доступа к данным, резервирование эталонных данных, выявление ложных данных, сохранение целостности структур данных).

Управление процессами противодействия компьютерным атакам реализуется следующим образом:

- запись данных мониторинга в сервер баз данных мониторинга состояния устойчивости функционирования и безопасности КВИС;
- визуализация результатов работы управляющих программ датчиков с использованием 2D-моделей (двумерного представления данных, как правило, в табличной форме), 3D-моделей (трехмерных моделей компьютерной графики), геоинформационных систем (ГИС), на которых наносятся местоположение компонентов КВИС и динамические характеристики выполнения ТЦУ и результатов противодействия атакам с привязкой к электронной карте;
- анализ ситуации по воздействию атак по сравнительному анализу фактической информации об атаках с базами данных сигнатур атак, функционального анализа и анализа аномалий;
- принятие в автоматизированном режиме решений оператором по корректировке функций управления СЗИ, повышению уровня защищенности и устойчивости функционирования КВИС;
- выбор параметров противодействия компьютерным атакам и запуск средств активного противодействия источникам атак.

Новизной предлагаемого алгоритма является то, что разработаны интеллектуальные датчики средств противодействия компьютерным атакам, которые

используются как для выявления атак, так и реализации активного противодействия по их нейтрализации и блокированию источника компьютерной атаки.

Рисунок 15 – Алгоритм противодействия компьютерным атакам на основе многодатчиковых систем

На рисунке 16 приведены возможные средства противодействия и реализация способов противодействия компьютерным атакам на КВИС.

В интересах эффективной реализации экспериментальных образцов средств противодействия атакам, применения их в режимах близких к реальному масштабу времени необходимо образовать и использовать стендовые полигоны, которые должны позволять:

- производить сбор и хранение аналитической информации о сценариях, способах применения и характеристиках компьютерных атак;
- вести оперативную оценку средств реализации компьютерных атак нарушителя,
- проводить мероприятия по анализу и устранению уязвимостей для проникновения в структуру КВИС,
- предотвращать воздействия атак средствами противодействия в автоматизированном режиме,
- формировать план противодействия атакам и в соответствии с ним нейтрализовывать их,
- оперативно устранять последствия воздействия атак,
- готовить предложения по созданию системы мониторинга угроз

компьютерных атак на КВИС и оперативного противодействия этим угрозам.

Отличительными факторами предлагаемых способов противодействия компьютерным атакам (рисунок 16) от существующих средств СЗИ НСД, защиты удаленного доступа к сети, других средств обнаружения атак являются следующие:

1. Возможность выявления воздействий, скрытых в сетевом трафике КВИС и изменяющих порядок выполнения программ, информационно-логического взаимодействия абонентов, доступа к данным и программам, режимы работы средств защиты информации.

2. Пассивное противодействие атакам – предупреждение об уязвимостях КВИС при установке средств СПКА, оповещение о применении средств противодействия, туннелирование и разработка дополнительных стеков протоколов передачи данных, проверка подозрительных событий нарушения устойчивости функционирования КВИС, реконфигурация и перезапуск КВИС и СЗИ НСД, ограничение доступных сервисных функций программ.

3. Активное противодействие атакам – блокирование источников атак и средств сканирования уязвимостей; перенаправление атак на ложные информационные объекты; использование ложных функций, обманных систем; противодействие выводу из строя и восстановление работоспособности КВИС; управление противодействием атакам на уровнях эталонной модели взаимодействия открытых систем; противодействие атакам на семи рубежах СПКА [Каталит].

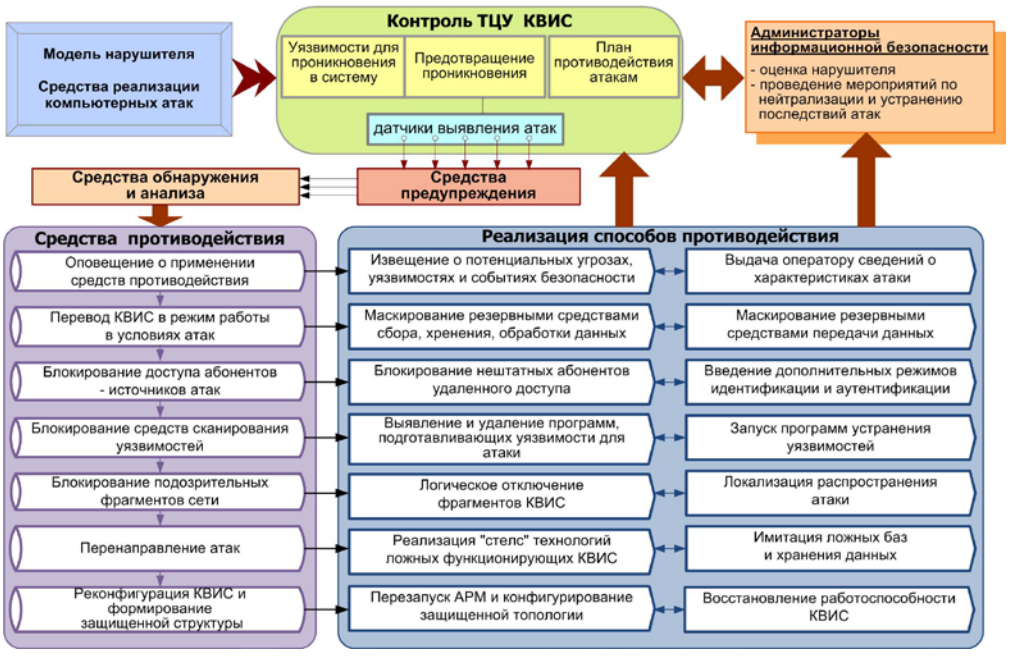


Рисунок 16 – Реализация способов противодействия компьютерным атакам на КВИС

На рисунке 17 приведена схема применения технологии противодействия компьютерным атакам на КВИС [37, 54, 55]. Особенностью предложенной схемы применения технологии противодействия компьютерным атакам на КВИС является то, что она объединяет два контура: первый контур применения средств противодействия компьютерным атакам и второй контур оперативного предупреждения о фактах воздействия компьютерных атак на КВИС.

Два контура схемы (рисунок 17) должны быть разделены, и не иметь общих каналов связи и интерфейсов. Так как объединение этих двух контуров приводит к дополнительному внесению уязвимостей в систему, функционирующую в режиме близком к реальному масштабу времени выполнения ТЦУ.

Первый контур исполняет роль противодействия компьютерным атакам средствами СПКА, сбора данных о результатах работы этих средств и о результатах мониторинга КВИС непосредственно на пунктах и центрах управления.

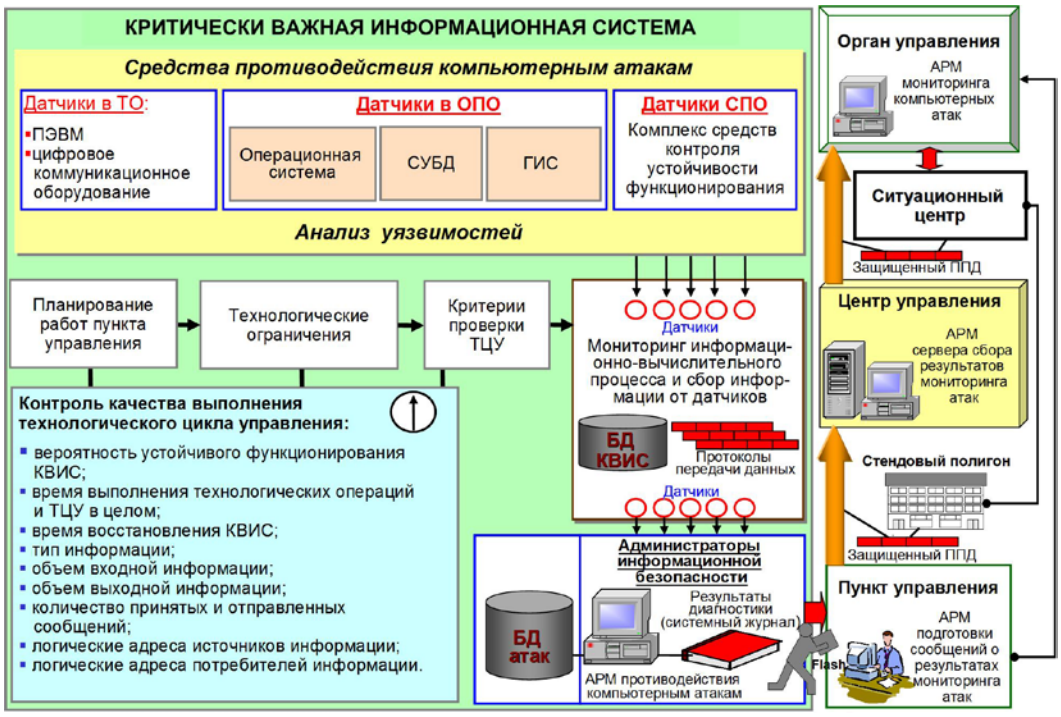


Рисунок 17 – Применение технологии противодействия компьютерным атакам на КВИС

Второй контур предназначен для оперативного оповещения органов управления о фактах воздействия компьютерных атак, принятия решений о состоянии устойчивости функционирования КВИС и мерах по противодействию массированным компьютерным атакам нарушителя.

Временная диаграмма противодействия компьютерным атакам на КВИС представлена на рисунке 18.

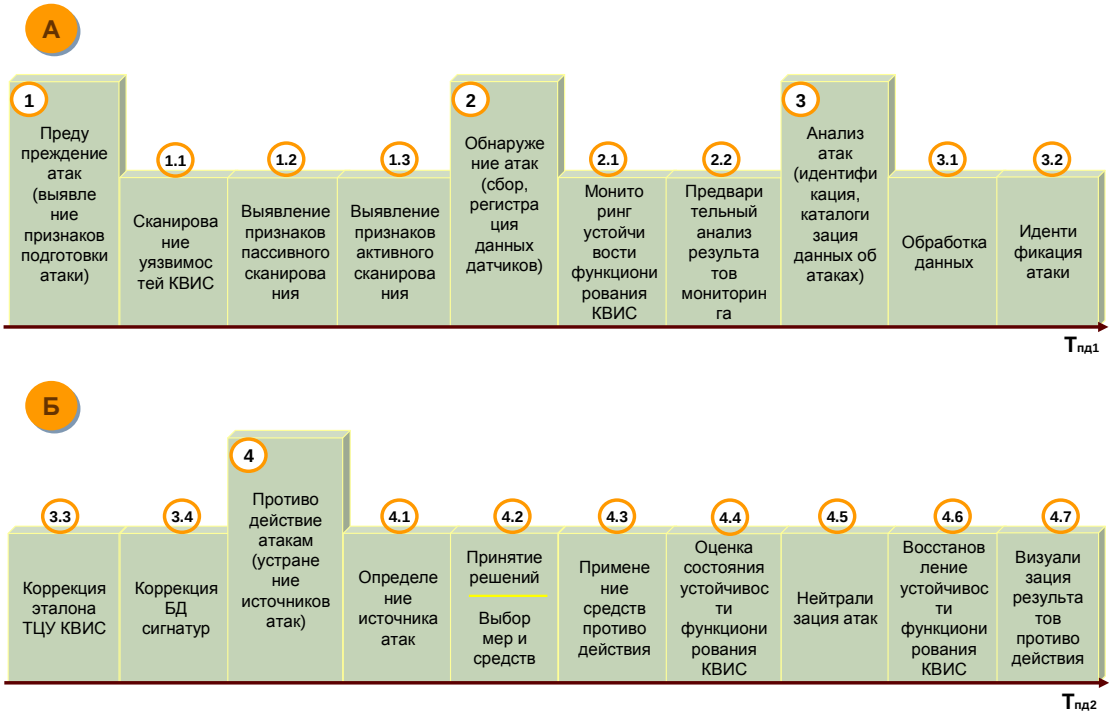


Рисунок 18 – Временная диаграмма противодействия компьютерным атакам на КВИС

Следует отметить, что методы предупреждения, обнаружения, анализа и активного противодействия им во многом зависят от используемого в КВИС принципа противодействия атакам. Предложенный принцип противодействия атакам на КВИС «запрещено все, что не разрешено» позволяет достаточно эффективно определять как известные, так и неизвестные атаки и реализовывать противодействие с требуемым значением вероятности обеспечения устойчивости функционирования КВИС.

7 АЛГОРИТМ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ НА КРИТИЧЕСКИ ВАЖНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Алгоритм противодействия компьютерным атакам на КВИС представляет собой взаимосвязанную иерархическую схему поддержки принятия решений по оценке потенциальных опасностей реализации компьютерных атак, выявлению уязвимостей типовых компонентов КВИС, признаков атак и декомпозиции опасностей их воздействия на компоненты КВИС, противодействию компьютерным атакам и восстановлению устойчивости функционирования компонентов КВИС. При формировании алгоритма противодействия компьютерным атакам использованы материалы по защите программного обеспечения и моделирования угроз нарушения информационной безопасности [1, 4, 5-10, 21, 22, 24, 28-31, 33, 36-46, 50-56, 58-60, 62-64, 68-70].

На рисунке 19 представлен алгоритм противодействия компьютерным атакам на КВИС, который включает в свой состав пять этапов:

1. Формализация опасностей реализации угрозы воздействия компьютерных атак путем формирования множества параметров сценария атак H_{a1} и средств реализации атак Y_{ai}.
2. Выделение типовых компонентов КВИС S_{ij} и соответствующих им уязвимостей $\xi_{уязij}$ в соответствии с таблицей 5.
3. Проведение декомпозиции опасностей по компонентам КВИС (элементам типовых компонентов) и оценка вероятности опасности воздействия атаки на каждый компонент P_{ij}^{n} согласно требованиям таблицы 5.
4. Разработка (выбор) и оценка оперативных возможностей средств противодействия компьютерным атакам $Z_{nдij}$.
5. Анализ устойчивости функционирования КВИС в условиях опасностей воздействия атак и оценка критических параметров $K_{вij}$ средств восстановления устойчивости функционирования КВИС.

Разработка алгоритма противодействия компьютерным атакам (рисунок 19) требует более детального рассмотрения особенностей компонентов КВИС (и соответствующих уязвимостей), которые могут быть подвержены воздействиям атак с целью нарушения конфиденциальности, целостности, доступности информации и

устойчивости функционирования КВИС. Классификация опасностей воздействия компьютерных атак на компоненты КВИС представлена в таблице 6.

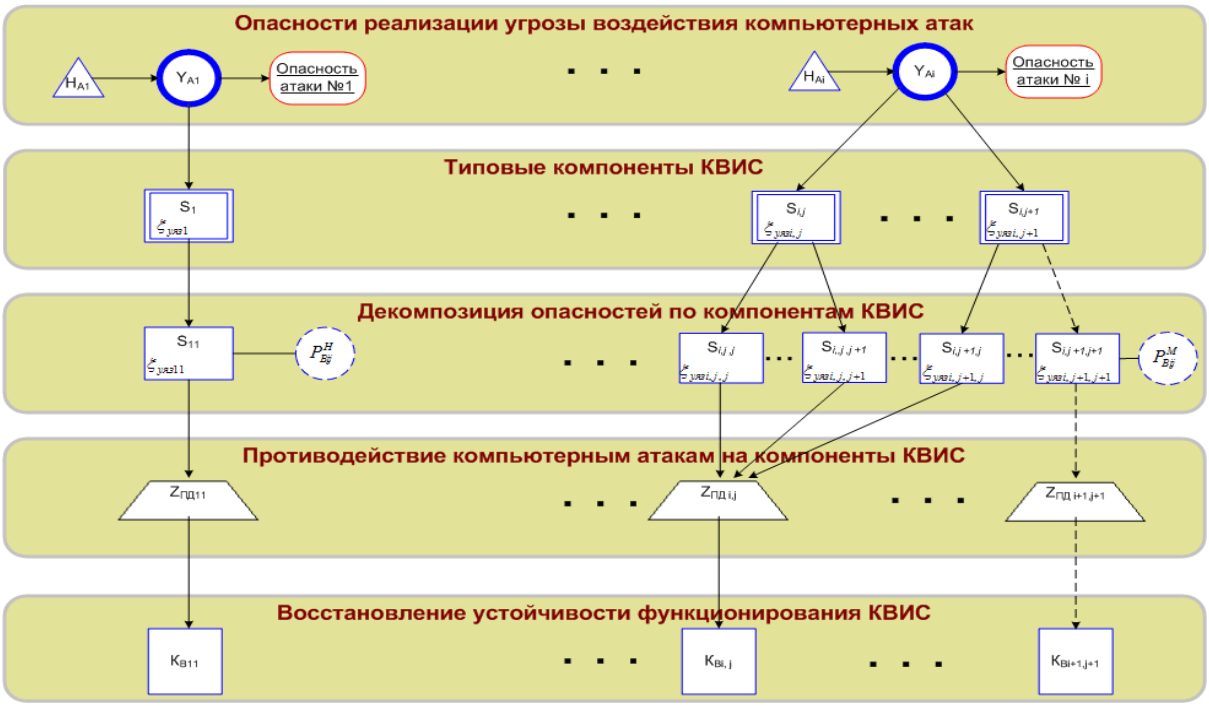
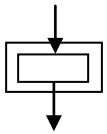
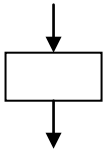
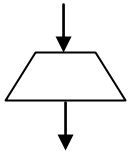
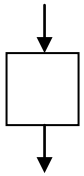


Рисунок 19 – Алгоритм противодействия компьютерным атакам на КВИС

Таблица 5 – Условные обозначения и описание базовых атрибутов алгоритма противодействия компьютерным атакам на КВИС

Условные обозначения	Описание базовых атрибутов					
	Сценарии компьютерных атак по нарушению устойчивости функционирования КВИС					
 Опасности атак	«Ложная информация»		«Функциональное поражение»		«Разрыв соединения»	
 Типовой компонент КВИС и его уязвимость	Пункт управления (ПУ)	Центр управления (ЦУ)	Сектор управления (СУ)	Подсистема визуализации	Средства защиты информации	
 Элемент типового компонента КВИС	АРМ сервера сбора данных пункта (ССД-П)	АРМ сервера сбора данных центра (ССД-Ц)	АРМ сервера электронной почты - клиента (СЭП-К)	АРМ сервера электронной почты - сервера (СЭП-С)	АРМ визуализации	АРМ администратора

Условные обозначения	Описание базовых атрибутов				
 Средства противодействия	АРМ мониторинга устойчивости функционирования КВИС	АРМ предупреждения, обнаружения анализа и атак	АРМ активного противодействия атакам	АРМ администрирования средств предупреждения, обнаружения, анализа атак и активного противодействия атакам	АРМ визуализации процессов предупреждения, обнаружения, анализа атак и активного противодействия атакам
 Средства восстановления устойчивости функционирования	Средства контроля информационно-вычислительного процесса и восстановления программ за время ТЦУ	Средства обеспечения выполнения идентичных функций различными способами	Средства контроля состояния устойчивости функционирования КВИС	Средства контроля соответствия входных и выходных данных по допустимым значениям	Средств диагностики нарушений и сбора статистики о работе КВИС
	Средства контрольного тестирования, анализа сбоев по суммированию кодов, контроля значений параметров по превышению количества прерываний и длительности расчетов		Средства динамического распределения ресурсов по алгоритму администрирования	Средства рестарта КВИС	Средства архивирования эталонных копий

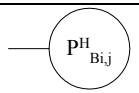
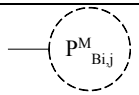
Условные обозначения	Описание базовых атрибутов
 Наиболее вероятное событие	Означает, что вероятность опасности воздействия атаки на компонент КВИС $S_{i,j}$ и уязвимость $\xi_{уяз\ i,j}$ высокая - $P_B^H \geq 0.6$
 Менее вероятное событие	Означает, что вероятность опасности воздействия атаки не высокая (маловероятное событие) - $P_B^M \leq 0.4$

Таблица 6 – Классификация опасностей воздействия компьютерных атак на компоненты КВИС

№ п/п	Компоненты КВИС ($S_{i,j}$) имеющие уязвимости ($\xi_{уяз\ i,j}$)	Цели воздействия компьютерных атак				
		Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности	Нарушение штатного режима функционирования	Функциональные признаки реализации воздействий компьютерных атак
1	Техническое обеспечение и цифровое коммуникационное оборудование	Хищение носителей информации. Несанкционированное подключение. Несанкциониров	Несанкционированная модификация. Несанкционированное изменение режимов маршрутизации	Нарушение полномочий доступа к устройствам. Нарушение взаимодействия между модулями	Нарушение регламентов работы. Преднамеренная перезагрузка. Отказ и вывод из строя элементов	Блокирование ИВП в оперативной памяти, процессоре и других аппаратных средствах. Блокирование удаленного доступа в ЦКО. Повреждение накопителей

№ п/п	Компоненты КВИС ($S_{i,j}$) имеющие уязвимости ($\xi_{уяз\ i,j}$)	Цели воздействия компьютерных атак				
		Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности	Нарушение штатного режима функционирования	Функциональные признаки реализации воздействий компьютерных атак
		анное использование вычислительных ресурсов.	и коммутации.	и со смежными средствами.	КВИС. Перепрограммирование коммуникационного оборудования.	информации и программируемых элементов компьютерного оборудования путем преднамеренного искажения режимов управления. Появление избыточных маршрутов коммутации потоков данных. Несанкционированный перезапуск (переключение) ПЭВМ.
2	ПО (операционная система, специальное программное обеспечение, система управления базами данных)	Несанкционированное копирование. Несанкционированное получение документации. Несанкционированное получение результатов выполнения	Внедрение программных закладок (оперативно-технических позиций). Внедрение дополнительных (избыточных) программ к	Перехват прерываний. Искажение сетевых протоколов. Искажение интерфейсов с системами управления базами данных.	Подмена программ. Искажение программ. Удаление программ. Имитация ненадежной работы программ. Нарушение	Самостоятельная инициализация избыточных программ по определенным условиям. Появление саморазмножающихся программ. Проявление недекларированных функций СПО.

№ п/п	Компоненты КВИС ($S_{i,j}$) имеющие уязвимости ($\xi_{уяз\ i,j}$)	Цели воздействия компьютерных атак				
		Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности	Нарушение штатного режима функционирования	Функциональные признаки реализации воздействий компьютерных атак
		СПО при выполнении ТЦУ. Использование недекларированных возможностей.	штатно поставляемым программам. Искажение полномочий доступа в операционной системе к доменам, файлам, программам.	Искажение интерфейсов со специальным ПО. Несанкционированное установление полномочий доступа к программным данным.	технологии выполнения информационно-вычислительного процесса.	Несанкционированное назначение привилегий программам. Несанкционированный мониторинг трафика сети. Наличие внешнего управления СПО. Повреждение программ. Имитирующие нарушения в работе ПО.
3	Структуры баз данных (измерительной информации и результатов вычислений)	Копирование данных. Хищение данных. Перехват данных. Сокрытие информации.	Искажение данных. Модификация данных. Запись избыточных данных.	Искажение структур. Перехват информационных потоков.	Удаление данных. Превышение допустимой информационной нагрузки. Имитация избыточных данных.	Внедрение непредусмотренных форм обмена данными абонентов КВИС. Попытки поиска и выдачи остаточной информации. Нарушение технологии информационного взаимодействия абонентов и доступа к данным. Подмена информации. Повреждение логической

№ п/п	Компоненты КВИС ($S_{i,j}$) имеющие уязвимости ($\xi_{уяз\ i,j}$)	Цели воздействия компьютерных атак				
		Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности	Нарушение штатного режима функционирования	Функциональные признаки реализации воздействий компьютерных атак
						структуры и потеря значительных объемов данных. Несанкционированное формирование носителей информации.
4	Операторы КВИС	Разглашение сведений. Передача сведений.	Превышение полномочий санкционированного оператора или подмена администратора.	Удаление санкционированных пользователей. Информационная маскировка под других операторов.	Искажение параметров доступа операторов. «Отказ в обслуживании» или логическое отключение оператора.	Скрытное проникновение к ресурсам КВИС. Логическая подмена оператора. Попытки подбора (подмены) параметров идентификации и аутентификации. Информационно-психологическое воздействие на оператора по каналу «оператор - ЭВМ».

Для применения алгоритма противодействия компьютерным атакам необходимо в соответствии с таблицами 5 и 6 классифицировать атаки и провести взаимоувязанную декомпозицию опасностей воздействия атак по компонентам КВИС.

Анализ сценариев и опасностей воздействия атак, детализация КВИС, средств противодействия атакам и устойчивости функционирования КВИС осуществляется по типовой иерархической структуре рисунка 19 сверху вниз. Каждому базовому атрибуту алгоритма противодействия компьютерным атакам соответствует реальный процесс применения КВИС. Атрибуты алгоритма противодействия компьютерным атакам по сути своей создают основу для диагностики состояния устойчивости функционирования КВИС в условиях воздействия атак, наличия уязвимых мест каждого элемента типового компонента и принятия решений по противодействию опасности воздействия атак на КВИС. Сплошными линиями на рисунке 19 обозначаются наиболее вероятные сценарии воздействия атак, а менее вероятные события реализации атак и соответствующие им вероятности обозначаются пунктирными линиями.

Специфические свойства атак, которые необходимо описать в комментариях к алгоритму противодействия компьютерным атакам на КВИС, описываются с использованием таблицы 6.

Оценка риска опасности воздействия атак на компоненты КВИС осуществляется по максимальному значению вероятности опасности воздействия атаки и соответствующим им уровням угроз воздействия атак в соответствии с методикой оценки ущерба от воздействия компьютерных атак. Общая оценка риска опасности воздействия атак на КВИС равна среднему значению оценок компонент КВИС. Описание методов и средств противодействия компьютерным атакам на КВИС $Z_{пдij}$ при разработке алгоритма противодействия атакам осуществляется исходя из методов, моделей и алгоритмов противодействия атакам путем адаптации их к конкретным условиям и особенностям применения.

Алгоритм противодействия компьютерным атакам, сформированный для конкретного КВИС по алгоритму рисунка 19 и таблицам 5, 6 позволяет:

- априорно на ранних стадиях создания КВИС промоделировать внутренние и внешние угрозы воздействия атак с привязкой к типовым компонентам КВИС;
- определить какими средствами будет осуществляться противодействие атакам и защита информации, как они будут взаимодействовать;
- установить как, в случае реализации атак, будет осуществляться

восстановление устойчивости функционирования системы.

Использование алгоритма противодействия компьютерным атакам при экспериментальной оценке устойчивости функционирования КВИС на стендовом полигоне в процессе предварительных и приемо-сдаточных испытаний дает возможность:

- прогнозирования сценариев возможных действий нарушителя по осуществлению компьютерных атак на КВИС,
- выявления уязвимостей КВИС и ошибок проектирования и разработки программного и информационного обеспечения,
- подготовки технических решений по выбору средств противодействия атакам и обеспечения устойчивости функционирования КВИС при выполнении ТЦУ.

Особую практическую значимость алгоритм противодействия компьютерным атакам имеет для декомпозиции структуры специального программного обеспечения КВИС и системного анализа опасностей воздействия на него в виде унифицированных структурных диаграмм, выполненных по условным обозначениям таблицы 6.

Таким образом, разработан алгоритм противодействия компьютерным атакам, позволяющий на основе типовых условных обозначений и базовых атрибутов дать взаимосвязанное описание опасностей реализации компьютерных атак и уязвимостей типовых компонентов КВИС, декомпозировать опасности воздействия атак по компонентам КВИС, выбрать методы, модели и средства противодействия компьютерным атакам на КВИС и восстановления устойчивости функционирования.

8 Паспорт компьютерных атак на критически важные информационные системы

С целью описания динамики событий и формализации параметров о внедрении и воздействии компьютерных атак, устойчивости функционирования КВИС, эффективности применения средств противодействия компьютерным атакам и сведений о нарушителях предлагается при сборе и анализе данных об атаке использовать паспорт атаки, включающий в свой состав пять вложенных таблиц (таблицы 7 – 11).

В таблице 7 (технологический паспорт компьютерной атаки) приведена общая характеристика атаки (условное наименование, идентификационный номер, тип атаки) и параметры КВИС, на который она воздействует. Эта таблица является первоначальной для последовательного заполнения таблиц 8 – 11 и является базовым докладом при оповещении об компьютерных атаках нарушителя.

Данные, помещенные в таблице 8, дают возможность описать параметры КВИС, из которых детально определяется уязвимое место объекта, оценивается опасность срыва технологических операций, условия проведения и источник атаки. Ключевыми параметрами данной таблицы следует считать: тип протокола передачи данных, IP–адрес объекта атаки, уязвимые места, нарушенные технологические операции.

Сведения, приведенные в таблице 9, позволяют сформировать детальное описание временных и технологических параметров компьютерной атаки и получить предварительную информацию об ущербе от реализации этой атаки.

В таблице 10 представлено описание параметров противодействия, которые заключаются в количественной и качественной оценке принятых мер и использованных средств противодействия компьютерной атаке.

Данные таблицы 11 (описание параметров нарушителей) являются исходными данными для принятия решения, обобщенной оценки обстановки и данных о нарушителе.

Унифицированный формат сообщения об обнаружении компьютерной атаки (например, СПКА Snort [Snort]) рассмотрен на рисунке 20.

1.	2.	3.	4.	5.
uiq	Version UFSOA	CreateDateTime	Alert	Analyzer
Уникальный номер сообщения	Версия формата сообщения об обнаружении компьютерной атаки	Дата/время создания сообщения	Сообщение о компьютерной атаке: - дата/время обнаружения; - описание атаки; - тип атак; - идентификатор; - приоритет.	Компонент СПКА (отправитель сообщения о компьютерной атаке): - IP адрес; - id СПКА; - id модуля анализа; - наименование.

6.	7.	8.	9.
SourceAtack	TargetAtack	Assessment	Recomendation
Предполагаемый источник компьютерной атаки: - IP атакующего (источника компьютерной атаки).	Предполагаемая цель компьютерной атаки: - IP адрес цели; - уровень объекта в сети (компонент КВИС); - id объекта; - тип протокола; - наименование.	Оценка события и прогноз	Рекомендации по устранению уязвимости

Рисунок 20 – Унифицированный формат сообщения об обнаружении компьютерной атаки

Таблица 7 – Технологический паспорт компьютерной атаки

№ п/п	Условное наименование	Идентификационный номер	Тип атаки	Параметры КВИС	Параметры атаки	Параметры противодействия	Параметры нарушителя	Краткое описание инцидента
1	2	3	4	5	6	7	8	9
1	«Цунами»	2008-10-07-014 ПУ {год} {месяц} {дата} {условное наименование акции}	«Отказ в выдаче информации»	**Пример заполнения** По табл. 3.5	По табл. 3.6	По табл. 3.7	По табл. 3.8	Текст доклада об инциденте

Таблица 8 – Описание параметров КВИС

Наименование КВИС	Тип СВТ	Программное, информационное обеспечение	Параметры эксплуатации (год эксплуатации, разработки)	Пропускная способность каналов связи (Кб/с)	Тип протокола передачи данных	IP-адрес объекта атаки	Какое уязвимое место использовано	Какие технологические операции нарушены	Принадлежность КВИС
1	2	3	4	5	6	7	8	9	10
Пункт управления «Углич»	ПЭВМ Pentium IV	ОС Windows NT, СУБД Oracle,	**Пример заполнения** Штатная эксплуатация с 2008 г. Опытная эксплуатация элементов с 2006 г.	64 Кб/с	TCP/IP	193.2 …	ЛВС	Сбор данных	Элемент объекта

Таблица 9 – Описание параметров компьютерной атаки

$t_н$, час, мин.	$t_{ок}$, час, мин	t_g, час, мин	IP-адрес	Объект атаки	Ущерб	Характеристика нарушений (искажение информации, ПО и т.п)
1	2	3	4	5	6	7
21.00	21.30	30	192 ПУ-7	**Пример** Сервер сбора данных	**заполнения** Не обеспечен прием данных	Искажен массив информации в БД, наличие возможности НСД через удаленный доступ по адресу 193.2…

Таблица 10 – Описание параметров противодействия

$t_{н\ пр}$, час, мин	$t_{ок\ пр}$, час, мин	$t_{g\ пр}$, час, мин	Тип средства противодействия	Результат противодействия	Принятие мер	Оповеще-ние
1	2	3	4	5	6	7
21.40	22.00	20	**Пример** СПКА	**заполнения** Логически устранен источник воздействия	Реконфигурация межсетевого экрана, настройка датчиков СПКА, перезапуск программ, настройка администраторов ЛВС и СПКА ПУ, смена схемы адресации	ПУ, ЦУ

Таблица 11 – Описание параметров нарушителей

Источник атаки	Страна	Нарушитель	Средства реализации компьютерных атак	Оценка обстановки	Примечания
1	2	3	4	5	6
Удаленный объект	Россия	**Пример** Залегендирован под	**заполнения** Средства сканирования, поиска	Признаки массированной	

нарушителя		штатного оператора	уязвимостей и анализа сетей	компьютерной атаки	

Таким образом, разработанный паспорт компьютерных атак на КВИС является информационной основой для сбора, регистрации и каталогизации сведений об атаках и применению адекватных средств противодействия компьютерным атакам на КВИС.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Понятие и задачи типовых КВИС. Технологические циклы управления в КВИС.
2. Условия воздействия компьютерных атак. Графы состояний и событий реализации компьютерных атак.
3. Способы реализации и обобщенный сценарий компьютерных атак.
4. Классификация компьютерных атак.
5. Обеспечение устойчивости функционирования и защищенности КВИС.
6. Анализ средств противодействия компьютерным атакам.
7. Технология противодействия компьютерным атакам на КВИС. Схема применения технологии в реальных системах. Особенности схемы. Назначение контуров схемы.
8. Алгоритм противодействия компьютерным атакам на основе многодатчиковых систем.
9. Реализация способов противодействия компьютерным атакам на КВИС.
10. Паспорт компьютерных атак на критически важные информационные системы. Назначение и состав.

Список литературы

1. Актуальные вопросы выявления сетевых атак. Александр Астахов. CISA. Информационный бюллетень Jet Info, № 3 (106) – Москва, 2002.
2. Бескоровайный М.М., Костогрызов А.И., Львов В.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем «КОК»: Руководство системного аналитика. – М., Вооружение. Политика. Конверсия. 2001. – 303 с., 2-е издание.
3. Бурков В.Н., Грацианский Е.В., Дзюбко С.И., Щепкин А.В. Модели и механизмы управления безопасностью. Серия «Безопасность». – СИНТЕГ, 2001, 160 с.
4. Вакка Дж. Безопасность интранет: Пер. с англ. – М.: ООО «Бук Медиа Паблишер», 1998.– 496 с.
5. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. – М: МИФИ, 1999. – 96 с.
6. Галатенко В.А. Информационная безопасность – обзор основных положений. Информационный бюллетень Jet Info, части № 1-3. – Москва, 1998.
7. Гаценко О.Ю. Защита информации. Основы организационного управления. СПб.: Изд. Дом «Сентябрь». 2001. 228 с.
8. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2 – х кн. Книга 1.– М.: Энергоатомиздат, 1994. – 400 с.
9. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2–х кн., Книга 2. – М.: Энергоатомиздат, 1994.– 176 с.
10. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: Издательство «Инкомбук», 1997. – 537 с.
11. Гостехкомиссия России. Сборник руководящих документов по защите информации от несанкционированного доступа. СИП РИА. – Москва, 1998.
12. Гостехкомиссия России. РД. Антивирусные средства. Показатели защищенности и требования по защите от вирусов. – Москва, 1998.
13. Гостехкомиссия России. РД. Программное обеспечение автоматизированных систем и средств вычислительной техники. Классификация по уровню гарантированности отсутствия недекларированных возможностей. – Москва,

1998.

14. ГОСТ Р 50922-96. Защита информации. Основные требования и определения.
15. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
16. ГОСТ Р 51275-99. Объекты информатизации. Факторы, воздействующие на информацию.
17. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем базовая эталонная модель. Часть 2. Архитектура защиты информации.
18. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения.
19. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
20. ГОСТ Р ИСО/МЭК 15408-2002. Информационные технологии. Методы и средства обеспечения безопасности. Критерии безопасности информационных технологий.
21. Губенков А.А., Байбурин В.Б. Информационная безопасность/ – М.: ЗАО «Новый издательский дом», 2005. – 128 с.
22. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. Пособие для студ. Высш. учеб. заведений/П.Н. Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.
23. Доктрина информационной безопасности Российской Федерации, Москва, 2000.
24. Домарев В.В. – Безопасность информационных технологий. Методология создания средств защиты. К.: ООО «ТИД «ДС», 2001.
25. Дорф Р. Современные системы управления/Р.Дорф, Р. Бишоп; Пер. с англ. Б.И. Копылова.- М.: Лаборатория Базовых Знаний, 2004. – 832 с.
26. Емельянов Г.В., Стрельцов А.А. Информационная безопасность России. Ч.1. Основные понятия и определения. Учебное пособие/Под общей ред. проф. А.А. Прохожева. – М.: РАГС при Президенте РФ, 1999. – 52 с.
27. Закон РФ «Об информации, информатизации и защите информации».
28. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. – 452 с.
29. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему//под ред. Зегжды Д.П. и Платова В.В. – СПб.: Мир и семья-95, 1997. –

312 с.

30. Зима Б., Молдовян А., Молдовян Н. – Безопасность глобальных сетевых технологий. СПб.: БХВ - Петербург, 2000 – 320 с., ил.
31. К. Дж. Джонс, М. Шема, Б.С. Джонсон Анти-хакер. Средства защиты компьютерных сетей. Справочник профессионала/ Пер. с англ. – М.: СП ЭКОМ, 2003. – 688 с. ил.
32. Калинин В.Н., Резников Б.А., Варакин Е.И. Теория систем и оптимального управления. - Л.: МО СССР, 1987. Ч. 2. – 589 с.
33. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с.
34. Костров Д.В. Рынок систем обнаружения компьютерных атак./Защита информации. Конфидент. 2002. № 6.
35. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации. – М.: Издательский центр «Академия», 2006. 256 с.
36. Липаев В.В. Программно-технологическая безопасность информационных систем. - М.: МИФИ, 1997. – 144 с.
37. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2001.– 624 с.
38. Лукацкий А.В. Мир атак многообразен. http://www.infosec.ru//press/pub_luka.html.
39. Мак-Клар, Стюарт, Скембрей Джоэл, Курц Джордж. Секреты хакеров. Безопасность сетей готовые решения, 3-е издание.: Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 736 с.: ил.
40. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. Пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с.ил.
41. Марк Джозеф Эдварс. Безопасность в Интернете на основе Windows NT/ Пер. с англ. – М.: Издательский отдел «Русская редакция» ТОО «Chanel Trading Ltd» - 199. – 656 с.: ил.
42. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Интернет/Под научной редакцией проф. Зегжды П.Д. – СПб.: «Мир и семья – 95», 1997. - 296 с.
43. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. – 2-е изд., перераб. и доп. – М.: ДМК, 1999. – 336 с.
44. Мельников В.В. Безопасность информации в автоматизированных системах. –

М.: Финансы и статистика, 2003. – 368 с.

45. Новак С., Новак Д., Маклахен Д. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу. М.: Изд. «Лори», 2001.
46. Обеспечение безопасности информации в центрах управления полетами космических аппаратов/Л.М. Ухлинов, М.П. Сычев, В.Ю. Скиба, О.В. Казарин. – М.: Издательство МГТУ им. Н.Э. Баумана, 2000. – 366 с.
47. Олифер В.Г., Олифер Н.А. – Компьютерные сети. СПб.: Питер, 2001 – 672 с., ил.
48. Петров В.А. Системный анализ моделей защиты информации//Безопасность информационных технологий. – 1998. – №1. – С.42-46.
49. Половко А.М., Гуров С.В. Основы теории надежности. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2006. – 704 с.
50. Расторгуев С.П. Введение в формальную теорию информационной войны. М.: Вузовская книга, 2002. – 120 с.
51. Ребров А.И. Кибервойны/Защита информации. Конфидент, 1999. №3.
52. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие – 2-е изд. – М.: Издательско-независимая корпорация «Дашков и К°», 2005. – 336 с.
53. Системный анализ и принятие решений: Словарь-справочник: Учеб. Пособие для вузов/Под ред. В.Н. Волковой, В.Н. Козлова. – М.: Высш. шк., 2004 – 616 с.: ил.
54. Скудис Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: Пер. с англ. – М.: ДМК Пресс, 2003. – 512 с.: ил.
55. Специальная техника и информационная безопасность. Учебник под редакцией В.И. Кирина. Том 1. М.: Академия управления МВД России, 2000, - 783 с.
56. Стенг Д., Мун С. Секреты безопасности сетей. – К.: «Диалектика», 1995. – 544 с.
57. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы/ Под ред. В.А. Садовничего и В.П. Шерстюка. – М., МЦНМО, 2002. – 296 с.
58. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение – М.: СОЛОН-Пресс, 2004, – 192 с.:ил.

59. Теоретические основы информатики и информационная безопасность: Под редакцией докторов технических наук, профессоров В.А. Минаева, В.Н. Саблина. – М.: Радио и связь, 2000. – 468 с.
60. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». – М.: СИНТЕГ, 2000. – 248 с.
61. Хижняк П.Л. Пишем вирус и антивирус. / Под ред. И.М. Овсянниковой.– М.: ИНТО, 1991. – 90 с.
62. Ховард М., Лебланк Д. Защищенный код: Пер. с англ. – 2-е изд., испр. М.: Издательско-торговый дом «Русская Редакция», 2004. – 704 с.:ил.
63. Хогланд, Грег, Мак-Гроу, Гари. Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 400 с.: ил.
64. Хоффман Л.Дж. Современные методы защиты информации. Пер. с англ. - М.: Советское радио, 1980.
65. Холстед М.Х. Начала науки о программах/Пер. с англ. В.М. Юфы. – М.: Финансы и статистика, 1981, 128 с.
66. Чирилло Дж. - Обнаружение хакерских атак.– СПб.:,2003.– 864 с.: ил.
67. Шикин Е.В., Чхартишвили А.Г. Математические методы и модели в управлении: Учеб. пособие. – 3-е изд. – М.: Дело, 2004. – 440 с.
68. Шумский А.А. Системный анализ в защите информации: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности/ А.А. Шумский, А.А. Шелупанов. – М.: Гелиос АРВ, 2005. – 224 с.
69. Щеглов А.Ф. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и Техника, 2004. – 384 с.
70. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006.274 с.: ил.