Оглавление

ПРИНЯТЫЕ СОКРАЩЕНИЯ

АБИ	–	администратор безопасности информации
АВП	–	антивирусная программа
АПК	–	аппаратно-программный комплекс
АРМ	–	автоматизированное рабочее место
БД	–	база данных
КВИС	–	критически важная информационная система
КИ	–	компьютерная игра
ЛВС	–	локальная вычислительная сеть
МЭ	–	межсетевой экран
НСД	–	несанкционированный доступ
ОПО	–	общее программное обеспечение
ОС	–	операционная система
ППД	–	протокол передачи данных
СЗИ	–	средства защиты информации
СОА	–	система обнаружения атак
СПКА	–	средства предупреждения компьютерных атак
СПО	–	специальное программное обеспечение
ССД	–	сервер сбора данных
ССИ	–	сервер сбора измерений
СУБД	–	система управления базами данных
СЭП	–	сервер электронной почты
ТЦУ	–	технологический цикл управления
ЭМ ВОС	–	эталонная модель взаимодействия открытых систем

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины	Определения
Информационный ущерб КВИС	Негативное изменение информационного ресурса, приводящее к невыполнению целевых задач КВИС, нарушению выполнения ТЦУ, принятию неблагоприятных решений, нарушению функций или блокированию управления КВИС и ведущее к увеличению затрат на достижение цели или большим материальным потерям.
Компьютерная игра оценки устойчивости функционирования КВИС в условиях атак	Комплекс программ, предназначенный для моделирования в реальном масштабе времени процессов функционирования системы, принятия решений и оценки эффективности выбранных средств противодействия атакам при различных вариантах игры.
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.
Стендовый полигон	совокупность общего и специального программного, информационного, технического обеспечения аппаратно-программных комплексов (АПК) оценки средств

	противодействия компьютерным атакам в составе замкнутой локальной вычислительной сети (ЛВС) и средств визуализации коллективного пользования
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.
Показатель оценки противодействия компьютерным атакам	Характеристика одного из свойств средств предупреждения, анализа, обнаружения компьютерных атак и активного противодействия компьютерным атакам.
Шкала показателей оценки противодействия компьютерным атакам	Совокупность характеристик свойств средств реализации компьютерных атак, средств противодействия этим атакам и устойчивости функционирования КВИС.
Уровень устойчивости функционирования КВИС	Качественный критерий, характеризующий интегральное свойство КВИС выполнять ТЦУ при воздействии компьютерных атак.

1 МЕТОД НАТУРНОГО И ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ НА КРИТИЧЕСКИ ВАЖНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Метод натурного и имитационного моделирования процессов противодействия компьютерным атакам на критически важные информационные системы (КВИС) разработан для экспериментальной оценки эффективности применения методов, моделей и алгоритмов путем испытаний (тестирования) макетов средств противодействия атакам в условиях близких к реальным на стендовом полигоне.

Применение данного метода направлено на решение следующих задач:

- выявление уязвимых мест в контуре управления КВИС;
- оценка потенциальных возможностей нарушителя по реализации угроз компьютерных атак;
- отладка элементов и функций средств противодействия путем иерархического многоуровневого моделирования;
- агрегированная оценка динамических процессов применения КВИС в защищенном исполнении на основе выделения базовых компонентов (автоматизированных рабочих мест (АРМ) имитатора атак, серверов сбора измерений и электронной почты (ССИ и СЭП), средств предупреждения компьютерных атак (СПКА) и других средств);
- комплексная оценка устойчивости функционирования КВИС в условиях компьютерных атак на основе разработанных методов, моделей и алгоритмов противодействия атакам.

В ходе натурного и имитационного моделирования на стендовом полигоне воспроизводятся реальные процессы применения КВИС и противодействия компьютерным атакам путем осуществления статистических испытаний совместно функционирующих имитатора компьютерных атак, макетов КВИС, и макетов средств противодействия. В качестве основы для разработки метода натурного и имитационного моделирования процессов противодействия компьютерным атакам использована теория моделирования и анализа сложных систем и метод Монте-Карло [3-10, 13, 14, 24, 25, 28, 29, 30, 32].

Метод натурного и имитационного моделирования процессов противодействия компьютерным атакам на КВИС основан на пошаговой стратегии экспериментальной оценки параметров компьютерных атак при воздействии на рубежи КВИС, контроле устойчивости функционирования системы, натурном моделировании и выборе средств противодействия. Этот метод выполняется в виде следующей последовательности шагов:

1. Формализация натурного и имитационного моделирования процессов противодействия компьютерным атакам на КВИС.

2. Разработка моделирующих алгоритмов.

3. Реализация имитационных и натурных моделей на стендовом полигоне в виде совокупности макетов АРМ.

4. Планирование натурного и имитационного моделирования (экспериментальных исследований).

5. Проведение натурного и имитационного моделирования (экспериментальных исследований).

6. Проверка выполнения требований к устойчивости функционирования вариантов построения структур и параметров КВИС и требований к СПКА по готовности к противодействию компьютерным атакам.

7. Анализ и интерпретация результатов моделирования.

Шаг 1. Формализация натурного и имитационного моделирования процессов противодействия компьютерным атакам на КВИС.

Формализация описания КВИС в условиях атак осуществляется в соответствии с постановкой задачи на моделирование и основана на подготовке исходных данных моделирования, представлении моделируемых процессов структурно-функциональной схемой (рисунок 1) и соответствующими математическими моделями.

Подготовка исходных данных для натурного и имитационного моделирования процессов противодействия компьютерным атакам на КВИС состоит в задании исходных параметров, характеризующих события и состояния на рисунке 1: $B_{Yi}, \xi_{уяз}^{воз}, S_i, Y_{i,}\tau_i, Z_{ПДi}$. Кроме того, определяется временной интервал моделирования, необходимый для отработки регламентов выполнения технологического цикла управления (ТЦУ), и проводится прогнозирование требуемых ресурсов для проведения экспериментальных исследований.

Динамика натурного и имитационного моделирования процессов противодействия компьютерным атакам в соответствии со схемой рисунка 1 реализуется следующим образом:

1. Моделирование штатного функционирования КВИС – поступление входных данных от источника информации (состояние) S_0, осуществление процессов функционирования КВИС при выполнении ТЦУ $S_1,...,S_{i+1},...,S_{j+1},...,S_r$, задержка на сбор, хранение, обработку и передачу информации $\tau_0,...,\tau_{i+1},...,\tau_{j+n}$.

2. Имитация и реальное воспроизведение на стендовом полигоне воздействий компьютерных атак в виде последовательности операций сканирования сети КВИС, внедрения атаки, ее распространения, воздействия атаки на иерархию КВИС и маскировки. На рисунке 1 начало воздействия атаки обозначено состоянием Y_{A0}, а дальнейшее развитие ситуации по сценарию нарушителя интерпретируется цепочкой состояний Y_{A1}, Y_{Ai}, Y_{Ai+1}. Определение «потенциальной площади» воздействия атак, то есть множества уязвимостей КВИС через которые потенциально могут быть внедрены компьютерные атаки – обозначается как $\xi_{уяз}^{воз}$.

3. Процессы противодействия компьютерным атакам, охватывающие выбор средств противодействия, нейтрализацию атак (обнаружение и анализ атак), выявление и устранение уязвимых мест $\xi_{уяз}$, активное противодействие атакам – моделируется параметрами $z_{ПД1},...,z_{ПДi+1},...,z_{ПДj+n}$.

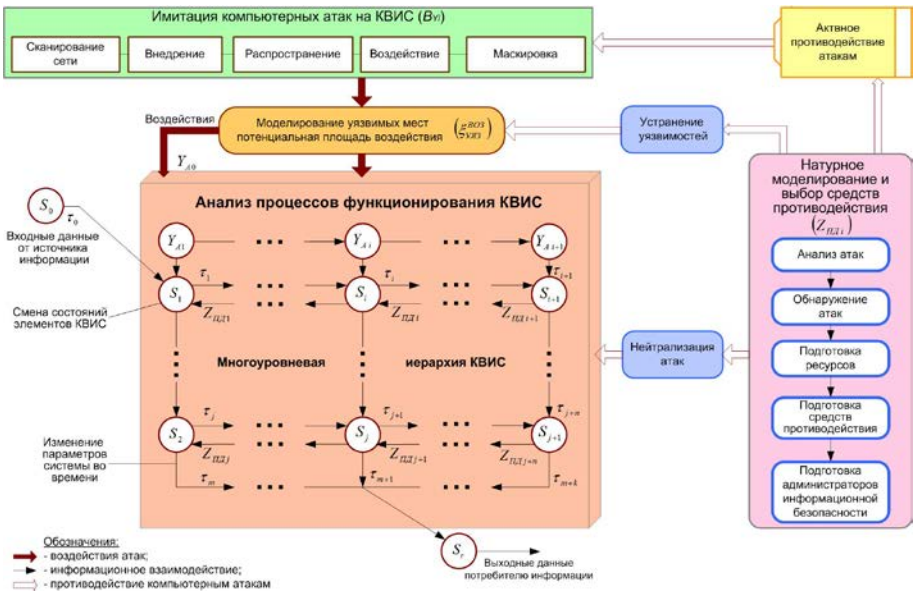


Рисунок 1 – Схема натурного и имитационного моделирования процессов противодействия компьютерным атакам на КВИС

Оглавление

В основе рассматриваемого метода лежит событийный способ имитации и натурного воспроизведения воздействий атак на КВИС при контроле требований к СПКА и устойчивости функционирования системы. Применение метода предполагает, что:

- на временном интервале выполнения ТЦУ имеется своя характерная последовательность состояний и событий сбора, обработки и передачи информации в КВИС;
- множество событий и состояний воздействия компьютерных атак конечно, модификации атак определяются исходя из знаний об известных атаках, неизвестные атаки обнаруживаются путем контроля выполнения ТЦУ в КВИС по принципу «запрещено все то, что не разрешено»;
- детализация представления КВИС соответствует макетам базовых АРМ, размещенных в составе локальной (возможно и распределенной) вычислительной сети стендового полигона (должно быть достаточно адекватное совпадение структурно-функционального построения КВИС и его модели);
- интенсивность и объем поступления потоков входной информации и воздействий компьютерных атак моделируются соответствующими имитаторами.

Шаг 2. Разработка моделирующих алгоритмов.

Разработка моделирующих алгоритмов состоит в представлении исследуемых процессов противодействия компьютерным атакам в соответствии с алгоритмами унифицированной имитационной модели противодействия компьютерным атакам на КВИС (рисунок 2) и сбора статистики о параметрах компьютерных атак на КВИС (рисунок 3).

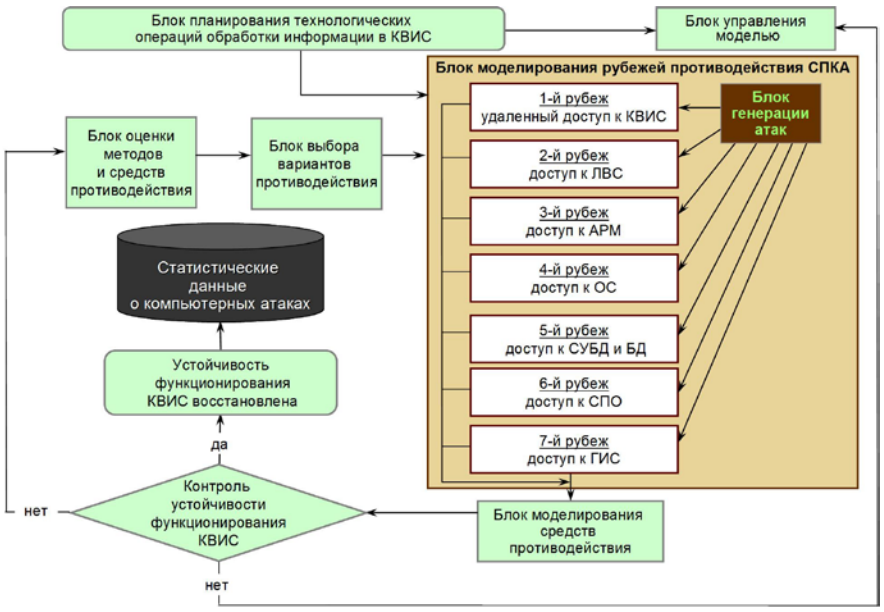


Рисунок 2 – Алгоритм унифицированной имитационной модели процессов противодействия компьютерным атакам на КВИС

Унифицированная имитационная модель процессов противодействия компьютерным атакам на КВИС разработана для прогнозирования поведения реального КВИС и соответствующих ему средств противодействия при воздействии атак. Основным требованием к модели является адаптация к широкому классу задач моделирования средств противодействия компьютерным атакам на КВИС.

Алгоритм унифицированной имитационной модели (рисунок 2) предназначен для сбора в едином формате необходимых статистических данных о процессах противодействия с целью выбора базовых элементов и параметров перспективных средств предупреждения, обнаружения, анализа компьютерных атак и активного противодействия им. Этот алгоритм включает в свой состав следующие основные элементы:

1. Блок планирования технологических операций обработки информации в КВИС, обеспечивающий моделирование реальных процессов сбора, обработки и передачи информации при выполнении ТЦУ.
2. Блок управления моделью осуществляет планирование имитационного эксперимента, запуск и остановку имитационной модели, контроль времени испытаний модели, диспетчеризацию и синхронизацию совместной работы блоков модели, отработку динамики поступления транзакций потоков данных информационно-управляющих процессов и процессов противодействия

компьютерным атакам.

3. Блок моделирования рубежей противодействия КВИС – позволяет провести оценку от одного до 7 рубежей противодействия компьютерным атакам, на которых встраиваются датчики СПКА:

– удаленного доступа от абонентов КВИС (датчики цифрового коммуникационного оборудования и межсетевого экрана);
– локальной вычислительной сети;
– доступа к АРМ КВИС;
– операционной системы;
– системы управления базой данных;
– специального программного обеспечения;
– геоинформационной системы, используемой в КВИС (датчики контроля работы с пространственными данными).

4. Блок генерации компьютерных атак, работа которого заключается в имитации потока возможных атак по заданным законам распределения вероятностей и интенсивностей воздействия атак на различные компоненты КВИС.
5. Блок моделирования средств противодействия, позволяет моделировать базовые функции средств предупреждения, обнаружения, анализа атак и активного противодействия им.
6. Блоки оценки методов и средств противодействия и выбора вариантов противодействия предназначены для сравнительного анализа и выбора варианта методов и средств противодействия атакам при сохранении заданной устойчивости функционирования КВИС (резерв времени на восстановление работоспособности КВИС), предполагаемой информационной нагрузке (задержках времени на обработку информации).
7. Блок сбора статистических данных о компьютерных атаках – запись, хранение и выдача сведений о параметрах атак в соответствии с их паспортом.

По результатам контроля устойчивости функционирования (рисунок 2) для получения рациональных вариантов построения средств противодействия атакам и восстановления устойчивости функционирования КВИС осуществляется корректировка параметров блоков оценки методов и средств противодействия, выбора вариантов средств противодействия и управления моделью.

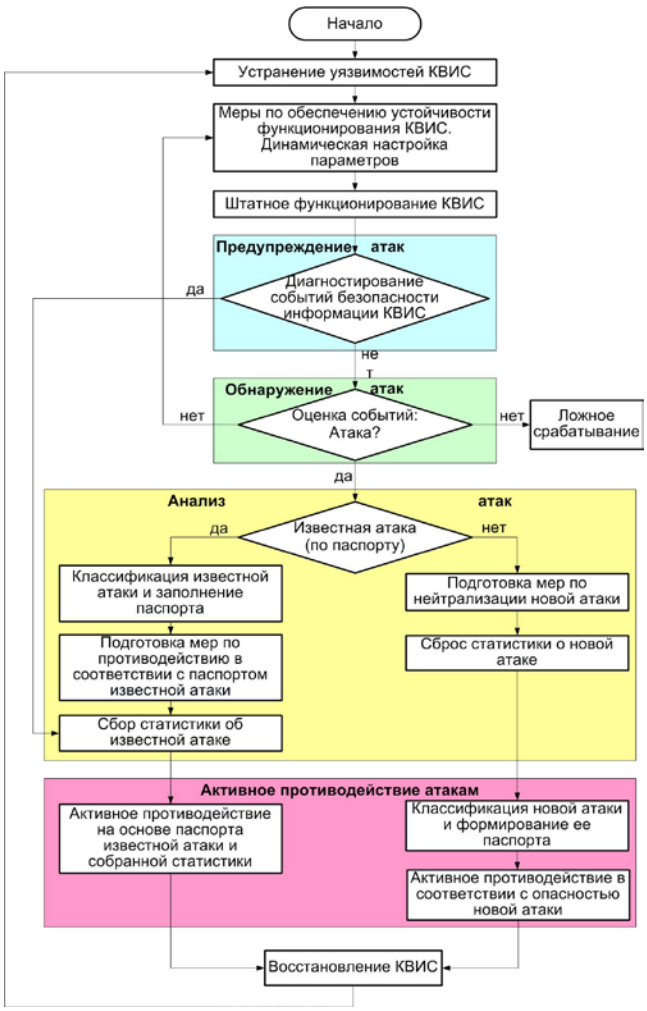


Рисунок 3 – Алгоритм сбора статистики о параметрах компьютерных атак на КВИС

Алгоритм на рисунке 3 позволяет провести натурное и имитационное моделирование процессов:

- предупреждения атак (предотвращение атак путем диагностики фактов нарушения безопасности информации КВИС);
- обнаружения атак (по результатам оценки событий срабатывания датчиков);
- сравнительного анализа атак (выявление известных и новых атак путем оценки признаков атаки по её паспорту комплексом методов – сигнатурного анализа, методами анализа аномальных отклонений и функционального анализа);
- активного противодействия известным и новым атакам в соответствии с исходными данными паспорта атаки;
- восстановления информационно-вычислительного процесса КВИС (путем

использования дополнительных задержек на обработку информации);

- устранения уязвимых мест (путем включения специальных программ «патчей», устраняющих возможность первоначального внедрения атаки через уязвимости операционной системы (ОС), системы управления базой данных (СУБД), специального программного обеспечения (СПО), протоколы передачи данных);
- динамической настройки параметров устойчивости функционирования КВИС (настройка минимального набора параметров, характеризующих штатные события и состояния КВИС).

При подготовке мер по нейтрализации новой компьютерной атаки используется принцип применения средств противодействия атаке в режиме «по умолчанию», который означает заполнение паспорта компьютерной атаки по имеющейся информации, локализация зоны действия атаки, нейтрализация источника атаки, оценка устойчивости функционирования КВИС и восстановление ее работоспособности.

Шаг 3. Планирование натурного и имитационного моделирования.

Планирование эксперимента позволяет найти такую совокупность доминирующих факторов, при которых достигается уменьшение числа необходимых испытаний и повышение экономичности экспериментов [30].

Формализация процессов противодействии компьютерным атакам на КВИС позволяет определить объем факторного пространства, анализ которого возможен при основных ограничениях на метод Бокса-Уилсона: существование только одного оптимума в факторном пространстве и наличие не более 15 факторов, влияющих на значение отклика. Данные ограничения удовлетворяют условию получения оценок КВИС в условиях атак с гарантированной достоверностью. Увеличение количества учитываемых факторов больше 10 (наилучшим количеством факторов является число максимально возможных различий для субъекта, равное 7 [30]) приводит к значительному усложнению моделирующих алгоритмов (увеличивается вероятность ошибки) и большому разбросу показателей противодействия атакам.

Необходимое общее количество испытаний имитационных и натурных моделей на стендовом полигоне соответствует сочетанию уровней факторов и определяется соотношением [30]:

$$N_o = \prod_{i=1}^{k} l_i , \qquad (1)$$

где l_i - число уровней i -го фактора; $i = 1,...,k$,

k - количество факторов в эксперименте.

При нормальном законе распределения значений оцениваемых параметров R_i для определения необходимого числа испытаний, обеспечивающих статистически гарантированные результаты с заданной ошибкой $\varepsilon_м$ и средним квадратическим отклонением $\sigma_м$, используем формулу, имеющую вид [1, 6, 30]:

$$N_u = \frac{(t_ф \sigma_м)^2}{\varepsilon_м^2}, \qquad (2)$$

где $t_ф$ - квантиль нормального распределения определяется с использованием таблиц функции Лапласа [1, 6].

Составление факторной матрицы планирования осуществляется при поиске условий планирования эксперимента на основе метода Бокса-Уилсона [30]. Необходимость поиска условий эксперимента вытекает из формулы (1), показывающей, что полный факторный эксперимент может содержать слишком большое количество испытаний, соответствующих возможным комбинациям уровней факторов (например, если $k = 5$, то при $l_i = 3$ $N_o = 243$). Модификация метода Бокса-Уилсона путем добавления расчетного соотношения (2) для определения количества прогонов при каждом испытании КВИС в условиях атак позволяет получить целостный алгоритм планирования экспериментов.

Шаг 4. Реализация имитационных и натурных моделей на стендовом полигоне в виде совокупности макетов АРМ.

Реализация имитационных и натурных моделей на стендовом полигоне в виде совокупности макетов АРМ проводится по схеме проведения экспериментальных исследований. Она заключается в комплексировании базовых компонентов КВИС, объединенных в локальную вычислительную сеть, в виде комплекса средств реального коммуникационного и компьютерного оборудования, макетов целевых АРМ, имитаторов информационной нагрузки и компьютерных атак, макетов СПКА. Средства имитационных и натурных моделей должны быть работоспособны, и адекватно воспроизводить на стенде процессы применения КВИС при выполнении ТЦУ.

Шаг 5. Проведение натурного и имитационного моделирования (экспериментальных исследований).

Данный шаг (рисунок 4) заключается в экспериментальной отработке на практике цепочки исследований: математическая модель – моделирующий алгоритм – макет КВИС – оценка параметров КВИС при имитации условий ее применения и воздействий атак – проверка обратной связи (соответствия) при проведении испытаний модели и реальной КВИС.

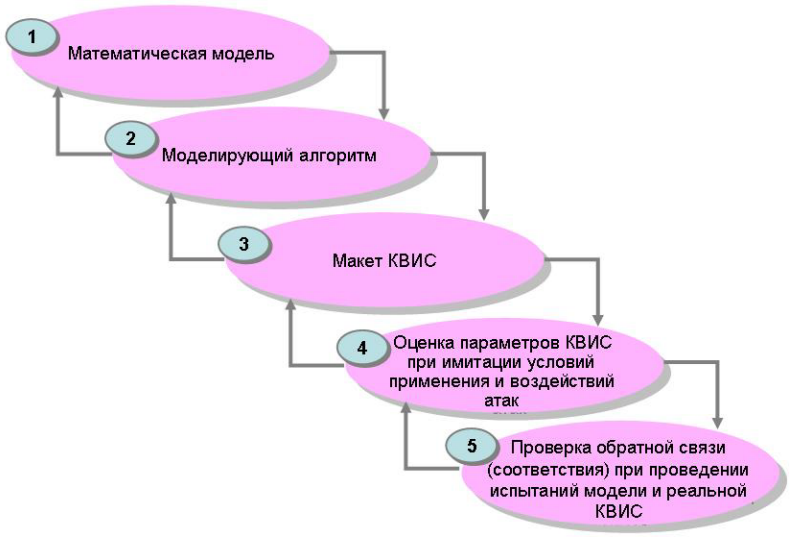


Рисунок 4 – Порядок проведения натурного и имитационного моделирования

Шаг 6. Проверка выполнения требований по противодействию компьютерным атакам

Шаг 6.1. Оценка выполнения требований по устойчивости функционирования возможных вариантов структур и параметров КВИС.

Оценка вариантов структур и параметров КВИС заключается в контроле выполнения требований по устойчивости функционирования системы по следующим факторам:

Шаг 6.1.1. Проверка безошибочности общего и специального программного обеспечения (устранение уязвимых мест) в ходе имитационного эксперимента по соотношениям:

$$\left[\begin{array}{l} S_{КВИС}^{СПО} \in S_{КВИС}^{уст} = \left\{ S_i^{СПО} \left| \begin{array}{l} \exists V_{тестi}^{СПО} \in V_{тест}^{СПО} \geq V_{тр}^{СПО}, \psi(b_{ош\,i}^{СПО}) = \\ = \sum_{i=1}^{k} P(N_{bi}^{исп} / N_b^{общ}) = 1, B_{ош\,н}^{СПО} = \varnothing \end{array} \right. \right\}; \\ B_{ош} = \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{r} b_{ош\,i}^{СПО}, b_{ош\,j}^{ОПО}, b_{ош\,k}^{ЦКО}; \\ \forall b_{ош\,i} \in \{1,\ldots,\mathrm{N}\} \rightarrow \exists \psi_{КВИС}^{ош} = \sum_{i=1}^{n} \sum_{k=1}^{m} \psi_{ОПОi}(b_{ош\,i}) \psi_{СПО\,k}(b_{ош\,k}), \\ t_{тест} \geq t_{треб}; \\ \exists \{\psi_{серв}\} \cap \{\psi_{кл}\} = \{\psi_{КВИС}^{тест}\} \succ \{\psi_{треб}\}; \end{array}\right., \quad (3)$$

где $S_{КВИС}^{СПО}, S_i^{СПО}$ - состояния СПО, принадлежащие множеству устойчивых состояний $S_{КВИС}^{уст}$;

$V_{тестi}^{СПО}$ – объем тестов СПО на требуемую безошибочность $V_{тр}^{СПО}$;

$b_{ош\,i}^{СПО}$ – ошибки СПО;

$N_{bi}^{исп}$ – количество исправленных ошибок СПО;

$N_b^{общ}$ – общее количество ошибок СПО

$b_{ош}$ – общее количество ошибок КВИС;

$b_{ош\,j}^{ОПО}$ – ошибки общего программного обеспечения (ОПО);

$b_{ош\,k}^{ЦКО}$ – ошибки в программах цифрового коммуникационного оборудования;

$\psi_{КВИС}^{ош}$ – функция безошибочности КВИС;

$\psi_{ОПОi}$ – функция безошибочности ОПО;

$\psi_{СПО\,k}$ – функция безошибочности СПО;

$t_{тест}$ – время тестирования программ;

$\psi_{серв}$ – программы функций «сервера» СПО;

$\psi_{кл}$ – параметры функций «клиента» СПО;

$\psi_{КВИС}^{тест}$ – параметры тестирования комбинаций функций взаимодействия «клиент-сервер» СПО.

Соотношение (3) формулируется как совокупность условий: для обеспечения состояний устойчивого функционирования СПО принадлежавших элементам множества устойчивых состояний КВИС необходимо провести требуемый объем тестирования СПО на безошибочность и исправить ошибки в программах, тогда функция вероятности исправленных ошибок будет стремиться к единице. Функция безошибочности КВИС определяется как аддитивная функция ошибок в СПО и ОПО. Проверка безошибочности СПО включает тестирование возможных комбинаций взаимодействия «клиент-сервер» и проверке того, что эти комбинации соответствуют требуемому множеству функций взаимодействия абонентов КВИС (отсутствуют недекларированные возможности).

В ходе моделирования ошибки в СПО устраняются путем тестирования программ в соответствии со спецификацией и техническим заданием. Обеспечить безошибочность ОПО предполагается путём проведения дополнительных испытаний компонентов КВИС на стендовых полигонах.

Шаг 6.1.2. Проверка выполнения требования к минимуму привилегий СПО и ОПО, что соответствует принципу «нет программ, которые не подлежат проверке», определяется соотношением:

$$\forall f_{СПО}(S_{КВИС}^{СПО}) \in f_{СПО}^{уст}(S_{КВИС}^{уст}), \exists f_{СПО}^{пр}(S_i^{СПО}) \Big| K_{ri} \geq K_{mpi}, \underset{i=1}{\overset{k}{U}} f_{СПО}^{непр}(S_i^{СПО}) \to \min, \qquad (4)$$

где $f_{СПО}^{уст}(S_{КВИС}^{уст})$ – привилегированные функции СПО по доступу к информационным и вычислительным ресурсам ОПО, элементов компьютерного и коммуникационного оборудования при сохранении устойчивости КВИС;

$f_{СПО}(S_{КВИС}^{СПО})$ – функции СПО, принадлежащие множеству функций устойчивого состояния КВИС;

$f_{СПО}^{пр}(S_i^{СПО})$ – функции СПО, проверенные на привилегии на i-м шаге моделирования;

K_{ri} - параметр, характеризующий критические процессы КВИС;

$f_{СПО}^{непр}(S_i^{СПО})$ – функции СПО, непроверенные на привилегии.

$$\forall f_{СПО}^{пр}(S_i^{СПО}) \to \exists P(x_{пр}) = \begin{cases} 0 - \text{не включены привилегии}, \\ 1 - \text{включены привилегии}, \\ 1 > \text{x}_{\text{пр}} > 0 - \text{не правомочно сть привилегий}, \end{cases} \quad (5)$$

где $f_{СПО}^{пр}(S_i^{СПО}) \notin f_{СПО}^{тр}(S_i^{СПО})$ – условие отключения всех нештатных программ, не предусмотренных техническим заданием;

$x_{пр}$ – проверочный параметр привилегий программ.

Шаг 6.1.3. Проверка качества администрирования сетей КВИС определяется согласно условиям:

$$\forall (a_{Иi}, a_{Пj}) \in A_{ИП} \to \exists (a_{Иi}^*, a_{Пj}^*) \in (a_{Иi}, a_{Пj}) \notin A_{ИП}, \quad (6)$$

где $A_{ИП}$ - полная совокупность параметров администрирования;

пусть существует параметр контроля защищенности протоколов передачи данных (ППД) $d_{ППД}^{з}$, тогда функция администрирования ППД должна быть свойством:

$$Ad_m(\text{S}_{\text{КВИС}}^{уст}) \mid d_{ППД}^{з}: \begin{cases} 0 - \text{не включена защита ППД и интерфейсов } КВИС \\ 1 - \text{защита интерфейсов "клиент – сервер"} \\ \text{между абонентами } КВИС \text{ включена}, \\ 2 - \text{защита внутренних интерфейсов "датчик – СПКА"}, \\ \text{"компонент – компонент" СПКА включена}. \end{cases} \quad (7)$$

На практике качество администрирования сетей КВИС определяется возможностями мониторинга безопасности информации, к которым относятся следующие действия:

- идентификация операторов и администратора КВИС;
- аутентификация операторов и администратора КВИС;
- авторизация доступа к коммуникационным ресурсам сети (ППД и интерфейсам) и информационным ресурсам КВИС (СУБД);
- авторизация доступа к базам и хранилищам данных;
- систематическое выявление уязвимостей сетевыми сканерами и анализаторами;
- оценка способов предотвращения атак организационно-техническими мерами.

Шаг 6.1.4. Проверка уязвимостей протоколов TCP/IP определяется минимумом разрешенных администратором прикладных (сетевых) протоколов (SMTP, SMNP, FTP, POP3, IMAP, LDAP и других), IP - адресов и стеков протоколов TCP/IP (путём введения ограничений на число прикладных протоколов; логического отключения не используемых IP-адресов и свободных портов коммуникационного оборудования) и осуществляется по соотношениям:

$$\begin{aligned}
&\forall \xi_{уяз}^{IP} \in M_{уяз}^{IP} \rightarrow \exists A_{IP} \in \{A_{IPj},\ldots, A_{IPj+1}\} \rightarrow \min \\
&-\text{анализ уязвимости } IP-\text{адресов}, \\
&\forall \xi_{уяз}^{DNS} \in M_{орг}^{DNS} \rightarrow \exists A_{DNS} \in \{A_{DNSj},\ldots, A_{DNSj+1}\} \rightarrow \min \\
&-\text{анализ уязвимости DNS адресов доступа к серверам } КВИС,
\end{aligned} \tag{8}$$

где $\xi_{уяз}^{IP}, \xi_{уяз}^{\text{DNS}}$ – уязвимости IP-адресов и DNS-адресов;

$M_{орг}^{IP}, M_{орг}^{DNS}$ – множество ограниченного числа IP-адресов и DNS-адресов;

A_{IP}, A_{DNS} – события использования уязвимостей IP-адресов и DNS-адресов.

Следует отметить, что переход со стандартного протокола TCP/IP на протокол IPv6 не решает проблемы защищенности от компьютерных атак, так как существует потенциальная возможность воздействия атаки через уязвимости некорректно используемых сервисов на одном из уровней семиуровневой модели взаимодействия открытых систем. Защищенный протокол информационного взаимодействия IPSec не соответствует требованиям российских стандартов и может включать в свой состав программные закладки нарушителя.

Шаг 6.1.5. Выполнение требований по устойчивости функционирования КВИС определяется исходя из соотношений:

$$S_{КВИС}^{\text{уст}}(t_м > T_{ТЦУ}) = \sum_{i=1}^{\text{k}} (S_{КВИС\,i}^{уст},\ldots S_{КВИС\,i+k}^{уст}) \geq \sum_{i=1}^{\text{k}} S_{КВИС\,i}^{уст\,тр}(T_{ТЦУ}) \rightarrow \max, \tag{9}$$

где $t_м$ – время моделирования;

$T_{ТЦУ}$ – время выполнения ТЦУ.

– выполнения заданного объема функций КВИС:

$$f_{СПО}(S_i^{СПО}) \in f_{СПО}^{зд}(S_i^{СПО}) \Big| t_м < T_{ТЦУ} \to \max; \quad (10)$$

– сохранения устойчивости функционирования при воздействии компьютерных атак:

$$\begin{aligned} &\forall Y_{Ai} \in Y_A \forall V_{КВИС\,i}^{СПО} \in V_{КВИС}^{СПО} \le V_{КВИС}^{СПО\,тр} \to \min, N_{ППД}^{ПП} \in N_{ППД} \to \min, \\ &\xi_{уяз} \to \min, \to \exists S_{КВИС}^{уст} \in S_{КВИС}^{уст\,зд}(t_{ТЦУ}) \Big| V_{вых} \in V_{вых}^{тр}; \end{aligned} \quad (11)$$

где $V_{КВИС}^{СПО}$ – объем СПО, который должен быть минимален как по функциям;

$N_{ППД}^{ПП}$ – количество разрешенных ППД;

$N_{ППД}$ – общее количество ППД.

– выполнения условия самовосстановления КВИС по контрольным точкам информационно-вычислительного процесса:

$$\forall Y_{Ai} \in Y_A \to \exists M_{ПДi} \in M_{ПД}, Z_{ПДi} \in Z_{ПД} \to S_{КВИС\,i}^{воссm} \in S_{КВИС}^{уст} \to \max, \quad (12)$$

где $S_{КВИСi}^{воссm}$ – состояния восстановления устойчивости функционирования КВИС.

Шаг 6.2. Оценка выполнения требований к СПКА по готовности к противодействию компьютерным атакам.

Шаг 6.2.1. Оценка оперативных возможностей воздействия атак на КВИС по соотношениям для «потенциальной площади» воздействия атак $\xi_{уяз}^{воз}$:

$$\forall(\xi_{Yi}, Y_{Ai}) \in \Xi = \{\xi_Y\} \cap \{Y_A\} \to \exists \Xi^* = P(\xi_{Yi}^*, Y_{Ai}^*) = 0, \quad (13)$$

где Ξ – множество соответствий параметров «уязвимость-атака»;

Ξ^* – функция реализуемых в атаках соответствий параметров «уязвимость-атака»;

ξ_{Yi}^* – параметры уязвимостей, реализованных в атаках;

Y_{Ai}^* – параметры, осуществленных атак;

– оценка характеристик сценариев компьютерных атак нарушителя:

$$J(S_{КВИС\,i})\left|P(h_{Yi}):\begin{cases}0-\text{блокирована атака},\\ 0{,}4>P(h_{Yi})>0-\text{внедрена атака, но обнаружена},\\ 1-\text{осуществлено функциональное поражение}\\ \text{КВИС компьютерной атакой}\end{cases}\right., \qquad (14)$$

где $J(S_{КВИСi})$ – функция, характеризующая сценарии атак;

h_{Yi} – параметр, описывающий результативность атак;

– оценка средств реализации компьютерных атак нарушителем:

$$\begin{aligned}&\forall Y_{Ai}\in Y_A\rightarrow\exists B_{Yi}\in\left\{B_{ск},B_{вн},B_{рас},B_{воз},B_{ин\,м}\right\}\left|\xi_{уязi}\notin\xi_{уяз}^{обн}\right.,\\ &\rightarrow\sum_{j=1}^{k}(B_{скj},B_{внj},B_{расj},B_{возj},B_{ин\,мj})\rightarrow\max\exists f(B_{Yi}):Y_A(A_i)\rightarrow S_{КВИС}^{ПОР}(X_i),\end{aligned} \qquad (15)$$

$f(B_{Yi})=P(B_{Yi})=0$ – условие неудачного применения средств реализации компьютерных атак нарушителем;

где $f(B_{Yi})$ – функция успешного применения средств реализации компьютерных атак нарушителем;

B_{Yi} – средства реализации атак;

$B_{ск}$ – средства сканирования уязвимостей КВИС;

$B_{вн}$ – средства внедрения атак;

$B_{рас}$ – средства распространения атак;

$B_{воз}$ – средства воздействия атак;

$B_{ин\,м}$ – средства маскировки атак;

– оценка «потенциальной площади» воздействия атак, определяемой количеством уязвимых мест, через которые могут воздействовать атаки:

$$\forall t_{мон}=t_{ск}+t_{ан}\geq t_{мон}^{тр},K_{yi}\geq K_{Yi}^{тр},\forall\xi_{уяз\,П}^{воз}=\sum_{j=1}^{k}\xi_{уязj}(S_{КВИС\,j})\rightarrow\min, \qquad (16)$$

где $t_{мон}$ – время мониторинга защищенности КВИС;

$t_{ск}$ – время сканирования уязвимостей КВИС;

$t_{ан}$ – время анализа сетевой защищенности КВИС;

K_{yi} – количество выявленных угроз воздействия атак;

– оценка «фактической площади» воздействия атак, определяемой количеством состояний и событий воздействия атак:

$$\forall t_м > \mathrm{T_{ТЦУ}}, K_{Yi} \geq K_i^{mp}, \forall \xi_{уяз\,Ф}^{воз} = \sum_{j=1}^{k} \xi_{уязj}(Y_{\mathrm{A}j}, A_j) \to \min, \qquad (17)$$

где $\xi_{уяз\,Ф}^{воз}$ – «фактическая площадь» воздействия атак.

Шаг 6.2.2. Оценка готовности СПКА к противодействию компьютерным атакам по принципу «7 + 7», означающему то, что обеспечение СПКА противодействия компьютерным атакам на основе обнаружения атак на семи рубежах СПКА и семи уровнях эталонной модели взаимодействия открытых систем, производится по соотношениям:

– оценка многоуровневой защищенности КВИС на основе проверки « 7 » рубежей СПКА (в соответствии с алгоритмом рисунка 2):

$$\forall V_{СПОКА\,i} \in r_{СПОКА} = \{1,...,7\}, Y_{Ai} \in Y_A, D_{СПОКА}^r \in R_{СПОКА},$$
$$\to \exists \mathrm{Z}_{ПД}^{СПОКА}(\mathrm{s_{КВИС}}) = \mathrm{P_{УФ}}(\mathrm{D_{СПОКА}^r}) \approx \begin{cases} 1, \text{ если } \mathrm{D_{СПОКА}^r} = 7, \mathrm{Y_{Ai}} \to 0; \\ 0.9 > \mathrm{P_{УФ}}(\mathrm{D_{СПОКА}^r}) > 0.7, \text{ если } \mathrm{D_{СПОКА}^r} = 5, \mathrm{Y_{Ai}} \to \min; \\ 0.5 > \mathrm{P_{УФ}}(\mathrm{D_{СПОКА}^r}) > 0.3, \text{ если } \mathrm{D_{СПОКА}^r} \subset \mathrm{K_i^{уст}} \subset \mathrm{R_{СПОКА}^n}; \\ 0, \text{ в противном случае}, \end{cases} \qquad (18)$$

где $r_{СПОКА}$ – рубежи противодействия СПКА;

$D_{СПОКА}^r$ – динамически управляемые параметры рубежей СПКА;

$R_{СПОКА} = \{R_{СПОКА\,i}, ..., R_{СПОКА\,i+1}, R_{СПОКА\,i+R-1}\}$ – совокупность показателей оценки средств противодействия компьютерным атакам на *R*-м шаге дискретизации;

$P_{УФ}(D_{СПОКА}^r)$ – вероятность обеспечения устойчивости функционирования КВИС на рубежах противодействия СПКА;

$K_i^{уст}$ – критически важные параметры мониторинга безопасности информации КВИС, принадлежащие пространству параметров противодействия $R_{СПОКА}^n$ (соответствуют совокупности мероприятий по безопасности информации в КВИС);

– на базе проверки ППД по « 7 »уровням ЭМ ВОС (в соответствии с рисунком 5):

$$\forall r_{ППДi} \in r_{ППД} = \{1,...,7\}, Y_{Ai} \in Y_A \to \min, d^r_{ППД} \in R^n_{серв}, T_{ТЦУ} \le T_{зад} \to \min,$$

$$l_{ППД} = \bigcup_{j=1}^{R} l_{ППДj} = l^{TP}_{ППД}, \tag{19}$$

$$\to \exists Z^{ППД}_{ПД}(s_{КВИС}) = P_{УФ}(D^r_{ППД}) \approx \begin{cases} 1, \text{если } D^r_{ППД} = 7; \\ 0.9 > P_{УФ}(D^r_{ППД}) > 0.7, \text{если } D^r_{ППД} \in \{4,...,7\}; \\ 0.5 > P_{УФ}(D^r_{ППД}) > 0.3, \text{если } D^r_{ППД} \in \{1,2,3\}; \\ 0, \text{в противном случае}, \end{cases}$$

где $r_{ППД} = \{1,...,7\}$ – последовательно реализованные рубежи противодействия ППД от физического до прикладного уровня ЭМВОС на основе защищенного ППД КВИС (разработанного на основе стеков TCP/IP путем внедрения дополнительных проверок сервисных функций на уровнях ЭМВОС);

$D^r_{ППД}$ – динамически управляемые параметры рубежей ППД;

$R^n_{серв}$ – пространство параметров, регулирующих сервисные функции реализации ППД на уровнях ЭМ ВОС;

$P_{УФ}(D^r_{ППД})$ – вероятность обеспечения устойчивости функционирования КВИС на рубежах противодействия ППД;

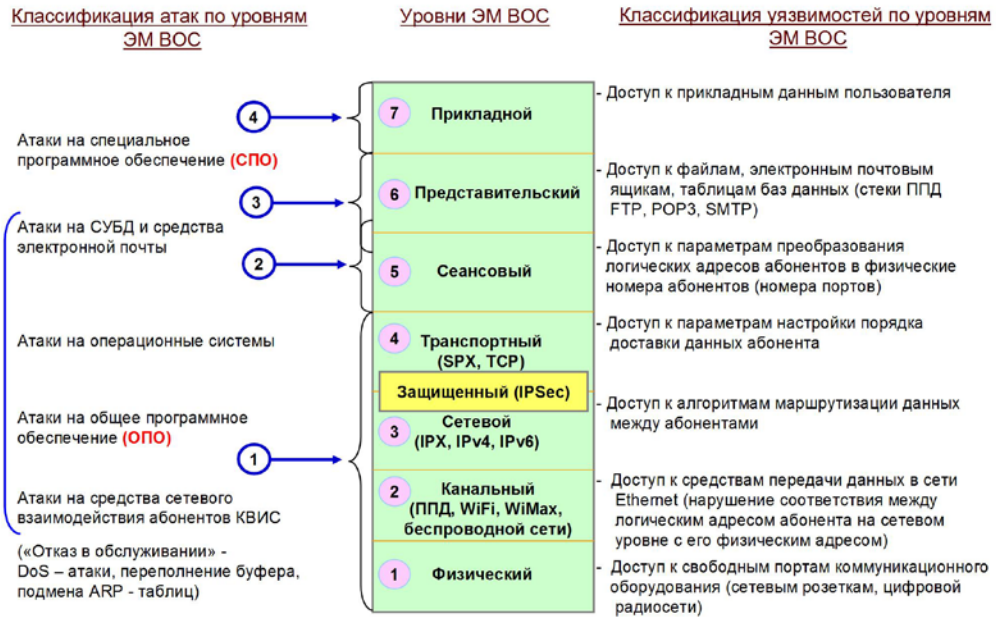


Рисунок 5 – Уязвимости КВИС на базе протокола TCP/IP

– оценка нейтрализации компьютерных атак (предупреждение, анализ, обнаружение атак):

$$
\begin{aligned}
&\forall(Z_{ПДi},M_{ПДi})\ э\ \{Z_{ПД},M_{ПД}\}\left|S_{КВИС}^{уст}\right.\to \max,\text{если } t_M > T_{ТЦУ},\\
&\exists\sum_{j=1}^{R} b_{общ},f_{СПО}^{непр}(S_j^{СПО}),\ f_{СПО}^{*}(S_j^{СПО}),(a_И^{*},a_П^{*}),\xi_{уяз\,П}^{воз*},\xi_{уяз\,П}^{воз}\to \min,\\
&\forall Y_{адi}^{н*},Y_{шт\,оп}^{н*},Y_{оп\,ат}^{н*},\to \exists Z_{ПД}(Y_{адi}^{н*},Y_{шт\,оп}^{н*},Y_{оп\,ат}^{н*})\to \max,\\
&\text{тогда } \forall P(\xi_{уяз})\in P(\xi_{уяз\,П}):\begin{cases}
0,\text{если } R_{КВИС\,i}\in R_{КВИС}\notin R_К^{p},\text{то } P(S_{КВИС}^{уст})\to 1,\\
\xi\ge 1,\forall Y_{Ai}\in Y_A\to \exists P\left[S_{КВИС}(T_{ТЦУ})\right]\to 0;\\
\exists P\left[S_{КВИС}^{уст}(T_{ТЦУ})\right]\to \max;\\
1,\text{если } R_{КВИС\,i}\in R_{КВИС}\in R_k^{p},\text{то } P(S_{КВИС}^{уст})\to 0,
\end{cases}
\end{aligned}
\qquad (20)
$$

где $f_{СПО}^{*}(S_j^{СПО})$ – функции СПО после тестирования и устранения ошибок и уязвимостей;

$\xi_{уяз\,П}^{воз*}$ – «потенциальная площадь» воздействия атак после тестирования и устранения ошибок в СПО;

$R_{КВИС}$ – динамически управляемые параметры КВИС;

R_k^{p} – разрешенные динамически управляемые параметры КВИС;

$Y_{адi}^{н*}$ – угрозы нештатного доступа нарушителя к ресурсам КВИС с полномочиями администратора;

$Y_{шт\,оп}^{н*}$ – угрозы нештатного доступа нарушителя к ресурсам КВИС с полномочиями штатного оператора;

$Y_{оп\,ат}^{н*}$ – угрозы нештатного доступа нарушителя к ресурсам КВИС с возможностями оператора, реализующего атаки на отдельные уязвимости или инициализирующего программные закладки.

– оценка активного противодействия атакам:

$$
\begin{aligned}
&\forall Y_{Ai}\in Y_A,f_{МЭ\,i}(S_{КВИС})\in f_{МЭ}(S_{КВИС})\to \exists A_{МЭ}\in\{A_{МЭ\,j},...,A_{МЭ\,j+1}\}\to \min;\\
&\forall Z_{ПДi}(S_{КВИС})\in Z_{ПД}(S_{КВИС}^{уст})\left|\forall Y_{Ai}\in Y_A\right.\to \min;\\
&\exists Y_A^{б}\subset Y_A^{пер}\subset Y_A^{ло}\subset Y_A^{иА}\in Y_A^{пр}\to \max,T_{ТЦУ\,i}\in T_{ТЦУ};\\
&\exists S_{КВИС}^{рек}\subset S_{КВИС\,Ф}^{защ}\subset S_{КВИС}^{уст}(f_{СПО}^{\min})\in S_{КВИС}^{уст}\left|\not\subset S_{КВИС\,Ф}^{н\,уст}\right.,
\end{aligned}
\qquad (21)
$$

где $f_{МЭ\,i}(S_{КВИС})$ – функции межсетевого экрана, работающего в составе КВИС;

$A_{МЭ}$ – множество параметров нарушения правил удаленного доступа к сети, установленных в межсетевом экране (пропускаются пакеты разрешенных ППД и допущенных IP-адресов, остальные пакеты блокируются);

$Y_{А}^{б}$ – заблокированные атаки;

$Y_{А}^{пер}$ – перенаправленные атаки на адрес программы удаления атаки;

$Y_{А}^{ло}$ – атака, направленная на ложный объект;

$Y_{А}^{иА}$ – блокирование источника атаки, путем отправки по адресу атаки (например, IP-адресу) пакета данных с блокирующей программой;

$Y_{А}^{пр}$ – множество атак, которым оказано противодействие;

$S_{КВИС}^{рек}$ – реконфигурирование состояния КВИС;

$S_{КВИС\,Ф}^{защ}$ – состояния защищенного фрагмента КВИС после локализации атак;

$S_{КВИС\,Ф}^{н\ уус}$ – состояния неустойчиво работающих фрагментов КВИС в условиях атак.

Шаг 7. Анализ результатов моделирования.

Анализ результатов натурного и имитационного моделирования состоит в обработке статистических данных со значениями параметров и показателей КВИС, СПКА и средств реализации компьютерных атак нарушителя, полученных по итогам испытаний КВИС на стендовом полигоне в условиях компьютерных атак, по методу Монте-Карло.

Законы распределения случайных величин, интерпретирующих транзакции заявок с входными и выходными данными, воздействиями атак, внутреннего обмена при выполнении информационно-вычислительного процесса, потоками данных по противодействию атакам заранее неизвестны и различны по своему виду.

Тем не менее, согласно центральной предельной теореме [6] при сложении достаточно большого числа независимых случайных величин, распределенных по различным законам и сравнимых по порядку дисперсий, закон распределения суммы случайных величин близок к нормальному.

Плотность распределения случайной величины определяется соотношением:

$$F(R_i) = \frac{1}{\sigma_{Ri}\sqrt{2\pi}} e^{-\frac{(R_i - m_{Ri})}{2\sigma_{Ri}^2}}, \qquad (22)$$

где $R_i = \{R_{КВИС\,i}, R_{СПОКА\,i}, R_{Yi}\}$ – множество параметров КВИС, СПКА и компьютерных атак нарушителя при исследовании процессов противодействия компьютерным атакам;

σ_{Ri} – среднее квадратическое отклонение случайной величины R_i;

m_{Ri} – математическое ожидание случайной величины R_i.

В соответствии с теорией вероятностей [1, 5, 6] для того, чтобы случайную величину R_i считать нормальной, достаточно «разыграть» методом Монте-Карло шесть случайных величин и сложить их. Тогда окончательное значение показателей, полученных путем натурного и имитационного моделирования, определяется по обобщенной формуле:

$$R = \sigma_{Ri}\sqrt{2}\left(\sum_{i=1+6\,j}^{6R} R_i - 3\right) + m_{Ri}, \qquad (23)$$

где $j = \{0,..., N\}, R = \{1,..., N\}$

Статистическая вероятность устойчивого функционирования КВИС в общем случае равна:

$$P_{УФ}(t_M > T_{ТЦУ}) = \frac{1}{n_Э}\sum_{i=1}^{n_Э} R_{КВИС\,i}(t_M > T_{ТЦУ}), \qquad (24)$$

где $n_Э$ – количество прогонов моделей на стендовом полигоне.

Статистическая вероятность противодействия компьютерным атакам СПКА с параметрами $R_{СПОКАi}$ равна:

$$P_{СПОКА}(Y_{Ai}) = \frac{1}{n_Э}\sum_{i=1}^{n_Э} R_{СПОКА\,i}(Y_{Ai}) \qquad (25)$$

Статистическая вероятность поражения КВИС компьютерными атаками нарушителя равна:

$$P_{YA}(\xi_{уязi}) = \frac{1}{n_Э}\sum_{i=1}^{n_Э} R_{Yi}(\xi_{уязi}) \qquad (26)$$

Степень доверия к полученным результатам моделирования, полнота и правильность системной оценки устойчивости функционирования КВИС определяются процедурами верификации, адекватности и калибровки имитационных и натурных моделей на основе материалов [23, 30].

Интерпретация результатов моделирования сводится к тому, что по результатам натурного и имитационного моделирования, полученных количественных оценок значений параметров компьютерных атак, устойчивости функционирования КВИС и средств противодействия вырабатываются рекомендации по противодействию компьютерным атакам с учетом специфики конкретного КВИС. Для общего случая рекомендации по противодействию компьютерным атакам на КВИС выглядят как совокупность требований, которые необходимо выполнять следующим образом:

- провести сравнительный анализ исследуемого КВИС с его прототипами, оценить возможность использования защищенных повторно используемых компонентов;
- использовать существующий опыт по устранению ошибок в программах;
- минимизировать уязвимости, увеличивающие «потенциальную площадь» воздействия компьютерных атак;
- обеспечить многоуровневое противодействие атакам по принципу «7+7» уровней противодействия СПКА и ППД;
- минимизировать функции СПО, использующие привилегированный доступ к информационным и программным ресурсам;
- проверить конфигурацию параметров администрирования безопасности информации ОПО и сертифицированных средств защиты информации от несанкционированного доступа;
- проверить настройку параметров удаленного доступа коммуникационного оборудования и межсетевых экранов;
- оценить защищенность режимов удаленного доступа в предположении, что точки удаленного доступа являются наиболее уязвимыми;
- отдельно проверить корректность модернизации КВИС и доработки СПО по добавлению новых функций и устранению ошибок;
- промоделировать критические функции КВИС и оценить ее возможности по сохранению устойчивости функционирования при воздействии имитатором атак и компрометации средств защиты информации КВИС.

Таким образом, метод натурного и имитационного моделирования процессов противодействия компьютерным атакам на КВИС основан на алгоритме унифицированной имитационной модели противодействия компьютерным атакам и математических соотношениях для контроля требований по противодействию компьютерным атакам.

2 Метод экспериментальной оценки эффективности компьютерных атак

Сущность метода экспериментальной оценки эффективности компьютерных атак на КВИС заключается в выполнении последовательности действий, представленных на рисунке 6. Эффективность компьютерных атак нарушителя определяется:

- характеристиками сценариев атак (временем проведения атак и преодоления рубежей противодействия, используемыми уязвимостями, порядком и начальными точками воздействия компьютерных атак на КВИС («точка – точка», «один ко многим», «многие ко многим»);
- характеристиками программно-технических средств реализации компьютерных атак (временем преодоления рубежей противодействия, интенсивностью воздействия атак, количеством средств реализации атак).

Оценка ущерба от воздействия компьютерных атак на КВИС проводится в соответствии с методикой раздела 6.

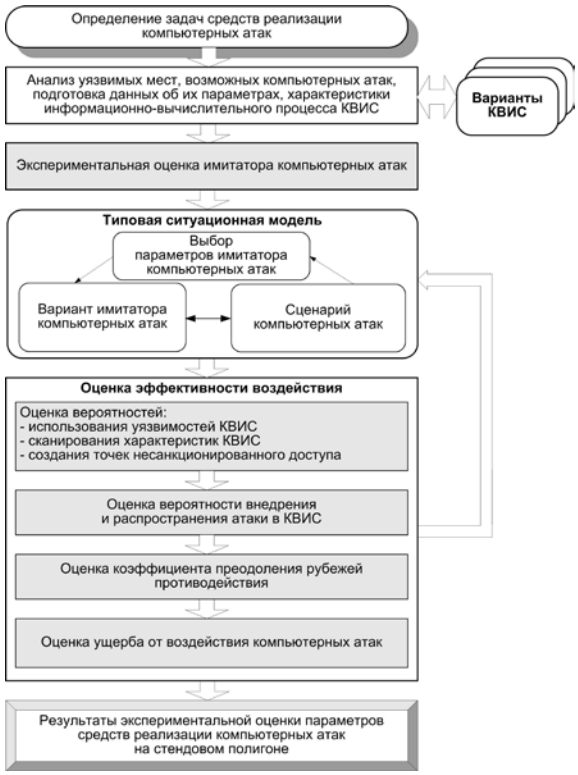


Рисунок 6 – Структурная схема метода экспериментальной оценки эффективности компьютерных атак

Вероятностные оценки эффективности компьютерных атак в рассматриваемом метода методе осуществляются следующим образом:

1. Оценка вероятности использования уязвимостей КВИС определяется по условной вероятности события ξ_Y использования уязвимостей при реализации атак из общего числа уязвимостей $\xi_{уязi}^{воз}$, на которые воздействуют атаки. Эта вероятность в соответствии с формулой Байеса имеет вид:

$$P_{уяз}\left(\xi_{уязi}^{воз}/\xi_Y\right)=\frac{P\left(\xi_{уязi}^{воз}\right)P\left(\xi_Y/\xi_{уязi}^{воз}\right)}{\sum_{i=1}^{n}P\left(\xi_{уязi}^{воз}\right)P\left(\xi_Y/\xi_{уязi}^{воз}\right)}, \quad (27)$$

где $P\left(\xi_{уязi}^{воз}\right)$ – вероятность использования i-й уязвимости КВИС; $i=\{1,...,N\}, \xi_{уяз1}^{воз}\cup\xi_{уяз2}^{воз}\cup...\cup\xi_{уязi}^{воз}=1$;

$P\left(\xi_Y/\xi_{уязi}^{воз}\right)$ – условная вероятность использования уязвимостей КВИС (события ξ_Y) при условии, что существуют уязвимости $\xi_{уязi}^{воз}$.

2. Оценка вероятности сканирования характеристик КВИС предполагает, что количество $N_э$ независимых испытаний по сканированию велико, а вероятность $P_{ск}$ наступления события $N_{ск}$ при каждом отдельном испытании мала, тогда на основе формулы Пуассона получим:

$$P_{ск}\left(N_{ск}\right)=\frac{\lambda^{N_{СК}}}{N_{ск}!}e^{-\lambda},, \quad (28)$$

где $P_{ск}\left(N_{ск}\right)$ – вероятность сканирования характеристик КВИС;

$\lambda=N_э\,p_{ск}$ – фиксированная величина, определяемая исходя из программы и методики испытаний сетевого сканера (анализатора) и требований к значению вероятности сканирования характеристик КВИС.

3. Оценка вероятности создания точек несанкционированного доступа в КВИС определяется по вероятности того события, что при $N_э$ воздействиях компьютерных атак на структуру КВИС (соответствующих числу независимых испытаний), число успешных попыток получения несанкционированного доступа $N_д$ к специальному

программному и информационному обеспечению КВИС попадет в заданный интервал значений данных $N_{д1} - N_{д2}$.

С использованием интегральной теоремы Муавра-Лапласа вероятность создания точек несанкционированного доступа в КВИС (то есть вероятность получения несанкционированного доступа к КВИС в пределах установленного интервала значений данных, характеризующих факт успешного несанкционированного доступа к информационным ресурсам КВИС) равна:

$$P_{ТНСД}\left(N_{д1} \le N_{д} \le N_{д2}\right) \approx \frac{1}{\sqrt{2\pi}} \int_{\frac{N_{д1}-N_э p}{\sqrt{N_э p_{ТНСД} q_{ТНСД}}}}^{\frac{N_{д2}-N_э p_{ТНСД}}{\sqrt{N_э p_{ТНСД} q_{ТНСД}}}} e^{-\frac{x^2}{2}} dx, \qquad (29)$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-x}^{x} e^{-\frac{t^2}{2}} dt$ – функция Лапласа, которая определяется из таблицы значений [1];

$N_{д} \ge 30 \div 50$ [1];

$q_{ТНСД} = 1 - p_{ТНСД}$.

При $p_{ТНСД} = q_{ТНСД}$ вероятность создания ТСНД равна:

$$P_{ТНСД}\left(N_{д}\right) \approx \Phi\left(\frac{N_{д} - N_э p_{ТНСД}}{\sqrt{N_э p_{ТНСД} q_{ТНСД}}}\right).$$

4. Оценка вероятности внедрения и распространения атак в КВИС производится исходя из предположения, что на стендовом полигоне осуществляется последовательность независимых испытаний с двумя возможными исходами – внедрение и распространение компьютерной атаки «выполнено» и «не выполнено». Тогда получим, что наиболее вероятное число возможного внедрения и распространения атак в КВИС при использовании формулы Бернулли определиться неравенством:

$$N_э p_{внрас} - q_{внрас} \le N_{внрас} \le N_э p_{внрас} + p_{внрас}, \qquad (30)$$

где $N_э$ – число экспериментов (испытаний) по исследованию внедрения и распространения атаки;

$p_{внрас}$ – вероятность того, что при каждом из $N_э$ экспериментов (испытаний) событие внедрения и распространения атаки наступит $N_{внрас}$ раз;

$q_{внрас} = 1 - p_{внрас}$ – вероятность того, что при каждом из $N_э$ экспериментов событие внедрения и распространения не наступит.

По результатам экспериментальных исследований процессов воздействия компьютерных атак на стендовом полигоне реализация метода экспериментальной оценки эффективности атак осуществляется в два этапа:

1. Оценка вероятностей, характеризующих возможности компьютерных атак нарушителя по преодолению рубежей противодействия СПКА, по соотношениям (27 – 30).

2. Расчет $K_{ПРП}$ коэффициента преодоления рубежей противодействия СПКА, характеризующего интенсивность и время преодоления компьютерными атаками рубежей противодействия.

Коэффициент преодоления рубежей противодействия компьютерным атакам характеризуется относительным числом преодоленных рубежей противодействия за время воздействия компьютерных атак. Вывод формулы для расчета коэффициента преодоления рубежей противодействия СПКА осуществляется исходя из следующих соображений.

Предполагается, что метод основан на двусторонней модели, в которой сторона В обеспечивает штатное функционирование КВИС и противодействие атакам, а сторона С является нарушителем, реализующим компьютерные атаки на КВИС. Кроме того, допускается, что у КВИС имеется ряд уязвимостей, через которые могут быть осуществлены компьютерные атаки. В составе СПКА организованы рубежи противодействия на основе использования специализированных компонентов СПКА по противодействию компьютерным атакам, комплекса средств защиты информации КВИС от несанкционированного доступа, встроенных средств защиты информации операционной системы и системы управления базой данных. Определены семь рубежей противодействия атакам в соответствии с рисунком 2.

Эффективность воздействия компьютерных атак нарушителя С характеризуется относительным числом преодолённых рубежей противодействия СПКА, определяемым

отношением $r_{СПКА}^{П}$ числа преодоленных рубежей противодействия к $r_{СПКА}^{О}$ общему количеству рубежей: $r_{СПКА}^{П}(t)/r_{СПКА}^{О}$.

В отличие от стороны В, осуществляющей противодействие атакам, сторона С производит воздействие средствами реализации компьютерных атак B_Y. Интенсивность успешного осуществления атак на рубежи противодействия ν_Y (интенсивность воздействия атак на один рубеж противодействия), постепенно приводит к уменьшению $r_{СПКА}^{О}$ общего количества рубежей противодействия атакам до величины $r_{СПКА}^{Ф}(t)$ функционирующих рубежей противодействия на момент времени t. Общее число рубежей противодействия компьютерным атакам равно:

$$r_{СПКА}^{О} = r_{СПКА}^{П}(t) + r_{СПКА}^{Ф}(t).$$

При вычислении коэффициента преодоления рубежей противодействия $K_{ПРП}$ необходимо учесть динамические процессы преодоления компьютерных атак стороны С рубежей противодействия СПКА стороны В, при описании которых использован подход, близкий к приведенному в материалах [1, 2, 36]. Дифференциальное уравнение, описывающее преодоление атаками рубежей противодействия СПКА имеет вид:

$$\begin{cases} \dfrac{dr_{СПКА}^{Ф}(t)}{dt} = -\mu_{уяз}\mu_{сс}\mu_{ТТНС}\mu_{ВНРАС}(\nu_Y P_{ПРП} B_Y) \\ \exists r_{СПКА}^{Ф}(t=0) = r_{СПКА}^{О};\ \exists B_Y = const - начальные\ условия, \end{cases} \quad (31)$$

где $\mu_{уяз}$ – параметр, характеризующий возможность использования уязвимостей КВИС;

$\mu_{ск}$ – параметр, характеризующий доступность сканирования КВИС;

$\mu_{ТНСД}$ – параметр, характеризующий возможности средств реализации атак для создания точек несанкционированного доступа в КВИС;

$\mu_{ВНРАС}$ – параметр, характеризующий возможность внедрения и распространения атак в КВИС при реализации сценария нарушителем.

Значения $\mu_{уяз}, \mu_{ск}, \mu_{ТНСД}, \mu_{ВНРАС}$ изменяются в пределах [0,1], определяются опытным путем и зависят от спецификации применения КВИС, СПКА и особенностей выполнения ТЦУ.

В формуле (31) интенсивность изменения во времени числа функционирующих рубежей противодействия атакам стороны В $\frac{dr^{Ф}_{СПКА}(t)}{dt}$ пропорциональна интенсивности воздействия атак нарушителя С на рубежи противодействия ν_Y, средней вероятности преодоления рубежа $P_{ПРП}$ при осуществлении одной компьютерной атаки, количеству компьютерных атак в сценарии нарушителя A_Y и времени действия атак $T_д$. Правая часть уравнения (31) интерпретирует совокупность компьютерных атак, направленных на преодоление рубежей противодействия, минус взят из соображения убывания рубежей противодействия стороны В.

В методе получение математических соотношений для определения коэффициента преодоления рубежей противодействия $K_{ПРП}$ стороной С при воздействии на сторону В основано на преобразовании уравнений (31) следующим образом.

1. Проведем решение уравнения формулы (31) разделением переменных левой и правой части этого уравнения. С учетом начальных условий (31) получаем выражение для текущего числа не преодоленных рубежей противодействия за время действия компьютерных атак $T_д$:

$$r^{Ф}_{СПКА}(T_д) = r^{О}_{СПКА} - \mu_{уяз}\mu_{ск}\mu_{ТНСД}\mu_{ВНРАС}A_Y\left(\nu_y P_{ПРП} T_д\right).$$

2. Преобразуем последнее уравнение с использованием понятия относительного числа преодолённых рубежей противодействия СПКА $r^{П}_{СПОКА}(t)/r^{О}_{СПОКА}$ за время действия компьютерных атак $T_д$ и получим базовую формулу для расчета коэффициента преодоления рубежей противодействия:

$$\begin{aligned} K_{ПРП}(T_д) &= \mu_{уяз}\mu_{ск}\mu_{ТНСД}\mu_{ВНРАС}A_Y\frac{\nu_Y P_{ПРП} T_д}{r^{О}_{СПКА}} = \\ &= \mu_{уяз}\mu_{ск}\mu_{ТНСД}\mu_{ВНРАС}\frac{r^{П}_{СПКА}(T_д)}{r^{О}_{СПКА}} \end{aligned} \qquad (32)$$

3. Определим интервал значений коэффициента преодоления рубежей противодействия $K_{ПРП}$, который находится в пределах $0 \le K_{ПРП} \le 1$, и определяет относительное число преодоленных рубежей противодействия: 1 – преодолены все рубежи, 0 – не преодолен ни один рубеж. Предполагается, что при реализации атаки нарушитель будет преодолевать требуемое число рубежей противодействия $r_{СПКА}^{ТРП}(T_д)$ за время действия компьютерных атак $T_д$. Тогда требуемый коэффициент преодоления рубежей противодействия будет равен:

$$K_{ПРП}^{ТР}(T_д) = \mu_{уяз}\mu_{ск}\mu_{ТНСД}\mu_{ВНРАС}\frac{r_{СПКА}^{ТРП}(T_д)}{r_{СПКА}^{О}}.$$

4. Получим расчетное соотношение для интенсивности потока компьютерных атак λ_Y, приходящегося на преодоление одного рубежа противодействия:

$$\lambda_Y = \mu_{уяз}\mu_{ск}\mu_{ТНСД}\mu_{ВНРАС}\frac{\nu_Y P_{ПРП} A_Y}{r_{СПКА}^{О}} \qquad (33)$$

5. С учетом расчетного соотношения для интенсивности потока компьютерных атак λ_Y преобразуем формулу (32) для коэффициента преодоления рубежей противодействия $K_{ПРП}$ к следующему виду:

$$K_{ПРП} = \mu_{уяз}\mu_{ск}\mu_{ТНСД}\mu_{ВНРАС}\lambda_Y T_д = \mu_{уяз}\mu_{ск}\mu_{ТНСД}\mu_{ВНРАС}\, T_д / T_{СР} \qquad (32\ а)$$

где $T_{СР}$ – среднее время преодоления одного рубежа компьютерными атаками нарушителя С.

6. Введем допущение о том, что известна функциональная зависимость для коэффициента преодоления рубежа противодействия: $K_{ПРП}(T_д) = f(\nu_Y, P_{ПРП}, A_Y, r_{СПКА}^{О})$, которая позволяет нарушителю С планировать необходимое время воздействия атак $T_д$, прогнозировать число преодоленных рубежей $r_{СПКА}^{П}$, и предъявлять требования к параметрам эффективности компьютерных атак ν_Y, $P_{ПРП}$, A_Y.

7. Выведем расчетное соотношение для коэффициента преодоления рубежей противодействия $K_{ПРП}$ для случая, если параметры эффективности компьютерных атак

принимают различные значения ($v_{Yi}, P_{ПРПi}, A_{Yi}, T_{\partial i}$) в процессе преодоления каждого i-го рубежа противодействия. Тогда обобщенная формула для коэффициента преодоления рубежей противодействия $K_{ПРП}$ (32) с использованием (32 а) примет вид:

$$K_{ПРП}(T_{\partial иа}) = \mu_{уяз}\mu_{ск}\mu_{ТНСД}\mu_{ВНРАС}\frac{\sum_{i=1}^{N_Y} v_{Yi}P_{ПРПi}A_{Yi}T_{\partial i}}{r_{СПКА}^{O}} = \\ = \mu_{уяз}\mu_{ск}\mu_{ТНСД}\mu_{ВНРАС}\frac{r_{СПКА}^{ТРП}(T_{\partial иа})}{r_{СПКА}^{O}}, \quad (32\ б)$$

где $T_{\partial иа}$ – период воздействия компьютерных атак нарушителя С.

Таким образом, метод экспериментальной оценки эффективности компьютерных атак на КВИС базируется на определении значений:

вероятности использования уязвимостей и сканирования параметров КВИС,

вероятности создания точек несанкционированного доступа в КВИС,

вероятности внедрения и распространения атаки,

коэффициента преодоления рубежей противодействия атакам $K_{ПРП}$.

3 Метод экспериментальной оценки эффективности средств противодействия компьютерным атакам на КВИС

Основные этапы метода приведены на рисунке 7. Замысел этого метода состоит в том, что главным критерием оценки является максимальное обнаружение (предупреждение, обнаружение и анализ) компьютерных атак на рубежах противодействия СПКА на требуемом интервале времени противодействия атакам нарушителя.

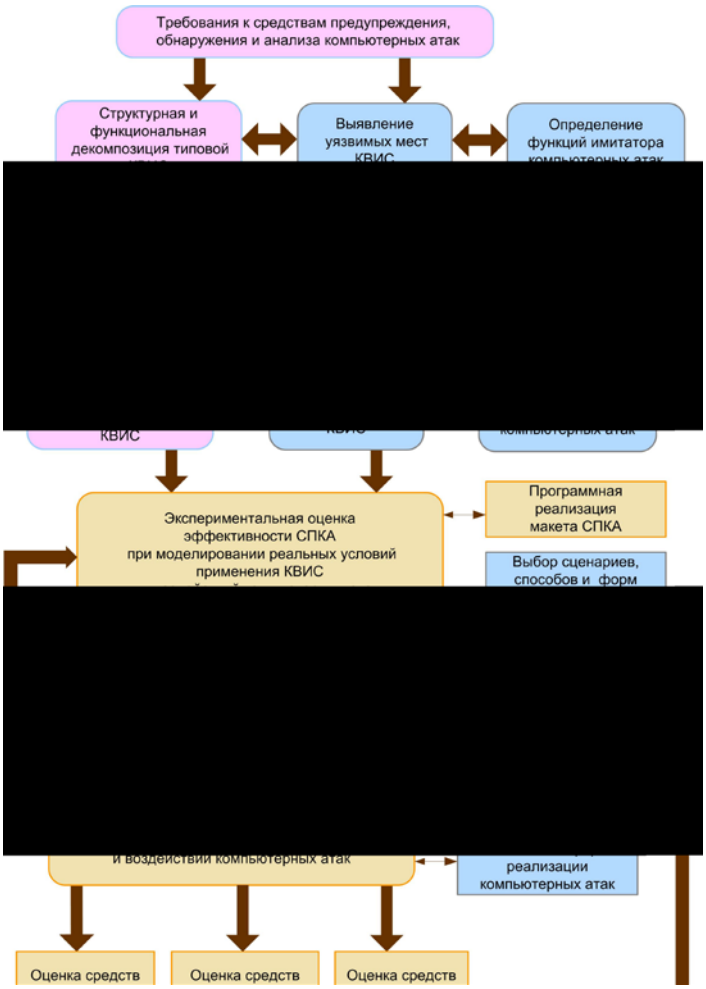


Рисунок 7 – Схема метода экспериментальной оценки эффективности средств противодействия компьютерным атакам на КВИС

Оценка эффективности средств противодействия атакам осуществляется по изменению значений вероятности предупреждения, обнаружения и анализа атак от

времени обнаружения атак. С помощью этой вероятности оценивается комплексное применение компонентов СПКА, средств защиты информации от несанкционированного доступа (СЗИ НСД), защищенность СПО КВИС, антивирусных средств по следующему соотношению:

$$P_{ПОА}(T_{об}) = 1 - \prod_{i=1}^{4} \left(P^{A}_{ykai} \times P^{НСД}_{hkai} \times P^{БИЗКТ}_{hkai} \times P^{B}_{zkai} \right) \qquad (34)$$

где $P_{ПОА}(T_{об})$ – вероятность предупреждения, обнаружения и анализа атак;

P^{A}_{ykai} – вероятность осуществления компьютерной атаки - y на рубеж противодействия - k и элемент КВИС - a;

$P^{НСД}_{hkai}$ – вероятность несанкционированного доступа нарушителя - h к рубежу противодействия - k и элементу КВИС - a;

$P^{БИЗКТ}_{hkai}$ – вероятность несанкционированного доступа нарушителя - h к рубежу противодействия СПО и ОПО - k и элементу КВИС - a;

P^{B}_{zkai} – вероятность воздействия компьютерным вирусом - z на рубеж противодействия - k и элемент КВИС - a.

Исходные положения метода:

1. Рассматривается ситуация двусторонней модели, в которой необходимо определить, насколько эффективно на рубежах противодействия СПКА сторона В («рубеж СПКА») противодействует компьютерным атакам нарушителя С («компьютерная атака»).

2. Коэффициент противодействия компьютерным атакам $K_{ПКА}$ определяется относительным числом не преодоленных (сохраненных) рубежей противодействия путем вычисления отношения $r^{НП}_{СПКА}$ числа не преодоленных рубежей противодействия к $r^{О}_{СПКА}$ общему количеству рубежей: $r^{НП}_{СПКА}(t) / r^{О}_{СПКА}$.

Получение в разработанном методе математических соотношений для определения этого коэффициента производится следующим образом:

1. С целью исследования динамики изменения коэффициента противодействия компьютерным атакам $K_{ПКА}$ на момент времени t используем дифференциальное уравнение (31), описывающее преодоление компьютерными атаками стороны С рубежей противодействия СПКА.

2. На основе введения понятия относительного количества средств противодействия компьютерным атакам, приходящихся на один рубеж $\delta_{П}\pi = \pi_{П} / r_{СПКА}^{НП}$, запишем дифференциальное уравнение для интенсивности противодействия компьютерным атакам стороной В:

$$\frac{da_{Y}(t)}{dt} = -\nu_{ПКА} P_{ПКА} \delta_{П} \pi, \tag{35}$$

где $a_{Y}(t)$ – количество обнаруженных атак на момент времени t,

$\nu_{ПКА}$ – интенсивность противодействия компьютерной атаке,

$P_{ПКА}$ – вероятность противодействия компьютерной атаке.

3. Перейдем к относительным величинам не преодоленного количества рубежей противодействия $x(t) = r_{СПКА}^{НП}(t) / r_{СПКА}^{О}$ стороны В и количества компьютерных атак $y(t) = a_{Y}(t) / A_{Y}$ стороны С. Тогда уравнения (31) и (35) примут вид:

$$\begin{cases} \dfrac{dx(t)}{dt} = -\dfrac{\nu_{Y} P_{ПРП} A_{Y} y(t)}{r_{СПКА}^{О}} = -\lambda_{Y} y(t) \\ \dfrac{dy(t)}{dt} = -\dfrac{\nu_{ПКА} P_{ПКА} \delta \pi_{П}}{A_{Y}} = -\lambda_{ПКА} \\ \exists x(t=0) = 1, \exists y(t=0) = 1 - \text{начальныеусловия}, \end{cases} \tag{36}$$

где λ_{Y} – интенсивность воздействия компьютерных атак, приходящихся на один рубеж противодействия:

$$\lambda_{Y} = \frac{\nu_{Y} P_{ПРП} A_{Y}}{r_{СПКА}^{О}}, \tag{37}$$

$\lambda_{ПКА}$ – интенсивность противодействия компьютерным атакам, приходящимся на одну атаку:

$$\lambda_{ПКА} = \frac{\nu_{ПКА} P_{ПКА} \delta_{П} \pi}{A_{Y}}. \tag{38}$$

4. Проведем решение второго уравнения формулы (36) путем разделения дифференциалов:

$$dy(t) = -\lambda_{\text{Y}} dt\,,$$

интегрирование полученного уравнения дает:

$$y(t) = -\lambda_{\text{Y}} t + K\,,$$

где K – постоянная интегрирования, которая находится из начальных условий: при $t = 0,\ y(t = 0) = 1$.

Тогда искомая величина $y(t)$ будет равна

$$y(t) = 1 - \lambda_{\text{ПКА}} t\,. \qquad (39)$$

5. Перейдем к нахождению величины $x(t)$ – относительного числа не преодоленных рубежей противодействия. Для этого значение $y(t)$ из (39) подставим в первое уравнение (36) и получим:

$$\frac{dx(t)}{dt} = -\lambda_{\text{Y}}(1 - \lambda_{\text{ПКА}} t) = -\lambda_{\text{Y}} + \lambda_{\text{Y}}\lambda_{\text{ПКА}} t\,, \qquad (40)$$

разделяя дифференциалы и интегрируя, получаем:

$$x(t) = -\lambda_{\text{Y}} t + 0{,}5\lambda_{\text{Y}}\lambda_{ПКА} t^2 + K\,,$$

где K – постоянная интегрирования, которая находится из начальных условий при $t = 0, x(t = 0) = 1$.

Тогда искомая величина $x(t)$ будет равна:

$$x(t) = 1 - \lambda_{\text{Y}} t + 0{,}5\lambda_{\text{Y}}\lambda_{ПКА} t^2\,. \qquad (41)$$

6. Получим два выражения для расчета коэффициента противодействия компьютерным атакам путем подстановки значений $\lambda_{\text{У}}, \lambda_{\text{ПКА}}$ из формул (37), (38) в уравнение (41):

$$K_{ПКА}(t) = 1 - \frac{\nu_Y P_Y A_Y}{r^O_{СПКА}} t + 0{,}5 \frac{\nu_Y \nu_{ПКА} P_Y P_{ПКА} \pi_П}{r^O_{СПКА}} t^2, \quad (42)$$

$$K_{ПКА}(t) = x(t) = 1 - \lambda_Y t + 0{,}5 \lambda_Y \lambda_{ПКА} \delta \pi_П t^2. \quad (43)$$

Уравнение (42) позволяет вычислять коэффициент противодействия компьютерным атакам для ситуации, когда воздействует множество атак с интенсивностью $\nu_{\text{У}}$ на совокупность рубежей СПКА, противодействующих с интенсивностью $\nu_{ПКА}$. Формула (43) позволяет производить оценку влияния при воздействии одной компьютерной атаки с интенсивностью $\lambda_{\text{У}}$, которой противодействует один рубеж СПКА с интенсивностью $\lambda_{ПКА}$ на момент времени t.

7. Получение расчетного соотношения для коэффициента противодействия компьютерным атакам с учетом периода времени запаздывания $\tau_{\text{З}}$ на обнаружение компьютерных атак стороной В на основе преобразования уравнения (43) к следующему виду:

$$K_{ПКА}(t) = 1 - \lambda_Y t + 0{,}5 \lambda_Y \lambda_{ПКА} \delta \pi_П (t - \tau_З)^2 \quad (44)$$

Уравнение (44) отражает факт замедления при обнаружении компьютерной атаки стороной В. При условии, что $0 \le t \le \tau_З$ выражения для интенсивности воздействия атак и соответственно для интенсивности противодействия атакам примут вид:

$$a_Y(t - \tau_З) = A_Y,$$
$$\pi_П(t - \tau_З) = 0.$$

Формулы (39) и (44) позволяют оценить влияние периода времени запаздывания $\tau_{\text{З}}$ при обнаружении компьютерных атак на значение коэффициента противодействия

компьютерным атакам с помощью построения зависимостей по этим формулам при значениях $r^{O}_{СПКА}/A_{Y} = \pi_{П}/r^{O}_{СПКА} = 1; \lambda_{Y} = 0{,}1$ (рисунки 8 и 9). На рисунке 8 показано изменение коэффициента противодействия компьютерным атакам при средних значениях $\tau_{З}$. Когда $K_{ПКА}(t) = x(t)$ он изменяется пропорционально t до значения $t = \tau_{З}$. После $t \geq \tau_{З}$, $K_{ПКА}(t) = x(t)$ изменяется в соответствии с формулой (43). В момент $t_{б}$ компьютерная атака стороны С преодолевает один рубеж из семи, а затем и другие рубежи. Для времени $t \geq \tau_{З}$ $y(\Delta t)$ убывает в соответствии с формулой (39). Рисунок 9 иллюстрирует сценарий нарушителя, при котором изменение коэффициента противодействия компьютерным атакам при малой величине задержки $\tau_{З}$ не позволяет нарушителю С преодолеть даже один рубеж противодействия СПКА.

Зависимости на рисунках 8 и 9 наглядно показывают роль оперативности предупреждения, обнаружения и анализа компьютерных атак на рубежах противодействия.

На основе использования формул (42) и (43) имеется возможность оценить влияние $\delta\pi_{П} = \pi_{П}/r^{НП}_{СПКА}$ относительного количества средств противодействия компьютерным атакам приходящихся на один рубеж и $\lambda_{ПКА}$ интенсивности противодействия на изменение значений коэффициента противодействия компьютерным атакам.

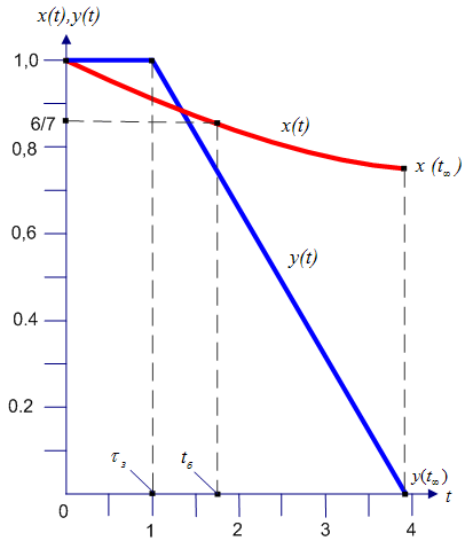


Рисунок 8 – Зависимость изменения коэффициента противодействия компьютерным атакам при средних значениях $\tau_{З}$ периода времени запаздывания на обнаружение атак

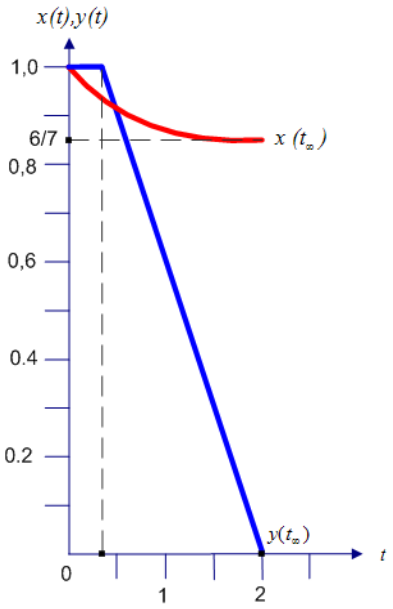


Рисунок 9 – Зависимость изменения коэффициента противодействия компьютерным атакам при малой величине $\tau_З$ периода времени запаздывания на обнаружение атак

На рисунке 10 показана зависимость изменения коэффициента противодействия компьютерным атакам при различных значениях $\delta\pi_{\text{В}}$ относительного количества средств противодействия компьютерным атакам приходящихся на один рубеж.

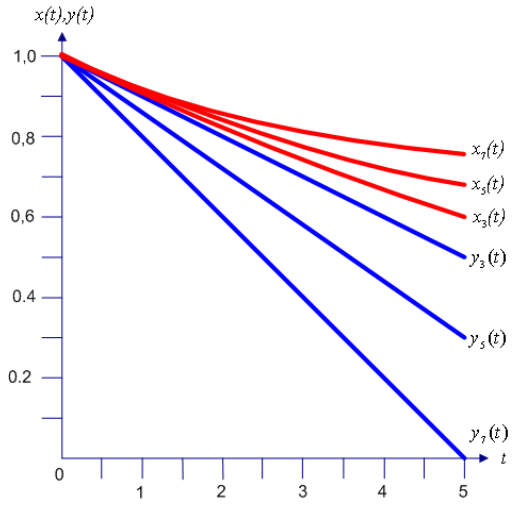


Рисунок 10 – Зависимость изменения коэффициента противодействия компьютерным атакам при различных значениях $\delta\pi_{\text{В}}$ относительного количества средств противодействия компьютерным атакам приходящихся на один рубеж

На рисунке 10 введены следующие обозначения:

$x_7(t), y_7(t)$ – изменение $x(t), y(t)$ при использовании 7 рубежей противодействия компьютерным атакам;

$x_5(t), y_5(t)$ – изменение $x(t), y(t)$ при использовании только 5 рубежей противодействия компьютерным атакам;

$x_3(t), y_3(t)$ – изменение $x(t), y(t)$ при использовании только 3 рубежей противодействия компьютерным атакам.

Анализ рисунка 10 показывает, что при относительном числе средств противодействия компьютерным атакам приходящихся на один рубеж не равном единице $\delta\pi_{П} = \pi_{П} / r_{СПКА}^{НП} \neq 1$ и количестве рубежей противодействия равном 7 величина $\delta\pi_{П}$ будет меняться с дискретностью 1/7 в интервале от 1 до 0.

Рисунок 10 наглядно демонстрирует необходимость противодействия компьютерным атакам на 7 рубежах противодействия СПКА. С уменьшением величины $\delta\pi_{П}$ число обнаруженных компьютерных атак возрастает $y_3(t=5) > y_7(t=5)$, а относительное число не преодоленных рубежей у стороны В уменьшается $x_3(t=5) < x_7(t=5)$.

Таким образом, метод экспериментальной оценки эффективности средств противодействия компьютерным атакам на КВИС основан на оценке вероятности предупреждения, обнаружения и анализа атак и коэффициента противодействия компьютерным атакам на совокупности рубежей противодействия СПКА. Эти показатели позволяют оценить возможности комплексного противодействия атакам на базе компонентов СПКА, СЗИ НСД и антивирусных средств, а также по результатам экспериментальных исследований и оценки коэффициента противодействия атакам найти значения для числа средств противодействия и времени обнаружения атак на каждом рубеже.

4 МЕТОД ОЦЕНКИ ЭФФЕКТИВНОСТИ АКТИВНОГО ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ НА КРИТИЧЕСКИ ВАЖНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Метод оценки эффективности активного противодействия компьютерным атакам на КВИС включает в свой состав:

1. Разработку сетевого графика противодействия компьютерным атакам.
2. Расчет вероятности отражения компьютерной атаки.
3. Выбор средств активного противодействия на основе игровых методов.
4. Расчет вероятности достижения информационного превосходства стороны В (активного противодействия компьютерным атакам) над стороной С (реализации компьютерных атак нарушителя).
5. Расчет коэффициента информационного превосходства.

Сетевой график противодействия компьютерным атакам на КВИС необходим для осуществления рационального плана активного противодействия компьютерным атакам и позволяет:

– определить порядок применения средств противодействия атакам,

– реализовать активное противодействие атакам в кратчайшие сроки,

– минимизировать затраты вычислительного ресурса КВИС и ущерба для устойчивого выполнения ТЦУ.

Разработка сетевого графика противодействия компьютерным атакам осуществляется в соответствии с графиком планирования применения средств противодействия компьютерным атакам (рисунок 11) и формулами (45):

$$M_{ПДi} = \frac{T_{\min} + 4T_{нв} + T_{\max}}{6},\ \sigma_i = \frac{T_{\max} - T_{\min}}{6},\ P_{СБППД} = 2\Phi\left(\frac{T_з - T_{пр}(i)}{\sqrt{\sum \sigma_i^2}}\right), \qquad (45)$$

где $M_{ПДi}$ – математическое ожидание продолжительности этапов (i) противодействия атакам,

$T_{\min}$ – период времени противодействия атакам при благоприятных условиях,

$T_{НВ}$ – наиболее вероятный период времени,

$T_{\max}$ – период времени противодействия атакам при неблагоприятных условиях,

σ_i – среднеквадратическая ошибка в определении времени этапа,

$P_{СБ\,ПД\,i}$ – вероятность наступления событий противодействия атакам,

Φ – функция Лапласа [1],

$T_з$ – заданный период наступления события противодействия атакам,

$T_{пр}$ – период наступления i-го события предупреждения атак.

Контроль выполнения графика (рисунок 11) осуществляется по событиям в моменты времени $T_{вi}$, когда проверяется соответствие критических показателей устойчивости функционирования КВИС по промежуточным значениям параметров противодействия.

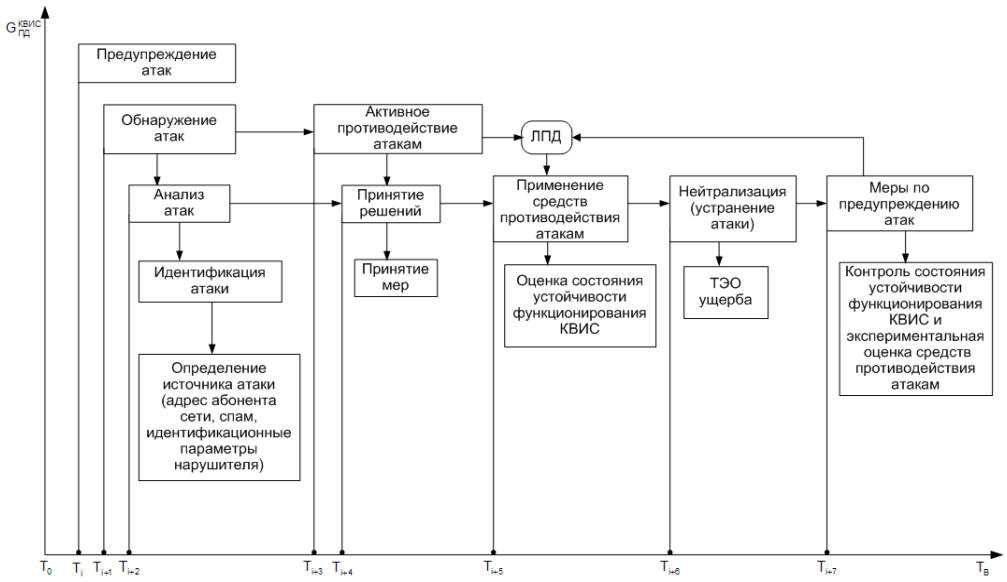


Рисунок 11 – График планирования применения средств противодействия компьютерным атакам на КВИС

Расчет вероятности отражения компьютерной атаки на КВИС проводится следующим образом:

$$P_{ОТР} = 1 - \left(1 - \frac{P_{УП} P_{вд}(A_K)}{M_A}\right)^{A_K}; \qquad (46)$$

где $P_{УП}$ – вероятность успешного активного противодействия атаке,

$P_{вд}$ – вероятность воздействия атаки нарушителя,

A_K – общее количество атак,

M_A – математическое ожидание числа атак, необходимых для преодоления рубежей средств противодействия.

Ограничения на проведение приближенных расчетов вероятности отражения компьютерной атаки на КВИС имеют вид:

– атаки независимы;

– одинаковая вероятность реализации атаки;

– показательный закон распределения $P_{вд}$;

– биномиальный закон распределения $P_{УП}$.

Критерии требуемого уровня противодействия компьютерным атакам на КВИС оцениваются по значениям вероятностей таблицы 1.

Оценка эффективности противодействия компьютерным атакам на основе игровых методов [1, 4, 33] осуществляется исходя из предположения наличия конфликтующих сторон (рассмотрена двусторонняя игра – сторона В противодействует компьютерным атакам на КВИС, а сторона С реализует воздействия компьютерных атак нарушителя на КВИС) и проводится следующим образом.

Первоначально в соответствии с таблицей 2 осуществляется подготовка исходных данных игры – выбор размера матрицы игры $m \times n$, при которой сторона В (строки матрицы) имеет m-стратегий (применения функций СПКА), а сторона С (столбцы матрицы) – n-стратегий (применения средств реализации различных типов компьютерных атак).

Стратегия определяет выбор варианта действий сторонами В и С в зависимости от успешных или неудачных результатов, соответственно, противодействия атакам или реализации атак на КВИС. Оптимальной стратегией считается та, которая при многократном повторении игры обеспечивает стороне В максимально возможный средний выигрыш. Выигрыш стороны В определяется как M^{O}_{Amn} математическое ожидание количества отраженных атак нарушителя и является результатом игры. Рассматривается двусторонняя игра (игра 2×2) с нулевой суммой когда сторона В выигрывает столько в противодействии атакам, сколько проигрывает сторона С в реализации атак на КВИС.

Таблица 1 – Критерии требуемого уровня противодействия компьютерным атакам на КВИС

№ п/п	Вероятность наступления события противодействия атаками	Значение вероятности	Уровень противодействия компьютерным атакам
1.	P_{yn}^1 (невозможное событие)	0	Нет противодействия
2.	P_{yn}^2 (маловероятное событие)	0.2	Низкий уровень противодействия
3.	P_{yn}^3 (событие вероятно наполовину)	0.5	
4.	P_{yn}^4 (событие вполне вероятно)	0.7-0.8	Средний уровень противодействия
5.	P_{yn}^5 (вероятность события высокая)	0.9	Высокий уровень противодействия
6.	P_{yn}^6 (вероятность события очень высокая)	0.95	Требуемый уровень противодействия
7.	P_{yn}^7 (событие произойдет наверняка)	0.99	

Таблица 2 – Выбор размера матрицы игры $m \times n$ в соответствии с функциями СПКА и типами компьютерных атак нарушителя

Функции СПКА стороны **B** (F_{ci})	Тип атаки нарушителя **C** (B_{yj})			maximin α_i
	B_{y1}	…	B_{yn}	
F_{c1} … F_{cm}	M_{A11}^O … M_{Am1}^O	… … …	M_{A1n}^O … M_{Amn}^O	α_1 … α_m
minmax β_j	β_1	…	β_n	

В таблице 2 использованы обозначения: maximinα_i – нижняя цена игры, minmaxβ_j – верхняя цена игры.

Если $\nu = \alpha_i = \beta_j$, то в матрице игры (таблицы 2) имеется седловая точка, которой соответствуют стратегии сторон B и C (максимальное значение в столбце матрицы и минимальное значение в строке матрицы). Тогда ν является общим значением верхней и нижней ценой игры и называется ценой игры. Графическая интерпретация для матрицы игры 2×2 имеет вид, приведенный на рисунке 12.

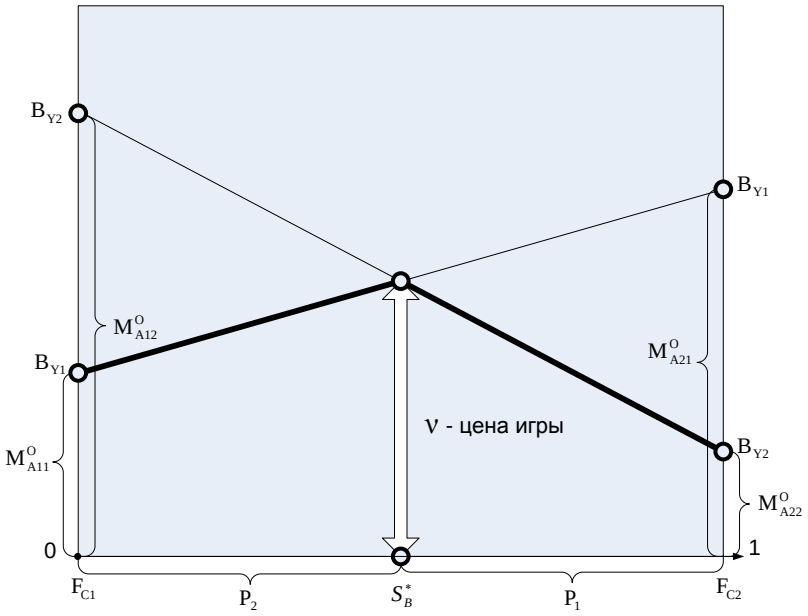


Рисунок 12 – Графическая интерпретация для матрицы игры 2x2

С использованием графической интерпретации рисунка 12 проводится оценка игры в конфликтной ситуации, при которой результат действий стороны В зависит от предполагаемых действий стороны С (решения принимаются экспертным путем исходя из существующей модели нарушителя, аналитической информации, имеющегося опыта) по следующим соотношениям:

а) определения стратегий сторон В и С:

$S_c^* = (p_1,...,p_m), S_A^* = (q_1,...,q_n)$;

где $(p_1,...,p_m)$ – вероятности применения стороной В стратегий $F_{ci},...,\mathrm{F_{cm}}$,

$(q_1,...,q_n)$ – вероятности применения стороной С стратегий $B_{yj},...,B_{yn}$;

б) вычисления вероятностей применения стратегий сторонами В и С на основе обобщенных формул для игры $m \times n$:

$$p_m = \frac{M^O_{Am,n+1} - M^O_{Am,n\text{-}1}}{M^O_{Am,n} + ... + M^O_{Am+1,n+1} - M^O_{Am-1,n+1} - ... - M^O_{Am,n\text{-}1}}; \quad (47)$$

$$q_m = \frac{M_{m,n+1} - M_{m-1,n}}{M^O_{Am,n} + ... + M^O_{Am+1,n+1} - M^O_{Am-1,n+1} - ... - M^O_{Am,n\text{-}1}}; \quad (48)$$

в) расчета цены игры на основе обобщенной формулы для игры $m \times n$:

$$\nu = \frac{M^{O}_{Am+1,n+1} M^{O}_{Am-1,n-1} - M^{O}_{Am-1,n+1} M^{O}_{Am+1,n-1}}{M^{O}_{Am,n} + \ldots + M^{O}_{Am+1,n+1} - M_{Am-1,n+1} - \ldots - M^{O}_{Am,n-1}} \quad (49)$$

Расчет вероятности достижения информационного превосходства стороны В (активного противодействия компьютерным атакам) над стороной С (реализации компьютерных атак нарушителя на КВИС) осуществляется в соответствии с графической интерпретацией двусторонней модели активного противодействия компьютерным атакам в виде последовательностей событий «воздействие атаки – противодействие атаке» (рисунок 13).

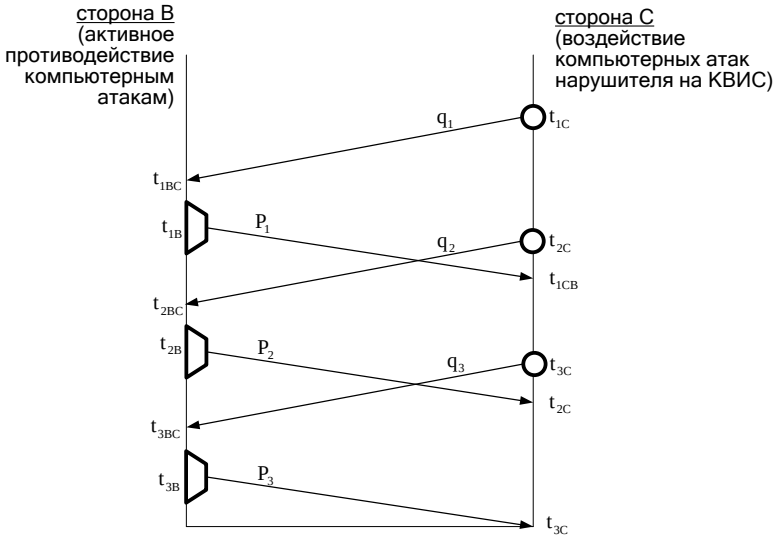


Рисунок 13 – Графическая интерпретация двусторонней модели противодействия компьютерным атакам для расчета вероятности достижения информационного превосходства

Предполагается, что известны средства реализации компьютерных атак стороны С (при использовании имитатора атак), средства активного противодействия атакам стороны В и заданы моменты времени:

t_{1C}, t_{2C}, t_{3C} – моменты времени реализации компьютерных атак нарушителя на КВИС (сторона С);

t_{1B}, t_{2B}, t_{3B} – моменты времени применения средств активного противодействия компьютерным атакам (сторона В) путем воздействия на источники атак;

$t_{1BC}, t_{2BC}, t_{3BC}$ – период времени для подготовки средств активного противодействия атакам (предупреждение, обнаружение, анализ атак) нарушителя С;

$t_{1CB}, t_{2CB}, t_{3CB}$ – период времени для подготовки средств реализации компьютерных атак для воздействия на сторону В.

Тогда вероятность завоевания информационного превосходства стороной В над стороной С на основе использования материалов [1] рассчитывается по формуле полной вероятности следующим образом:

$$P_{BC} = P_1 + (1-P_1)(1-q_1)P_2 + (1-P_1)(1-P_2)(1-q_1)(1-q_2)(1-q_3)P_3; \quad (50)$$

где: P_1, P_2, P_3 – вероятности реализации средствами активного противодействия стороной В воздействия на источники атак стороны С;

q_1, q_2, q_3 – вероятности успешного воздействия стороны С компьютерными атаками на КВИС стороны В.

Нахождение математических соотношений для расчета коэффициента информационного превосходства состоит в следующем.

Предположим, что имеется двусторонняя модель, в которой сторона С является «источником компьютерных атак», а сторона В реализует «активное противодействие компьютерным атакам» с целью их устранения (нейтрализации по результатам работы компонентов предупреждения, обнаружения и анализа компьютерных атак в СПКА). Сторона С обладает возможностью воздействовать компьютерными атаками на сторону В с ν_Y интенсивностью осуществления потенциальных угроз реализации компьютерных атак, $P_{во}$ вероятностью реализации воздействия компьютерной атакой и имеет ресурс реализации атак в количестве A_Y. Сторона В противодействует атакам с $\nu_{АП}$ интенсивностью активного противодействия, $P_{АП}$ вероятностью наступления события активного противодействия атакам с помощью средств активного противодействия атакам в количестве $Z_{АП}$. Устранение стороной В источников компьютерных атак стороны С дает возможность завоевать информационное превосходство стороны В над стороной С при функционировании КВИС в условиях воздействия компьютерных атак и противодействия им.

Требуется определить коэффициент информационного превосходства $K_{ИП}$ стороны В над стороной С в следующей последовательности:

1. Опишем процесс активного противодействия стороны В компьютерным атакам стороны С на основе использования математического аппарата, близкого к дифференциальным уравнениям Ланчестера [1, 2, 36]. В методе экспериментальной оценки эффективности активного противодействия компьютерным атакам эти дифференциальные уравнения доработаны и представлены в виде:

$$\begin{aligned} \frac{dZ_{АП}(t)}{dt} &= -\nu_Y P_{ВД} A_Y(t), \\ \frac{dA_Y(t)}{dt} &= -\nu_{АП} P_{АП} Z_{АП}(t). \end{aligned} \qquad (51)$$

2. Получим математические соотношения для получения коэффициента информационного превосходства стороны В основано на преобразовании уравнений (51) следующим образом:

а) разделим левые и правые части первого уравнения на левые и правые части второго уравнения формулы (51):

$$\frac{dZ_{АП}(t)}{dA_Y(t)} = \frac{\nu_Y P_{ВД} A_Y(t)}{\nu_{АП} P_{АП} Z_{АП}(t)};$$

б) проведем диагональное перемножение соответствующих числителей и знаменателей полученного уравнения и интегрирование левых и правых частей этого уравнения:

$$\nu_{АП} P_{АП} \int Z_{АП}(t) dZ_{АП} = \nu_Y P_{ВД} \int A_Y(t) dA_Y,$$

и получим уравнение, разность между двумя составляющими которого является постоянной величиной

$$2\nu_{АП} P_{АП} Z^2_{АП}(t) - \nu_Y P_{ВД} A^2_Y(t) = const;$$

в) преобразуем последнее уравнение при изменяемых во времени параметрах $Z_{АП}(t)$ и $A_Y(t)$ с учетом того, что левая часть уравнения сохраняется неизменной в

любой момент времени t (также и по отношению ко времени $t=0$), к следующему виду:

$$2\nu_{АП}P_{АП}Z^2_{АП}(t)-\nu_{У}P_{ВД}A^2_{У}(t)=2\nu_{АП}P_{АП}Z^2_{АП}(t=0)-\nu_{У}P_{ВД}A^2_{У}(t=0); \quad (52)$$

г) определим неравенство информационного превосходства стороны В, вытекающее из правой части уравнения (52):

$$2\nu_{АП}P_{АП}Z^2_{АП}(t=0)-\nu_{У}P_{ВД}A^2_{У}(t=0)>0;$$

д) приведем последнее неравенство к соотношению, которое отражает информационное превосходство стороны В:

$$\frac{2\nu_{АП}P_{АП}Z^2_{АП}(t=0)}{\nu_{У}P_{ВД}A^2_{У}(t=0)}>1. \quad (53)$$

3. Выведем расчетное соотношение для коэффициента информационного превосходства извлекая квадратный корень из неравенства (4.53):

$$K_{ИП}=\sqrt{2}\cdot\left(\frac{Z_{АП}}{A_{У}}\right)\cdot\sqrt{\frac{\nu_{АП}}{\nu_{У}}}\cdot\sqrt{\frac{P_{АП}}{P_{ВД}}}=\sqrt{2}K_1K_2K_3. \quad (54)$$

Коэффициент информационного превосходства $K_{ИП}$ в соответствии с уравнением (53) стороны В при активном противодействии компьютерным атакам стороны С принимает три множества значений:

$K_{ИП}>1$ – достигается информационное превосходство стороны В;

$K_{ИП}<1$ – информационное превосходство стороны В не достигнуто;

$K_{ИП}=1$ – имеет место равновесие между потенциальными источниками реализации атак стороны С и средствами активного противодействия атакам стороны В.

Формула (54) представляет собой математическое выражение для получения комплексного коэффициента информационного превосходства при мультипликативной свертке локальных коэффициентов информационного превосходства $K_j\left(j=\overline{1,3}\right)$,

характеризующих специфику взаимосвязи средств активного противодействия атакам и ресурса реализации атак нарушителя.

При этом каждый локальный коэффициент информационного превосходства характеризует:

а) соотношение количества средств активного противодействия стороны В и ресурса реализации атак стороны С:

$$K_1 = \left(\frac{Z_{\text{АП}}}{A_{\text{У}}} \right);$$

б) соотношение показателей интенсивности активного противодействия стороны В и интенсивности источника атак стороны С:

$$K_2 = \sqrt{\frac{\nu_{АП}}{\nu_{\text{У}}}};$$

в) соотношение вероятности активного противодействия атакам стороной В и вероятности воздействия атак стороны С:

$$K_3 = \sqrt{\frac{P_{АП}}{P_{ВД}}}.$$

Таким образом, метод экспериментальной оценки эффективности активного противодействия компьютерным атакам на КВИС основан на сетевом графике противодействия компьютерным атакам, расчете вероятности отражения компьютерной атаки, выборе рациональных средств активного противодействия на основе игровых методов, расчете вероятности достижения информационного превосходства стороны В (активного противодействия компьютерным атакам) над стороной С (реализации компьютерных атак нарушителя), а также определении значений коэффициента информационного превосходства $K_{ИП}$.

5 МЕТОД ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СЕГМЕНТОВ

Сущность метода заключается в экспериментальной оценке вероятности устойчивости функционирования КВИС, анализе способности сегмента восстанавливать устойчивое состояние после воздействия компьютерных атак и оценке коэффициента устойчивости функционирования сегмента.

Исходные положения:

1. Воздействия компьютерных атак на КВИС могут снизить устойчивость функционирования КВИС за счет нарушения процессов сбора, обработки и передачи информации.
2. Эффективное противодействие компьютерным атакам и восстановление заданных параметров и функций КВИС позволяет перевести систему в устойчивое состояние, соответствующее средней эффективности выполнения ТЦУ.
3. Высокая эффективность выполнения ТЦУ, соответствующая требуемому значению вероятности устойчивого функционирования КВИС, равна 0,95 («номинальное значение»).
4. Средняя эффективность выполнения ТЦУ соответствует значению вероятности устойчивости функционирования КВИС – 0,8 («реальное значение»).

Для обеспечения устойчивости функционирования КВИС с высокой и средней эффективностью выполнения ТЦУ при воздействии компьютерных атак с λ_Y интенсивностью необходима соответственно высокая или средняя эффективность противодействия атакам на $r_{СПОКА}^{O}$ рубежах СПКА.

Восстановление устойчивости функционирования КВИС осуществляется на основе:

1. Применения и выбора более эффективных средств предупреждения, обнаружения и анализа компьютерных атак и активного противодействия атакам компонентами СПКА (максимальное обнаружение и нейтрализация атак).
2. Комплексного применения СЗИ НСД, включая средства администрирования информационной безопасности, сетевые анализаторы трафика сети КВИС,

антивирусные средства, межсетевые экраны, средства защиты информации, встроенные в ОС и СУБД (максимальное выявление аномальных событий в КВИС и попыток НСД).

3. Восстановления динамически регулируемых параметров КВИС (СПО, ОС, СУБД, структур данных).
4. Устранения уязвимостей КВИС (максимальное обновление программного обеспечения с возможными точками несанкционированного доступа, минимизация привилегированных функций программ, устранение ошибок в программном обеспечении).
5. Уточнения исходных данных о сценариях и характеристиках средств реализации атак нарушителя (уточнение базы данных атак СПКА).

При экспериментальной оценке устойчивости функционирования КВИС на стендовом полигоне отрабатываются логические цепочки «воздействие компьютерной атаки – реакция КВИС и СПКА – восстановление устойчивости функционирования КВИС». Необходимым условием восстановления устойчивости функционирования КВИС является способность КВИС возвращаться в состояние, которое близко к исходному состоянию после воздействия компьютерных атак. Достаточное условие восстановления устойчивости функционирования КВИС определяется способностью сегмента поддерживать в реальных условиях применения значение вероятности устойчивости функционирования КВИС на уровне 0,8.

В ходе экспериментальных исследований оценка вероятности устойчивости функционирования КВИС при выполнении ТЦУ в условиях воздействия компьютерных атак, противодействия им и динамического восстановления КВИС вычисляется по эмпирической формуле:

$$P_{УФ} = \prod_{i=1}^{N_Э} \left[1 - P_{УФ}^{тр}\left(1 - P_{УФi}^{нш} P_{УФi}^{вс}\right)\right], \qquad (55)$$

где $P_{УФ}^{тр}$ – требуемое значение вероятности устойчивости функционирования КВИС равное 0.95;

$P_{УФi}^{нш}$ – вероятность нарушения устойчивости функционирования КВИС при воздействии компьютерных атак;

$P_{УФi}^{вс}$ – вероятность восстановления устойчивости функционирования КВИС средствами СПКА и настройкой динамических параметров КВИС (номинальное значение $P_{УФ}^{вс} = 0.8$).

Контроль экспериментального значения $P_{УФ}^{*}$ вероятности устойчивости функционирования КВИС проводится с помощью неравенства:

$$P_{УФ}^{*} \geq P_{УФ}^{тр} \tag{56}$$

Максимальное значение вероятности устойчивости функционирования КВИС будет обеспечена, если при заданном множестве компьютерных атак нарушителя и реализованных средствах противодействия им практически каждая атака будет обнаружена и нейтрализована (блокирована или направлена на ложный информационный объект) компонентами СПКА и будет осуществлена реконфигурация КВИС для восстановления устойчивости выполнения технологических операций ТЦУ.

Оценка степени влияния средств восстановления КВИС на повышение значений вероятности устойчивости функционирования и анализ степени снижения этой вероятности вследствие воздействия компьютерных атак проводится с использованием весовых коэффициентов по неравенствам:

$$\begin{cases} 1 \geq \prod_{j=1}^{K_{\Pi}} \left(P_{УФ} + \alpha_{\Pi j}\right) \geq 0.7, \\ 1 \geq \prod_{i=1}^{A_{У}} \left(P_{УФ} - \beta_{Ci}\right) \geq 0.5, \\ \alpha_{\Pi j}, \beta_{C\,i} = \{0.15,\ldots,0.45\}, \end{cases} \tag{57}$$

где $\alpha_{\Pi j}$ – весовые коэффициенты повышения устойчивости функционирования, определяемые как:

$\alpha_{П1}$ – весовой коэффициент регулирования параметров СПКА;

$\alpha_{П2}$ – весовой коэффициент регулирования параметров СЗИ НСД;

$\alpha_{П3}$ – весовой коэффициент динамически регулируемых параметров КВИС;

$\alpha_{П4}$ – весовой коэффициент устранения уязвимостей КВИС;

$\alpha_{П5}$ – весовой коэффициент полноты и достаточности исходных данных об информационных акциях нарушителя;

$\beta_{Сi}$ – весовые коэффициенты снижения устойчивости функционирования за счет воздействия компьютерных атак, выбираемые из множества:

$\beta_{С1}$ – весовой коэффициент компьютерной атаки типа «ложная информация»;

$\beta_{С2}$ – весовой коэффициент компьютерной атаки типа «функциональное поражение»;

$\beta_{С3}$ – весовой коэффициент компьютерной атаки типа «разрыв соединения»;

K_p – количество регулируемых параметров СПКА, КВИС, СЗИ НСД;

A_Y – количество компьютерных атак.

В теории устойчивости технических систем, основы которой были сформированы Ляпуновым А.М. и А. Пуанкаре, используется ряд критериев оценки устойчивости состоянии равновесия систем за счет использования обратной связи для регулирования её параметров [3, 13, 31, 34]. Эти критерии основаны на составлении таблицы коэффициентов характеристического уравнения или системы дифференциальных уравнений и исследовании их по одному из критериев устойчивости: Рауса-Гурвица, Найквиста, Михайлова.

При оценке устойчивости функционирования КВИС вводится допущение о том, что если состояние равновесия КВИС асимптотически устойчиво S_t, то при воздействии произвольных компьютерных атак A_t на незначительном интервале времени действия атаки $T_д << T_{ТЦУ}$, отклонения регулируемых параметров будут малы по величине K_p, и таким образом будет обеспечена устойчивость функционирования КВИС в условиях воздействия атак.

Кроме того, для получения количественных оценок устойчивости функционирования КВИС считаем, что на произвольном интервале времени выполнения ТЦУ сегмент является линейной системой. В соответствии с теорией Ляпунова А.М. оценки устойчивости линейных систем можно использовать для оценки нелинейных систем в соответствии с правилом: «если состояние равновесия линеаризованной системы асимптотически устойчиво, то состояние равновесия

нелинейной системы также асимптотически устойчиво; если состояние равновесия линеаризованной системы неустойчиво, то неустойчиво и состояние равновесия нелинейной системы» [35].

Наибольшее практическое применение для оценки устойчивости функционирования современных автоматизированных систем нашел критерий Рауса-Гурвица [13, 34].

Отклонения значений регулируемых параметров устойчивости функционирования КВИС в результате воздействия компьютерных атак должны быть компенсированы средствами противодействия компьютерным атакам. Средства мониторинга устойчивости функционирования КВИС и предупреждения компьютерных атак должны максимально ограничивать входные воздействия на информационно-вычислительный процесс в системе от источников компьютерных атак нарушителя.

Коэффициент устойчивости функционирования КВИС характеризует способность сегмента восстанавливать свои функции полностью или близко к штатному режиму работы после воздействия компьютерных атак. Восстановление устойчивости функционирования КВИС реализуется на основе противодействия атакам средствами СПКА, СЗИ и путем динамической настройки параметров и реконфигурации структуры КВИС. Результатом восстановления устойчивости функционирования КВИС является выполнение функций сегментом в штатном режиме. Штатное функционирование КВИС определяется количеством произведенных функций и требуемым объемом технологических операций $V_{ОП}$ по сбору, хранению, обработке и передаче информации при осуществлении ТЦУ за установленный интервал времени $T_{ТЦУ}$.

Математические выражения для вычисления коэффициента устойчивости функционирования КВИС имеют вид:

$$K_{УФ} = \frac{\sum_{i=1}^{m} \overline{\lambda^{B}_{ОПi}} F^{B}_{КВИСi}}{\sum_{i=1}^{m} \overline{\lambda^{B}_{ОПi}} F^{O}_{КВИСi}}, \qquad (61)$$

где $\overline{\lambda_{ОПi}^{О}} = \frac{V_{ОП\,i}}{T_{ТЦУ\,i}}$ – интенсивность выполнения КВИС технологических операций по сбору, обработке и передаче измерительной информации в штатном режиме ТЦУ;

$\overline{\lambda_{ОПi}^{В}} = \frac{V_{ОПi}^{В}}{T_{ТЦУ} - T_{УФ} + T_{М} + T_{В}}$ – интенсивность выполнения КВИС технологических операций в режиме восстановления устойчивости функционирования;

$T_{УФ}$ – период времени устойчивого функционирования КВИС;

$T_{М}$ – время мониторинга устойчивости функционирования КВИС;

$T_{В}$ – время восстановления устойчивости функционирования КВИС.

Оценка значения коэффициента устойчивости функционирования КВИС $\Delta K_{УФ}$ по отклонению его от требуемого значения $\Delta K_{УФ}^{ТР}$ при экспериментальных исследованиях на стендовом полигоне осуществляется по формуле:

$$\Delta K_{УФ} = \left[K_{УФШ} - K_{УФН} + \left(1 - K_{УФВ}\right)\right] \geq \Delta K_{УФ}^{ТР}, \qquad (62)$$

где $K_{УФШ}$ – коэффициент устойчивости функционирования КВИС в штатном режиме;

$K_{УФН}$ – коэффициент устойчивости функционирования КВИС в нештатном режиме;

$K_{УФВ}$ – коэффициент устойчивости функционирования КВИС после восстановления КВИС в состояние, которое близко к исходному.

Коэффициент показывает степень отклонения управляющих (выходных) параметров КВИС от заданных значений при искажении внутренних параметров системы вследствие того, что было воздействие атак и в системе недостаточно реализованных функций по компенсации этих воздействий (динамическому восстановлению устойчивости функционирования КВИС по контрольным точкам выполнения ТЦУ). Чем выше значение коэффициента устойчивости функционирования, тем более устойчивая работа системы в условиях воздействия атак, и чем ниже значение коэффициента, тем меньше способность системы восстановить свои параметры до состояния близкого к состоянию устойчивости функционирования КВИС.

6 МЕТОДИКА ОЦЕНКИ УЩЕРБА ОТ ВОЗДЕЙСТВИЯ КОМПЬЮТЕРНЫХ АТАК НА КРИТИЧЕСКИ ВАЖНЫЕ ИНФОРМАЦИОННЫЕ СЕГМЕНТЫ

Методика оценки ущерба от воздействия компьютерных атак на КВИС заключается в согласованном проведении математического и имитационного моделирования, экспертных исследований последствий от вторжения атак в КВИС в соответствии с рейтингами нарушения устойчивости функционирования и множеством параметров информационного ущерба. Оценка ущерба от воздействия компьютерных атак на КВИС ограничена ущербом, нанесенным информации и программному обеспечению КВИС (т.е. информационным ущербом КВИС).

Под информационным ущербом КВИС будем понимать негативное изменение информационного ресурса, приводящее к невыполнению целевых задач КВИС, нарушению выполнения ТЦУ, принятию неблагоприятных решений, нарушению функций или блокированию управления КВИС и ведущее к увеличению затрат на достижение цели или большим материальным потерям.

Информационный ущерб заключается в нарушении конфиденциальности, целостности и доступности информации, что проявляется следующим образом:

- нарушение конфиденциальности информации в КВИС (потеря ее ценности);
- разрушение информационного ресурса КВИС (полная или частичная потеря целостности информации, резервных копий, нарушение информационных таблиц специализированных баз и хранилищ данных);
- недоступность информационного ресурса КВИС (невозможность доступа или недоступность в течение определенного периода времени – «отказ в обслуживании»);
- искажение информационного ресурса при сборе и передаче данных удаленному абоненту в территориально-распределенной вычислительной сети КВИС;
- подготовка неверных управляющих воздействий на основе «ложной» информации;
- нарушение установленных регламентов выполнения ТЦУ в структуре КВИС;
- нарушение устойчивости функционирования КВИС, приводящее к потере

управляемости и «функциональному поражению» КВИС»;

– перегрузка абонентов неактуальной информацией – «спамом».

Показатели оценки информационного ущерба представлены в таблице 3.

Обобщенными критериями оценки информационного ущерба КВИС могут быть следующие:

– ущерб национальной безопасности;
– ущерб, связанный с нарушением требований действующего законодательства;
– ущерб, который привел к финансовым затратам от потери ценности информации;
– ущерб, приведший к финансовым потерям, связанным с восстановлением информационных ресурсов КВИС;
– ущерб, связанный с дезорганизацией процессов функционирования КВИС и не выполнением ТЦУ.

Таблица 3 – Показатели оценки информационного ущерба

№ п/п	Показатель информационного ущерба	Определение показателя информационного ущерба
1.	$V_{н}$	Объем нарушенной, искаженной и разрушенной информации (нарушение конфиденциальности, целостности и доступности информации)
2.	$V_{ПО}$	Объем нарушенного, искаженного и разрушенного общего и специального программного обеспечения КВИС
3.	$N_{АРМ}$	Количество выведенных из строя АРМ КВИС
4.	$N_{срв}$	Количество выведенных из строя серверов баз данных КВИС
5.	$N_{кс}$	Количество выведенных из строя каналов связи, цифрового коммуникационного оборудования и протоколов передачи данных КВИС
6.	K_{YA}	Количество воздействий компьютерных атак
7.	$K_{аб}$	Количество воздействий на абонентов КВИС, подключенных к информационным ресурсам сегмента
8.	$K_{взл}$	Количество попыток взлома средств защиты доступа к информационным ресурсам КВИС
9.	$T_{в\text{КВИС}}$	Время восстановления КВИС
10.	$T_{в\text{ЛВС}}$	Время восстановления ЛВС КВИС

Оценка информационного ущерба КВИС осуществляется по пяти бальной шкале, соответствующей степени выполнения ТЦУ и уровню угроз воздействия компьютерных атак [15, 16, 27]:

5 – ущерб максимальный, восстановление КВИС требует существенных материальных затрат и времени на восстановление превышающее годовое техническое обслуживание;

4 – ущерб значительный, время восстановления КВИС превышает заданное и КВИС не выполняет ТЦУ более суток;

3 – ущерб средний, то есть произошел срыв регламентов выполнения ТЦУ, но устойчивость функционирования восстановлена менее чем за 1 час;

2 – ущерб минимальный, то есть восстановление характеристик КВИС менее чем за 5 минут не привело к срыву ТЦУ;

1 – ущерб устойчивости функционирования не нанесен.

При определении информационного ущерба КВИС оценка производится по совокупности показателей ущерба КВИС (таблица 3). Ущерб, связанный со срывом ТЦУ оценивается по интервалу времени восстановления штатного функционирования КВИС.

В интересах определения значения шкалы ущерба используется детальное описание структуры данных об информационном ущербе, связанном с нарушением устойчивости функционирования КВИС (таблица 4).

При оценке показателей информационного ущерба КВИС определяется коэффициент информационного ущерба γ_{ij}, связанный с нарушением отдельных функций КВИС и характеризующий степень этих нарушений.

С учетом принятой пяти бальной шкалы информационного ущерба введем обозначения:

Пусть $\xi_{УЯЗ}^{УЩ} = \{1,2,3,4,5\}$ – множество значений показателя уязвимых мест КВИС (очень низкая, низкая, средняя, высокая, очень высокая).

Пусть $\eta_{УЯЗ} = \{1,2,3,4,5\}$ – множество значений показателя частоты использования уязвимостей КВИС (используется очень редко, используется редко, использование усредненное, используется часто, используется очень часто).

Пусть $B^{УЩ} = \{1,2,3,4,5\}$ – множество значений показателя возможного информационного ущерба.

Тогда коэффициент информационного ущерба γ_{ij} будет определяться соотношением:

$$\gamma_{ij} = \xi^{УЩ}_{УЯЗ\,ij}\ \eta_{УЯЗ\,ij}\ B^{УЩ}_{ij}, \qquad (63)$$

где i-й информационный ущерб для j-го компонента КВИС.

Таблица 4 – Структура данных об информационном ущербе

Наименование источника данных об ущербе	Наименование типа ущерба	Описание факта ущерба
Журнал регистрации событий в операционной системе (ОС)	Нарушение дат	Искажение даты информации, настроек функций программного обеспечения
	Нарушение количества инициализаций ОС	Искажение числа инициализаций ОС
	Нарушение времени регистрации оператора	Искажение времени идентификации и аутентификации операторов
	Нарушение номера записи оператора	Искажение порядкового номера записи оператора
	Нарушение идентификатора абонентов КВИС	Искажение кодов элементов КВИС
	Проявление компьютерной атаки в нарушении функционирования ОС	Параметры компьютерной атаки в соответствии с паспортом атаки
Журнал регистрации событий в системе управления базой данных (СУБД)	Нарушение даты изменений в информационном обеспечении КВИС	Подмена дат записей информации в БД КВИС
	Нарушение целостности структур данных	Искажения информационных таблиц и их связь
	Отказ в доступе к данным – «отказ в обслуживании»	Искажение интерфейсов доступа к данным, блокирование, стирание информации

	Использование «ложной информации» при выполнении ТЦУ	Введение дезинформации
	Нарушение идентификатора СУБД	Искажение кодов элементов СУБД и БД КВИС
	Нарушение номера записи информации в СУБД	Искажение порядкового номера записи в СУБД
	Нарушение идентификатора объектов СУБД	Искажение кодов элементов СУБД
	Нарушение времени выдачи команды на инициализацию считывания информации	Искажение времени поступления команды на инициализацию считывания информации
	Нарушение текстового описания порядка работы оператора с СУБД и БД	Искажение текстового описания, устанавливающее порядок применения СУБД и БД
Журнал администратора информационной безопасности КВИС	Нарушение сведений о местоположении	Искажение наименования местоположения
	Нарушение порядка администрирования КВИС	Искажение схемы адресации, несанкционированное получение привилегий администратора
	«Разрыв соединения» абонентов КВИС, приведение к не выполнению ТЦУ	Искажение порядка информационного взаимодействия и логическое отключение абонентов
	Нарушение принадлежности КВИС по выполнению ТЦУ	Искажение сведений о том, в интересах какого ТЦУ функционирует КВИС
	Нарушение сокращенного наименования	Искажение шифра КВИС
	Нарушение идентификатора КВИС	Искажение уникального децимального номера КВИС
Средства вычислительной техники (СВТ)	Нарушение характеристик СВТ	Искажение обобщенных характеристик средств вычислительной техники, связи или передачи данных
	Нарушение кода типа СВТ	Искажение идентификатора типа СВТ
	Нарушение идентификатора СВТ	Искажение уникального номера СВТ
СЗИ	Нарушение характеристик СЗИ	Искажение общих характеристик СЗИ

	Нарушение идентификатора СЗИ	Искажение кода конкретного образца СЗИ
Тип ЛВС	Нарушение наименования типа ЛВС	Искажение наименования типа ЛВС
	Нарушение кода типа ЛВС	Искажение идентификатора типа ЛВС
Тип специального ПО (СПО)	Нарушение кода типа СПО	Искажение идентификатора типа СПО
	Нарушение функций СПО	Искажение функций СПО при выполнении ТЦУ
	Нарушение наименования типа СПО	Искажение наименования типа СПО
Типовые уязвимые места	Нарушение описания типовых уязвимых мест КВИС	Искажение текстового описания основных характеристик типовых уязвимых мест КВИС
	Нарушение идентификатора СЗИ	Искажение кода конкретного образца СЗИ
	Нарушение функций СПКА	Искажение параметров настройки СПКА
	Нарушение кода типа данных	Искажение идентификатора типа хранения и машинного представления данных
	Нарушение кода типа ЛВС	Искажение идентификатора типа ЛВС
	Нарушение идентификатора СПО	Искажение кода конкретного образца СПО
	Нарушение идентификатора СВТ	Искажение кода конкретного образца СВТ
	Нарушение идентификатора уязвимости в БД	Искажение номера уязвимости в БД

В таблице 5 представлены результаты экспериментальных расчетов коэффициента γ_{ij} на основе обработки результатов экспертного оценивания КВИС на основе типовых решений по противодействию компьютерным атакам. При этом значения коэффициента γ_{ij} нормировано по модулю 10 относительно максимально возможного значения $(\gamma_{ij} = 0.1 - 12.5)$.

Таблица 5 – Значения коэффициента информационного ущерба

Ущерб, связанный с нарушением отдельных функций КВИС	Нарушение, искажение и разрушение общего и специального программного обеспечения	Вывод из строя АРМ	Вывод из строя серверов баз данных	Вывод из строя каналов связи, цифрового коммуникационного оборудования и протоколов передачи данных
Нарушение режимов работы операционной системы (приоритетности администратора, операторов и т.п.)	5	1	12.5	10
Имена операторов получены без идентификации и аутентификации в операционной системе и СПКА	0.2	3	12.5	12.5
Неправильные права доступа к ключу реестра операционной системы	0.1	2	5	7
Возможность редактирования реестра операционной системы и изменения функций КВИС по сети	7	8	12.5	12.5

В таблице 5 показана наихудшая ситуация когда значения коэффициента информационного ущерба максимально: $\gamma_{ij} \to \max$.

Структура и порядок применения методики оценки информационного ущерба от воздействия компьютерных атак на КВИС представлены в таблице 6 (обозначения в таблице: индекс «д» – допустимый уровень).

С учетом изложенного оценку информационного ущерба от компьютерных атак на КВИС определим на базе двух функций:

– функции потерь устойчивости функционирования КВИС, характеризующей информационный ущерб КВИС и описываемой соотношением:

$$F_{ПТ}\left(B_{ij}\right)=\left\{V_{Hij},V_{nij},N_{\text{армij}},N_{\text{срвij}},N_{ксij},K_{\text{YABij}},K_{\text{abij}},K_{\text{взл ij}},T_{в\ квисij},T_{в\ лвсij}\right\};\qquad(64)$$

– функцию потери ценности информации, характеризующей воздействие на информационный ресурс и утечку информации в КВИС в результате нарушения конфиденциальности, целостности и доступности информации, определим как:

$$F_{\text{ПЦИ}}\left(I_{ij}\right)=\left(F\left(I_{Kij}\right),F\left(I_{\text{Цij}}\right),F\left(I_{\text{ДТij}}\right)\right).\qquad(65)$$

Тогда обобщенная функция потерь устойчивости функционирования от воздействия компьютерных атак, которая позволяет оценить информационный ущерб, имеет вид:

$$F_{ПТ}^{ущ}\left(B_{i\,j},I_{i\,j}\right)=\gamma_{i\,j}\sum_{i=1}^{k}\sum_{j=1}^{k}F_{ПТi\,j}\left(B_{i\,j}\right)F_{ПЦИi\,j}\left(I_{i\,j}\right).\qquad 66)$$

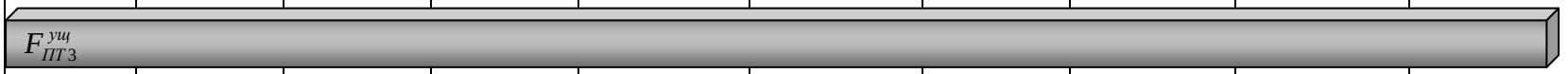
Функция ожидаемого ущерба от реализации компьютерных атак на КВИС представляется в виде отображения множества угроз атак на множество уязвимостей КВИС и соответствия их множеству параметров информационного ущерба:

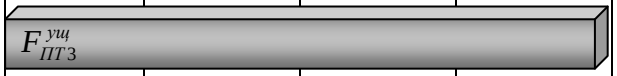
$$\forall\Phi_{ущ}^{ож}\left(S_{КВИС}\right):Y_A\times\xi_{уяз}^{ущ}\rightarrow\exists\left\{B_{i\,j},I_{i\,j}\right\}.\qquad(67)$$

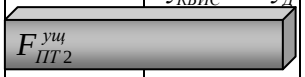
Таким образом, разработанная методика позволяет оценить информационный ущерб КВИС во взаимосвязи с различными сочетаниями реализации угроз компьютерных атак для вариантов построения КВИС и СПКА.

Таблица 6 – Структура и порядок применения методики оценки информационного ущерба от воздействия компьютерных атак

Рейтинг нарушения устойчивости функционирования КВИС	Угрозы воздействия компьютерных атак				Причины нарушения устойчивости функционирования			Информационный ущерб			
	Типы компьютерных атак Y_A	Уязвимые места КВИС $\xi_{КВИС}$	Возможные методы и средства реализации атак нарушителем B_Y	Характеристики сценария компьютерных атак J	Требования к КВИС не обеспечены $G_{КВИС}$	Требования к СПКА не обеспечены $G_{СПКА}$	Неверно выбраны СЗИ или защита не надежна $G_{СЗИ}$	Нарушение конфиденциальности информации $I_К$	Нарушение целостности информации $I_Ц$	Нарушение доступности информации $I_{ДТ}$	Нарушение устойчивости функционирования $S_{КВИС}^{УСТ}$
Очень высокий	$Y_A << Y_Д$	$\xi_{КВИС} << \xi_Д$	$B_Y << B_Д$	$J << J_Д$	$G_{КВИС} << G'_Д$	$G_{СПКА} << G''_Д$	$G_{СЗИ} << G'''_Д$	$I_К << I'_Д$	$I_Ц << I''_Д$	$I_{ДТ} << I'''_Д$	$S_{КВИС}^{УСТ} << S_{ТР}$
Высокий	$Y_A < Y_Д$	$\xi_{КВИС} < \xi_Д$	$B_Y < B_Д$	$J < J_Д$	$G_{КВИС} < G'_Д$	$G_{СПКА} < G''_Д$	$G_{СЗИ} < G'''_Д$	$I_К < I'_Д$	$I_Ц < I''_Д$	$I_{ДТ} < I'''_Д$	$S_{КВИС}^{УСТ} < S_{ТР}$
Средний	$Y_A = Y_Д$	$\xi_{КВИС} = \xi_Д$	$B_Y = B_Д$	$J = J_Д$	$G_{КВИС} = G'_Д$	$G_{СПКА} = G''_Д$	$G_{СЗИ} = G'''_Д$	$I_К = I'_Д$	$I_Ц = I''_Д$	$I_{ДТ} = I'''_Д$	$S_{КВИС}^{УСТ} = S_{ТР}$
Низкий	$Y_A \geq Y_Д$	$\xi_{КВИС} \geq \xi_Д$	$B_Y \geq B_Д$	$J \geq J_Д$	$G_{КВИС} \geq G'_Д$	$G_{СПКА} \geq G''_Д$	$G_{СЗИ} \geq G'''_Д$	$I_К \geq I'_Д$	$I_Ц \geq I''_Д$	$I_{ДТ} \geq I'''_Д$	$S_{КВИС}^{УСТ} \geq S_{ТР}$
Очень низкий	$Y_A > Y_Д$	$\xi_{КВИС} > \xi_Д$	$B_Y > B_Д$	$J > J_Д$	$G_{КВИС} > G'_Д$	$G_{СПКА} > G''_Д$	$G_{СЗИ} > G'''_Д$	$I_К > I'_Д$	$I_Ц > I''_Д$	$I_{ДТ} > I'''_Д$	$S_{КВИС}^{УСТ} > S_{ТР}$







Оглавление

7 КОМПЬЮТЕРНЫЕ ИГРЫ ОЦЕНКИ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ И УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИИ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Наличие факторов неопределенности априорных знаний о характеристиках сценария нарушителя и средствах реализации атак, сложность процессов управления и защиты информации КВИС приводит к необходимости создания компьютерных игр (КИ) оценки устойчивости функционирования КВИС в условиях компьютерных атак [22].

Компьютерная игра оценки устойчивости функционирования КВИС в условиях атак представляет собой комплекс программ, предназначенный для моделирования в реальном масштабе времени процессов функционирования системы, принятия решений и оценки эффективности выбранных средств противодействия атакам при различных вариантах игры.

Компьютерные игры включают в свой состав совокупность методов математического, имитационного и полунатурного моделирования и являются мощным инструментом поиска, и принятия решений в реальном масштабе времени. Они характеризуются строгим логическим и многоуровневым построением алгоритмов, формализованными сценариями возможных действий и используемым комплексом динамических моделей нарушителей. Экспертные оценки в играх реализуются через роли игроков компьютерной игры.

В конечном итоге компьютерная игра служит для выработки рекомендаций по рациональным действиям и согласованному выбору средств противодействия атакам на КВИС при разработке компонентов системы в условиях наличия неопределенности действий нарушителя и принятия решений по противодействию атакам. Подобные игры могут быть эффективно использованы для выработки решений по реализации новых подходов к защите информационных инфраструктур от массированных воздействий компьютерных атак.

По сравнению с традиционными методами планирования и исследования операций использование компьютерных игр дает преимущества по сокращению времени и повышению качества подготовки служб информационной безопасности к

выполнению предстоящих задач, использованию автоматизированных средств принятия решении в реальном масштабе времени.

Назначение КИ: практическое обучение специалистов по защите информации анализу сценариев нарушителя по реализации компьютерных атак, приобретение навыков по выявлению уязвимых мест и противодействию атакам на основе применения средств защиты информации (СЗИ) и средств восстановления КВИС.

Цель КИ: повышение уровня квалификации специалистов по защите информации и оценка устойчивости функционирования и уровня защиты информации КВИС в условиях компьютерных атак

Задачи КИ: имитационное моделирование двухсторонних действий нарушитель – администратор информационной безопасности (АБИ):

1. Формирование процессов функционирования КВИС (технологических циклов сбора, обработки, передачи информации и выдачи управляющей информации).
2. Формирование элементов КВИС и анализ потенциальных уязвимых мест.
3. Размещение СЗИ по элементам КВИС.
4. Формирование сценариев типовых компьютерных атак на уязвимые места КВИС.
5. Реализация типовых компьютерных атак на КВИС.
6. Реализация функций противодействия компьютерных атак на основе применения комплекса СЗИ (СПКА (СОА), МЭ, антивирусных программ (АВП), СЗИ НСД).

Технология оценки эффективности противодействия компьютерным атакам с использованием компьютерных игр (рисунок 14) определяет стратегию, тактику и реализацию КИ.

Игра позволяет проверить стратегии при решении проблемных вопросов выбора мер и средств противодействия атакам:

- предупреждения атак;
- обнаружения атак;
- сравнительного анализа атак (комплексом методов – сигнатурного анализа, методами анализа аномальных отклонений и функционального анализа);
- активного противодействия атакам;
- восстановления информационно-вычислительного процесса КВИС,
- устранения уязвимых мест (путем включения специальных программ, устраняющих возможность первоначального внедрения атаки через

уязвимости КВИС);

– динамической настройки параметров устойчивости функционирования КВИС.

В ходе игры по оценке устойчивости функционирования КВИС в условиях воздействия компьютерных атак проводятся исследования особенностей противодействия компьютерным атакам, оценки возможностей отражения модификаций и различных сочетаний атак при реализации сценариев атакующей стороной.

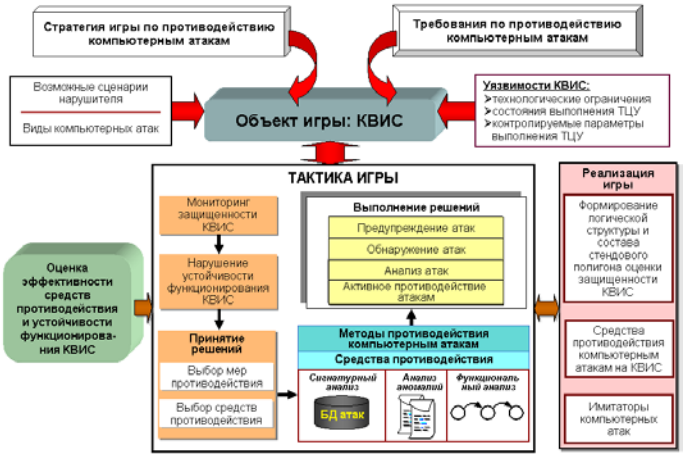


Рисунок 14 – Технология оценки эффективности противодействия компьютерным атакам с использованием КИ

Типовая структура аппаратно-программных комплексов (АПК) компьютерных игр по оценке устойчивости функционирования и уровня защиты информации КВИС в условиях компьютерных атак приведена на рисунке 15.

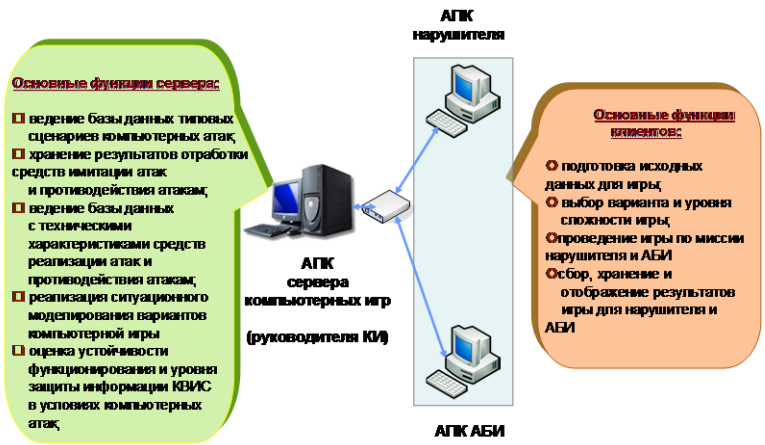
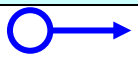


Рисунок 15 – Структура АПК компьютерных игр по оценке устойчивости функционирования и уровня защиты информации КВИС в условиях компьютерных атак

Организация игры (рисунок 15) предполагает двустороннюю модель «нарушитель – администратор безопасности информации (АБИ)» и проведение игры в учебной группе по парам. Сервер реализует сценарий игры, осуществляет сбор и хранение данных, необходимых для выполнения игры.

В таблице 7 приведены основные графические элементы КИ.

Таблица 7 – Графические элементы КСИ

№ п/п	Обозначение	Наименование обозначения
1.		Компьютерная атака
2.		Уязвимое место КВИС
3.		КВИС
4.		СЗИ НСД
5.		Антивирусные средства
6.		Система обнаружения атак
7.		Виртуальные частные сети
11.		Информационно-логическое взаимодействие

На рисунке 16 представлена модель компьютерной игры, состоящей из трех информационных моделей: нарушителя, КВИС (с предполагаемыми уязвимостями) и применения СЗИ. Проведение компьютерной игры заключается во взаимосвязанном выполнении этих информационных моделей и оценке полученных результатов.

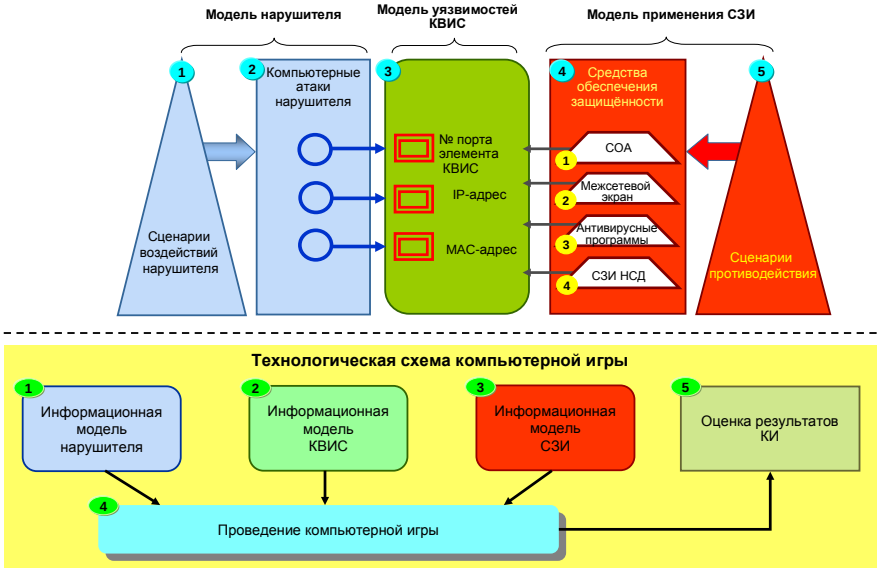


Рисунок 16 – Модель компьютерной игры

Стратегия игры определяется иерархической структурой возможных действий сторон и совокупностью правил по выбору вариантов противодействия атакам на каждом этапе в зависимости от условий обстановки и сложившейся ситуации.

Типовая информационная модель КВИС на рисунке 17 включает в свой состав четыре основных взаимосвязанных М-процессов (соответствующих подсистемам): сбора, обработки, передачи и выдачи управляющей информации. В целом эти процессы образуют технологический цикл управления КВИС. На эти процессы накладываются временные ограничения (ΔТ) по выполнению технологического цикла (значения времени на рисунке 17 условные).

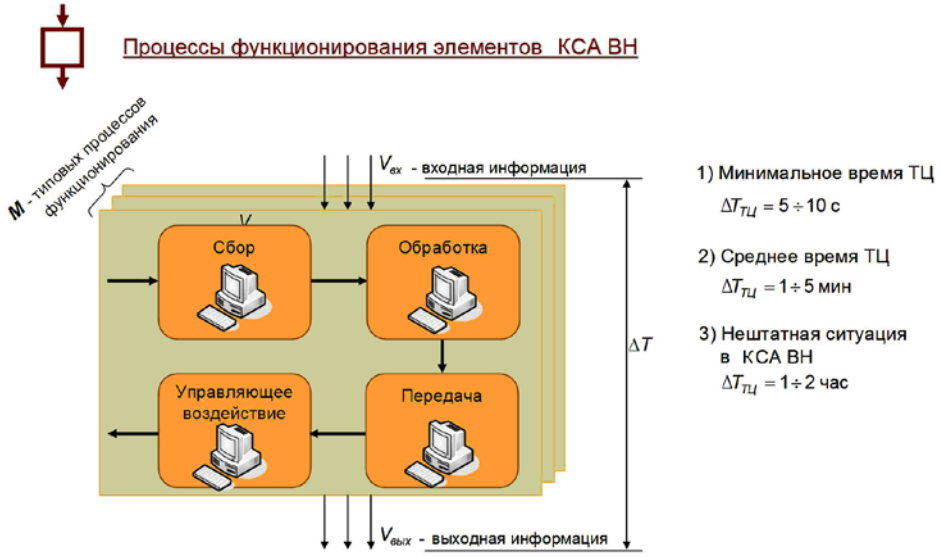


Рисунок 17 – Типовая информационная модель КВИС в КИ

Определение ограничений на выполнение технологического цикла КВИС, осуществляется в соответствии с рисунком 18.

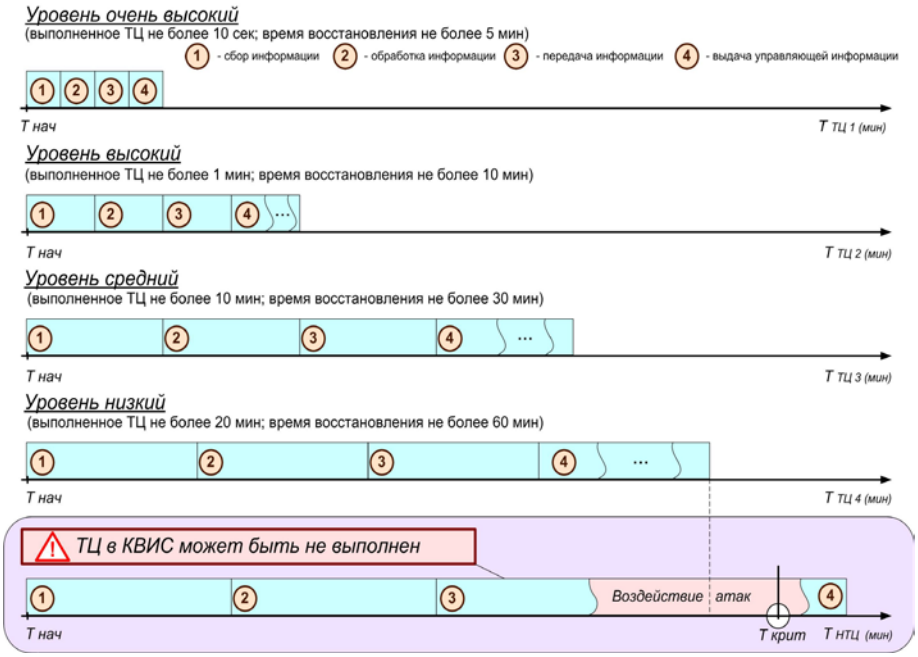


Рисунок 18 – Определение ограничений на выполнение технологического цикла

Выбранному уровню сложности соответствуют временные ограничения на выполнение ТЦУ. Если игрок в роли АБИ недостаточно обеспечил рубежи защиты и компьютерные атаки привели к значительному замедлению технологического цикла, то миссия этого игрока считается не выполненной.

Игровое поле моделируется вычислительной сетью КВИС со средствами удаленного доступа на базе протокола передачи данных (стеков протокола) TCP/IP. Графически вычислительная сеть КВИС представляется на экране монитора типовыми элементами (АРМ, серверы, коммуникационное оборудование, СЗИ, оборудование проводных и беспроводных каналов связи).

У каждого игрока свое игровое поле, обусловленное спецификой его действий: захвата информационного ресурса (нарушителем) или сохранения информационного ресурса (АБИ) КВИС в условиях компьютерных атак. Оценка результатов действий на игровых полях производится взаимосвязано через шкалу бальной оценки эффективности действий игроков и анализа сохранения или практического захвата информационного ресурса КВИС.

Игра состоит из последовательности миссий нарушителя и АБИ.

Нарушитель выбирает миссию и получает ее описание: сценарий воздействия на КВИС, возможные уязвимые места системы, тип компьютерных атак на выявленные уязвимости.

Администратор безопасности информации выбирает свою миссию и также получает ее описание: технологию КВИС, возможные СЗИ, а также требования к времени выполнения ТЦУ (сбора, обработки, передачи и выдачи управляющей информации).

Руководителем игры устанавливается ориентировочное среднее время базовых вариантов миссий и подмиссий игры. Миссии реализуются через роли АБИ и нарушителя, которые они выполняют на игровом поле (графической имитационной модели КВИС, функционирующей в условиях атак). Порядок организации КИ состоит из четырех этапов:

1. Тестирование игроков в роли АБИ и нарушителя.

2. Выполнение миссии АБИ.

3. Выполнение миссии нарушителя.

4. Реализация игрового процесса.

5. Оценка результатов игры.

Формирование КВИС осуществляется по трем графическим группам на экране монитора (рисунок 19):

1.Элементы КВИС.

2.Каналы связи.

3.Удаленные абоненты КВИС.

Элементы КВИС разбиты на четыре логических фрагмента, объединяющих совокупность АРМ:

средств обработки информации,

средств сбора информации,

средств передачи информации,

средств выдачи управляющей информации,

коммуникационное оборудование.

Каналы связи изображаются на экране и моделируются четырьмя группами:

спутниковые каналы связи (СКС),

магистральные каналы связи (МКС),

наземные каналы связи (НКС) – проводные каналы тональной частоты для модемной связи,

беспроводные каналы связи (БКС) – для организации информационного взаимодействия по беспроводным протоколам передачи данных.

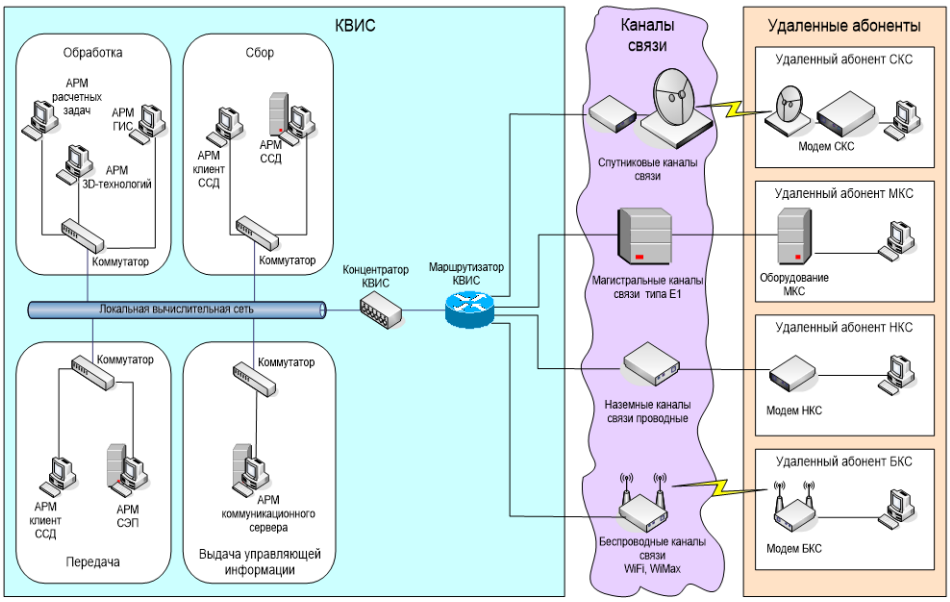


Рисунок 19 – Формирование элементов КВИС игроком в роли АБИ

Анализ уязвимых мест КВИС выполняется путем преобразования структуры и состава системы (рисунок 20) в структуру из условных графических элементов (на основе таблицы 7) и размещения по ней знаков потенциальных уязвимостей и угроз компьютерных атак.

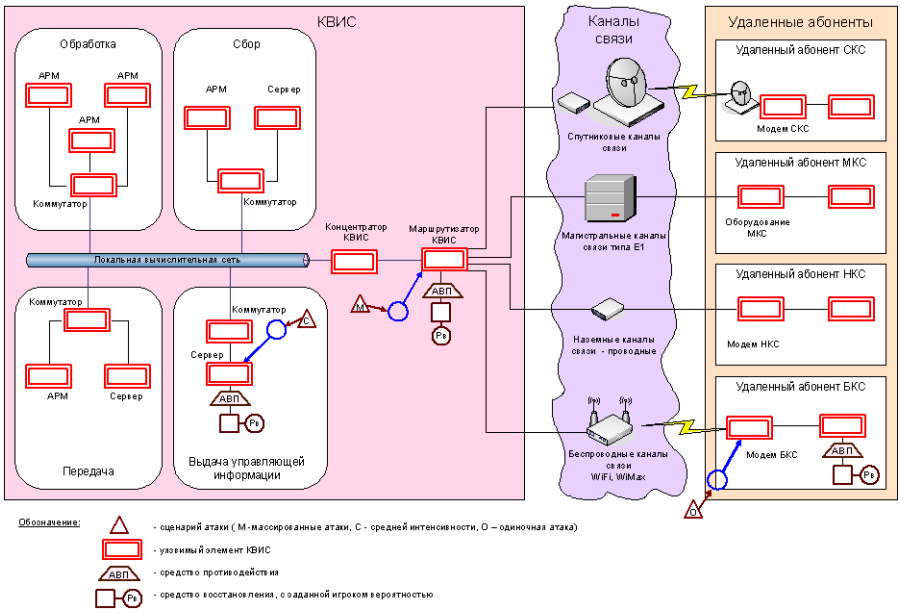


Рисунок 20 – Анализ уязвимых мест КВИС

Размещение СЗИ в игре проводится на сформированной графической структуре КВИС путем добавлении графических объектов обозначающих элементы комплекса

СЗИ (МЭ СЗИ НСД, АВП, СОА, датчики СОА). Пример осуществления миссии для максимально возможного размещения СЗИ приведен на рисунке 21.

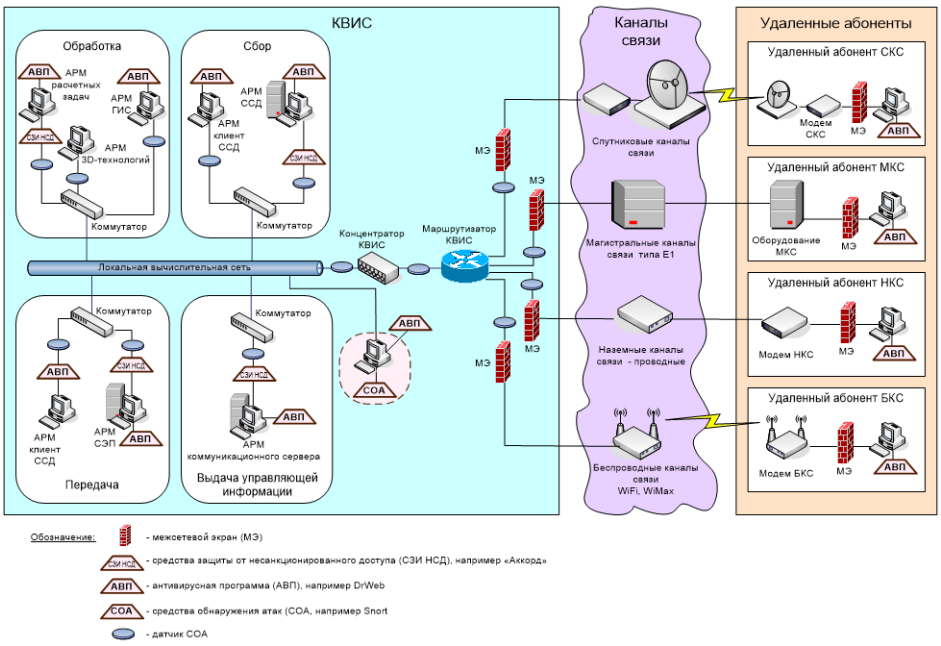


Рисунок 21 – Пример размещения СЗИ в КВИС

Формирование сценариев типовых компьютерных атак на КВИС осуществляется в игре по типовой технологии действий нарушителя (рисунок 22).

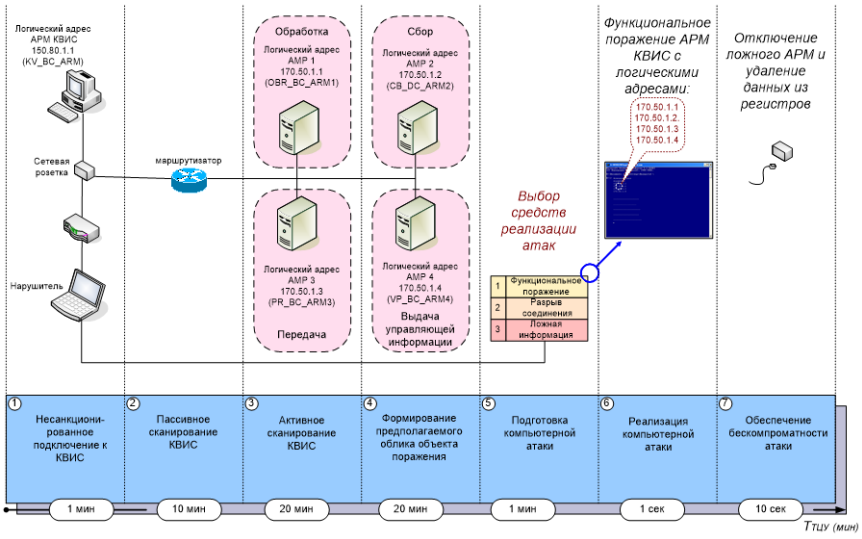


Рисунок 22 – Формирование сценариев типовых компьютерных атак на КВИС

Реализованная в игре классификация компьютерных атак приведена на рисунке 23.

№ п/п	Классификация компьютерных атак	
	Типы атак	Подтипы атак
1.	Функцио нальное поражение (ФП) («синий экран», зависание, перезагрузка)	ФП1: Вывод из строя нескольких серверов (более одного сервера) *)
		ФП2: Вывод из строя отдельного сервера **)
		ФП3: Вывод из строя нескольких АРМ (более одного АРМ) *)
		ФП4: Вывод из строя отдельного АРМ
2.	Разрыв соединения (РС) (подмена ARP-таблиц)	РС1: Отключение удаленного доступа КВИС к абоненту по нескольким каналам связи (более одного канала связи)
		РС2: Отключение удаленного доступа КВИС к абоненту по одному из каналов связи
		РС 3: Отключение нескольких образцов (более одного) коммуникационного оборудования в КВИС (маршрутизаторы и коммутаторы)
		РС 4: Отключение отдельного коммуникационного оборудования в КВИС (маршрутизатор, коммутатор)
3.	Ложная информация (ЛИ) (получение удаленной консоли управления)	ЛИ1: Введение дезинформации на сервере
		ЛИ2: Искажение информации на сервере
		ЛИ3: Введение дезинформации на АРМ
		ЛИ4: Искажение информации на АРМ
4.	Спам (СП)	СП1: Критическая нагрузка на сервер (отказ в обслуживании)
		СП2: Перегрузка сервера (снижение производительности)
		СП3: Критическая нагрузка на АРМ
		СП4: Перегрузка АРМ

Рисунок 23 – Реализованная в игре классификация компьютерных атак

Для определения квалификации игроков с ролью нарушителя и АБИ они проходят тестирование по ряду тем. Пример интерфейса КИ для тестирования игроков представлен на рисунке 24.

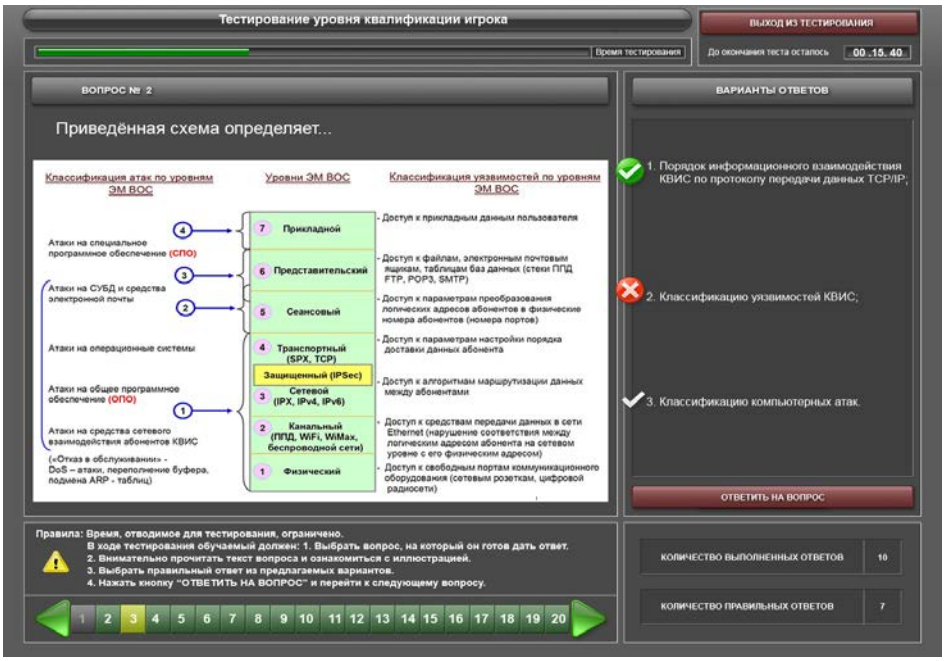


Рисунок 24 – Пример интерфейса КИ для тестирования игроков

На рисунках 25 - 27 представлены интерфейсы игры при выполнении соответствующих функций администратора информационной безопасности, нарушителя и противодействия компьютерным атакам на основе применения комплекса СЗИ.

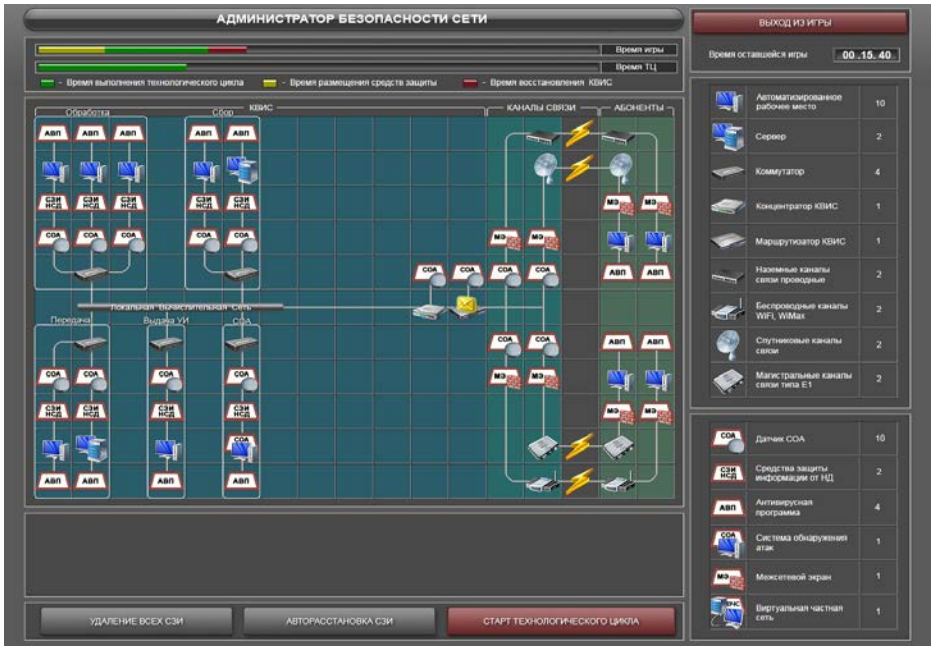


Рисунок 25 – Интерфейс администратора информационной безопасности

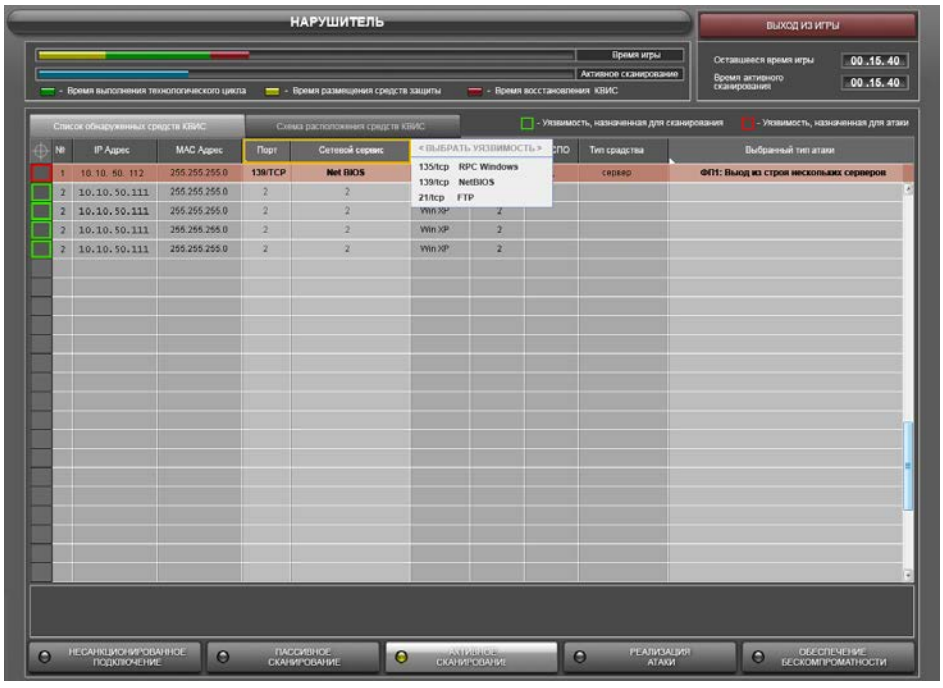


Рисунок 26 – Интерфейс нарушителя

Рисунок 27 – Интерфейс противодействия компьютерным атакам на основе применения комплекса СЗИ

Оценка результатов КИ проводится двумя способами:

– по времени выполнения ТЦУ;

– по бальной шкале оценки действий игроков (максимальному значению баллов, набранных АБИ или нарушителем за игру).

В игре реализована следующая методика оценки результатов:

1. Расчёт баллов, набранных оператором в роли АБИ, осуществляется по формуле:

$$W_{АБИ} = W_{ЕГ}^{АБИ} + W_{разм}^{СЗИ} + W_{ВТЦ}^{КВИС}, \quad (68)$$

где

$$W_{ЕГ}^{АБИ} = K_{ЕГ} \frac{B_{АБИ}}{B_{\max}} \text{ – баллы, набранные по результатам тестирования оператора в роли АБИ,} \quad (69)$$

$K_{ЕГ} = 6$ – весовой коэффициент уровня квалификации оператора,

$B_{АБИ}$ – баллы, набранные оператором в роли АБИ при тестировании,

$B_{\max}$ =20 – max количество баллов.

$$W_{разм}^{СЗИ} = K_{разм}\left(1-\frac{T_{разм}-T_{шт\,разм}}{T_{разм}}\right) \text{ – баллы за размещение СЗИ,} \quad (70)$$

$K_{разм}=2$ – весовой коэффициент уровня оператора при размещении СЗИ,

$T_{разм}$ – реальное время размещения СЗИ,

$T_{шт\,разм}$ – штатное время размещения СЗИ = Nсредств*10 сек.

$$W_{ВТЦ}^{КВИС} = K_{ТЦ}\left(1-\frac{T_{РТЦ}-T_{штТЦ}}{T_{РТЦ}}\right) \text{ – баллы за своевременное выполнение КВИС в условиях атак,} \quad (71)$$

$K_{ТЦ}=6$ – весовой коэффициент уровня оператора при восстановлении ТЦ КВИС,

$T_{РТЦ}$ – реальное время выполнения ТЦ КВИС,

где $T_{РТЦ}=T_{шт\,ТЦ}+T_{восст}$,

$T_{шт\,ТЦ}$ – штатное время выполнения ТЦ КВИС.

С учётом выражений (69 - 71) формулу (68) запишем

$$W_{АБИ}=K_{ЕГ}\frac{B_{АБИ}}{B}+K_{разм}\left(1-\frac{T_{разм}-T_{штразм}}{T_{разм}}\right)+K_{ТЦ}\left(1-\frac{T_{РТЦ}-T_{штТЦ}}{T_{РТЦ}}\right). \quad (72)$$

2. Расчёт баллов, набранных оператором в роли нарушителя, проводится по следующей формуле:

$$W_{нар}=W_{ЕГ}^{нар}+W_{атак}^{выб}+W_{ЗТЦ}, \quad (73)$$

$$W_{ЕГ}^{нар}=K_{ЕГ}\frac{B_{нар}}{B_{\max}}, \quad (74)$$

где $B_{нар}$ – баллы, набранные оператором в роли нарушителя при тестировании,

$K_{ЕГ} = 6$ – весовой коэффициент уровня квалификации оператора.

$$W_{атак}^{выб} = K_{атак}\left(1 - \frac{T_{атак}^{P} - T_{атак}^{шт}}{T_{атак}^{P}}\right), \quad (75)$$

где $K_{атак} = 4$ – весовой коэффициент оператора при выборе средств реализации заданных типов атак по выявленным при пассивном и активном сканировании уязвимостям,

$T_{атак}^{P}$ – реальное время выбора атак по выявленным уязвимостям,

$T_{атак}^{шт}$ – штатное время выбора атак по выбранным уязвимостям равно $N_{средств}$*10 сек.

$$W_{ЗТЦ} = K_{ВТЦ}\left(\frac{T_{РТЦ} - T_{штТЦ}}{T_{РТЦ}}\right), \quad (76)$$

где $K_{ВТЦ} = 6$ – весовой коэффициент замедления ТЦ КВИС на время воздействия *N*-атак типа ФП, РС, ЛИ и СП,

$T_{РТЦ}$ – реальное время выполнения ТЦ КВИС,

где

$T_{РТЦ} = T_{штТЦ} + T_{восст}$,

$T_{штТЦ}$ – штатное время выполнения ТЦ КВИС.

С использованием выражений (74 - 76) формула (73) имеет вид:

$$W_{нар} = K_{ЕГ}\frac{B_{нар}}{B_{\max}} + K_{атак}\left(1 - \frac{T_{атак}^{P} - T_{атак}^{шт}}{T_{атак}^{P}}\right) + K_{ВТЦ}\left(\frac{T_{РТЦ} - T_{штТЦ}}{T_{РТЦ}}\right). \quad (77)$$

3. Определение победителя в игре по критериям оценки результатов игры:

если $W_{АБИ} > W_{нар}$, то выиграл оператор в роли АБИ;

если $W_{нар} < W_{АБИ}$, то выиграл оператор в роли нарушителя.

Результаты оценок эффективности противодействия атакам создают возможность для сбора и хранения знаний о типовых уязвимостях КВИС, принятых решениях по противодействию атакам в условиях динамически меняющейся обстановки, устранению нештатных ситуаций в КВИС при воздействии компьютерных атак.

Предложенная КИ может быть использована как средство контроля выполнения требований к защищенности КВИС в условиях воздействия атак и оценки знаний операторов.

8 Требования к средствам противодействия компьютерным атакам на КВИС

Основой разработки средств противодействия компьютерным атакам являются требования, которые формируются в соответствии с подходом к построению КВИС в защищенном исполнении [11, 12]. Кроме того, важно учесть знания о характеристиках прототипов средств противодействия атакам, средств администрирования и мониторинга сети, межсетевых экранов, а также результаты экспериментальной отработки макетов СПКА на стендовом полигоне.

Создание КВИС, защищенных от воздействия компьютерных атак, предполагает интеграцию информационных технологий КВИС с внедренными в ее структуру датчиками СПКА, а также взаимодействие средств администрирования с управляющими программами СПКА.

Наиболее целесообразный путь разработки СПКА формирование ее из элементов со стеками к стандартным протоколам передачи данных КВИС (в частности TCP/IP) и использование защищенного внутреннего протокола и интерфейсов средств противодействия атакам. Однако эффект состояния защищенности КВИС будет достигнут тогда, когда наряду с компонентами СПКА осуществляется комплексное использование организационно-технических мер, максимальное применение средств администрирования и мониторинга сети, используются антивирусные средства, сертифицированное программное обеспечение, компьютерное и коммуникационное оборудование.

Кроме того, необходимо экспериментально проверить согласованность работы компонентов СПКА, средств защиты информации от несанкционированного доступа и КВИС при выполнении реальных ТЦУ КА, и по контролируемым параметрам уточнить технические решения.

Общие требования к противодействию компьютерным атакам на КВИС заключаются в следующем [26]:

1. Аппаратно-программный комплекс противодействия компьютерным атакам (АПК СПКА) должен быть программно и информационно совместим с компонентами КВИС на базе современного цифрового коммуникационного оборудования.

2. Для проверки функций АПК СПКА должны использоваться образцы коммуникационного оборудования и межсетевые экраны.

3. При проверке функциональных возможностей АПК СПКА должен использоваться имитатор компьютерных атак.

4. Взаимодействие между подсистемами АПК СПКА осуществляется через защищенный протокол передачи данных.

5. Выявление атак осуществляется от транспортного до сетевого уровня эталонной модели взаимодействия открытых систем. Противодействие атакам от физического до транспортного уровня реализуется средствами межсетевого экрана.

6. Работоспособность АПК СПКА должна быть подтверждена в составе действующих автоматизированных рабочих мест КВИС.

7. При разработке АПК СПКА должны быть использованы результаты проведения экспериментальных исследований на стендовом полигоне.

Технические требования к функциям и структуре средств противодействия компьютерным атакам формализованы следующим образом.

Базовые функции АПК СПКА по противодействию компьютерным атакам:

– мониторинг устойчивости функционирования КВИС;

– предупреждение;

– обнаружение;

– анализ;

– активное противодействие;

– каталогизация компьютерных атак;

– визуализация результатов предупреждения, обнаружения, анализа атак и активного противодействия компьютерным атакам в текстовом, графическом и картографическом виде.

Применение АПК СПКА основано на комбинированном способе обнаружения атак, который состоит во взаимосвязанном применении многодатчиковых систем и осуществлении сигнатурного анализа, анализа аномальных отклонений, функциональном анализе технологических циклов управления (по интервалам времени выполнения планов работ, объемам передаваемой и хранимой информации, анализе протоколов передачи данных и другим параметрам ТЦУ).

Обнаружение известных атак осуществляется сигнатурным анализом – выявление последовательности данных, соответствующих атаке, записанных в базе данных компьютерных атак.

Обнаружение неизвестных атак производится путем анализа аномалий в КВИС и функционального анализа, заключающихся в динамическом контроле

технологических операций сбора, обработки и передачи информации по типовым технологическим циклам управления (отклонения от технологических циклов управления воспринимаются как аномальные явления, оценка которых осуществляется в соответствия со сценарием атак).

При реализации АПК СПКА необходимо использовать подход многодатчиковых систем, в которых иерархическая сеть датчиков (программных и программно-аппаратных средств) позволяет извещать о событиях нарушения безопасности КВИС, анализировать и реагировать на компьютерную атаку. Датчики должны быть встроены в операционную систему, СУБД (БД), СПО, межсетевой экран и коммуникационное оборудование.

Фиксирование факта нарушения устойчивости функционирования КВИС осуществляется по критическому порогу событий информационной безопасности и выявлению моментов времени, когда информация по плану работ не могла поступать или превышению граничного значения принятого объема данных, а также ложным адресам абонентов сети и неверной сенсорной информации (сведений от датчиков АПК СПКА).

Структура АПК СПКА в соответствии с требованиями к средствам противодействия компьютерным атакам на КВИС приведена на рисунке 28.

Описание состава средств автоматизированных рабочих мест АПК СПКА и требований к их функциям представлено в таблице 8.

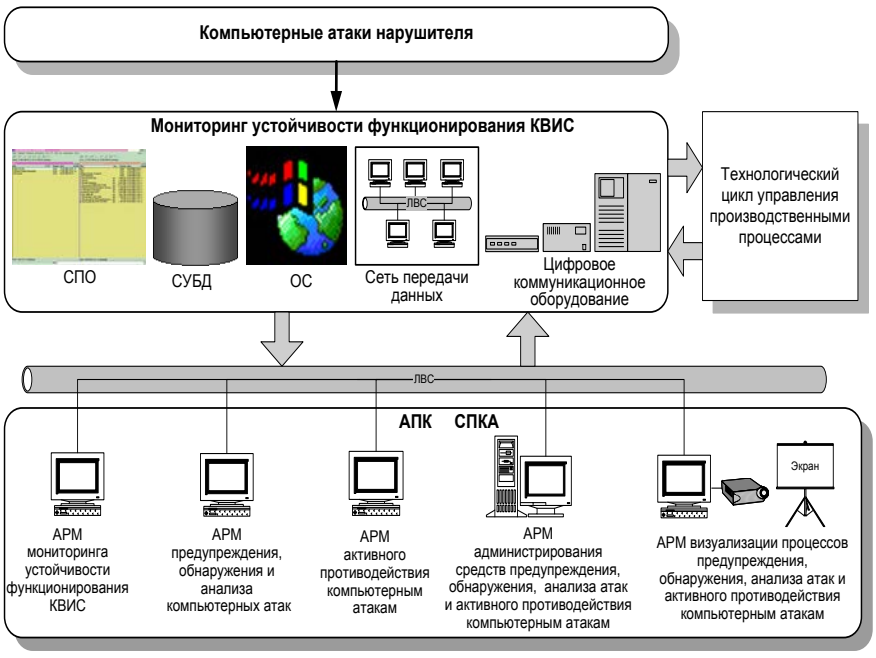


Рисунок 28 – Структура аппаратно-программного комплекса СПКА

Структура АПК СПКА должна включать в свой состав следующие унифицированные автоматизированные рабочие места (АРМ):

1. АРМ мониторинга устойчивости функционирования КВИС.

2. АРМ предупреждения, обнаружения и анализа компьютерных атак.

3. АРМ активного противодействия компьютерным атакам.

4. АРМ администрирования средств предупреждения, обнаружения, анализа атак и активного противодействия компьютерным атакам.

5. АРМ визуализации процессов предупреждения, обнаружения, анализа атак и активного противодействия компьютерным атакам.

Таблица 8 – Состав и требования к функциям средств автоматизированных рабочих мест АПК СПКА

№ п/п	Наименование АРМ	Состав средств	Требования к функциям
1.	 АРМ мониторинга устойчивости функционирования КВИС	– средства (программные датчики) мониторинга операционной системы; – средства (программные датчики) мониторинга специального программного обеспечения КВИС; – средства (программные датчики) мониторинга СУБД; – средства (программно-аппаратные датчики) мониторинга сети передачи данных КВИС; – средства (программно-аппаратные датчики) мониторинга цифрового коммуникационного оборудования.	– мониторинг устойчивости функционирования операционной системы КВИС; – мониторинг устойчивости функционирования специального программного обеспечения КВИС; – мониторинг устойчивости функционирования СУБД; – мониторинг устойчивости функционирования сети передачи данных КВИС; – мониторинг устойчивости функционирования цифрового коммуникационного оборудования; – передача данных мониторинга в АРМ предупреждения, обнаружения и анализа компьютерных атак; – передача данных мониторинга в АРМ активного противодействия компьютерным атакам.
2.	 АРМ предупреждения, обнаружения и анализа компьютерных атак	– средства выявления фактов подготовки компьютерных атак нарушителем; – средства сбора и регистрации информации, поступающей от АРМ мониторинга устойчивости функционирования; – средства обнаружения и анализа известных атак, записанных в базе данных компьютерных атак; – средства обнаружения и анализа неизвестных атак путем динамического	– извещение о потенциальных угрозах, уязвимостях и событиях информационной безопасности; – сбор данных о фактах подготовки компьютерных атак нарушителем; – сбор и регистрация данных мониторинга устойчивости функционировании операционной системы, СПО, СУБД, сети передачи данных, цифрового коммуникационного оборудования; – обнаружение и анализ атак на операционную систему; – обнаружение и анализ атак на специальное

№ п/п	Наименование АРМ	Состав средств	Требования к функциям
		контроля технологических операций сбора, хранения, обработки и передачи информации в КВИС; – средства каталогизации неизвестных атак в базе данных компьютерных атак; – средства взаимодействия с АРМ администрирования средств предупреждения, обнаружения, анализа атак и активного противодействия компьютерным атакам.	программное обеспечение; – обнаружение и анализ атак на систему управления базами данных; – обнаружение и анализ атак на сеть передачи данных; – обнаружение и анализ атак на цифровое коммуникационное оборудование; – обнаружение, сигнатурный анализ, анализ аномальных отклонений известных атак путем выявления признаков атак и сверки их с базой данных компьютерных атак; – обнаружение и анализ неизвестных атак путем динамического контроля технологических операций сбора, хранения, обработки и передачи информации в КВИС; – каталогизация неизвестных атак в базе данных компьютерных атак.
3.	 АРМ активного противодействия компьютерным атакам	– средства сохранения информационно-вычислительного процесса в условиях компьютерных атак по контрольным точкам; – средства блокирования источников атак; – средства блокирования подозрительных фрагментов сети; – средства перенаправления атак на обманные системы; – средства реконфигурации КВИС и инсталляции защищенной топологии сети.	– оповещение о применении средств противодействия компьютерным атакам; – маскирование резервными средствами сбора, хранения, передачи и обработки данных; – сохранение и восстановление информационно-вычислительного процесса по контрольным точкам; – блокирование нештатных технологических операций и абонентов удаленного доступа; – удаление вредоносных программ компьютерных атак и устранение уязвимостей; – логическое отключение фрагментов КВИС;

№ п/п	Наименование АРМ	Состав средств	Требования к функциям
			– реализация «стелс»-технологий информационных объектов КВИС (ложных серверов баз данных и электронной почты); – реконфигурация КВИС в защищенной топологии сети.
4.	 АРМ администрирования средств предупреждения, обнаружения, анализа атак и активного противодействия компьютерным атакам	– средства администрирования АРМ мониторинга устойчивости функционирования КВИС; – средства администрирования АРМ предупреждения, обнаружения и анализа компьютерных атак; – средства администрирования АРМ активного противодействия компьютерным атакам; – средства администрирования АРМ визуализации процессов предупреждения, обнаружения, анализа атак и активного противодействия компьютерным атакам.	– настройку администратором параметров АРМ мониторинга устойчивости функционирования КВИС, предупреждения, обнаружения и анализа компьютерных атак, активного противодействия компьютерным атакам, визуализации процессов предупреждения, обнаружения, анализа атак и активного противодействия компьютерным атакам; – предупреждение администратора об обнаружении компьютерных атак; – отображение детальной информации об обнаруженных атаках; – ввод в базу данных компьютерных атак сведений об известных атаках; – контроль функционирования автоматизированных рабочих мест АПК СПКА.
5.	 АРМ визуализации процессов предупреждения,	– средства визуализации результатов мониторинга устойчивости функционирования КВИС; – средства визуализации процессов функционирования АРМ предупреждения, обнаружения и анализа компьютерных атак; – средства визуализации процессов	– визуальное представление результатов мониторинга устойчивости функционирования КВИС; – визуальное представление процессов функционирования АРМ предупреждения, обнаружения, и анализа компьютерных атак; – визуальное представление процессов функционирования АРМ активного противодействия

№ п/п	Наименование АРМ	Состав средств	Требования к функциям
	обнаружения, анализа атак и активного противодействия компьютерным атакам	функционирования АРМ активного противодействия компьютерным атакам; – средства визуализации параметров компьютерных атак; – средства визуализации критически важных технологических операций КВИС.	компьютерным атакам; – визуальное представление параметров обнаруженных компьютерных атак; – визуальное представление критически важных технологических операций КВИС; – обеспечение отображения данных с использованием геоинформационных систем и программ 3D-моделирования; – выдача данных на средства отображения коллективного пользования.

Таким образом, обеспечение устойчивости функционирования КВИС в условиях компьютерных атак осуществляется на основе обоснования требований к средствам противодействия компьютерным атакам и разработки унифицированных автоматизированных рабочих мест аппаратно-программного комплекса СПКА в составе:

- мониторинга устойчивости функционирования КВИС;
- предупреждения, обнаружения и анализа компьютерных атак;
- администрирования средств предупреждения, обнаружения, анализа атак и активного противодействия компьютерным атакам;
- активного противодействия компьютерным атакам;
- визуализации процессов предупреждения, обнаружения, анализа атак и активного противодействия компьютерным атакам.

9 Стендовый полигон для оценки средств противодействия компьютерным атакам

Стендовый полигон представляет собой совокупность общего и специального программного, информационного, технического обеспечения аппаратно-программных комплексов (АПК) оценки средств противодействия компьютерным атакам в составе замкнутой локальной вычислительной сети (ЛВС) и средств визуализации коллективного пользования [19-21].

Задачи применения стендового полигона состоят в следующем:

1. Подготовка исходных данных для обоснования требований к средствам противодействия компьютерным атакам.
2. Экспериментальная оценка устойчивости функционирования КВИС в условиях компьютерных атак.
3. Отработка технических и программных образцов средств противодействия компьютерным атакам.
4. Тестирование и апробация имитаторов компьютерных атак на КВИС.
5. Разработка и проведение экспериментов по оценке средств противодействия компьютерным атакам.
6. Испытания КВИС в защищенном исполнении в условиях компьютерных атак.
7. Разработка и испытания программно-технических средств мониторинга угроз функционального поражения КВИС.
8. Практическая отработка методов и показателей оценки эффективности противодействия компьютерным атакам на КВИС.

Структура стендового полигона оценки средств противодействия компьютерным атакам представлена на рисунке 29 и включает в свой состав:

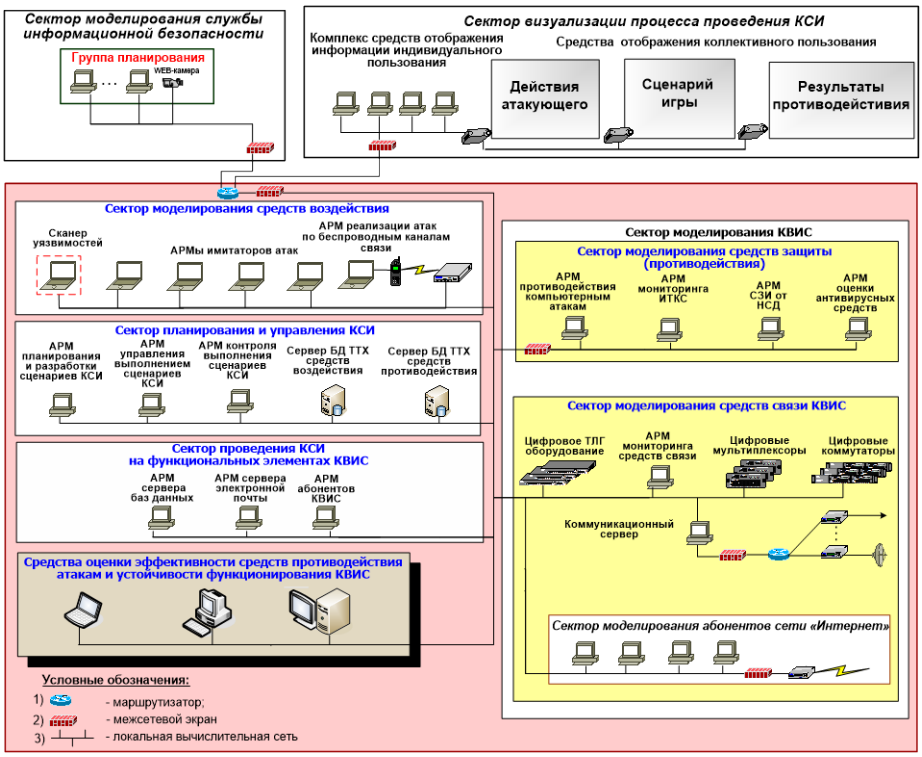


Рисунок 29 – Структура стендового полигона оценки средств противодействия компьютерным атакам

1. Сектор моделирования службы информационной безопасности.

Включает в свой состав АРМ группы планирования противодействия компьютерным атакам. На этих АРМ осуществляется контроль выполнения планов противодействия компьютерным атакам, подготовка исходных данных о характеристиках и уязвимостях КВИС, сведений о нарушителе, данных предупреждения о фактах угроз воздействия компьютерных атак и управление средствами противодействия атакам.

2. Сектор визуализации процессов проведения КИ.

Сектор предназначен для оперативной и наглядной визуализации результатов экспериментальных исследований, а также управления отображением при проведении компьютерных игр в интересах принятия решений в реальном масштабе времени.

3. Стенд испытаний средств противодействия компьютерным атакам, включающий в свой состав:

а) Сектор моделирования средств воздействия.

Сектор оснащается различными имитаторами средств реализации компьютерных атак нарушителя: сканером уязвимостей, АРМ имитатора атак, АРМ реализации атак по беспроводным каналам связи.

б) Сектор моделирования средств защиты (противодействия компьютерным атакам).

В секторе установлены и испытываются средства АРМ СПКА, АРМ «ложных» информационных объектов, АРМ мониторинга устойчивости функционирования КВИС, АРМ СЗИ НСД, антивирусные средства, межсетевые экраны.

в) Сектор моделирования КВИС.

Сектор моделирования КВИС одновременно является сектором проведения КИ на функциональных элементах КВИС. Совместно с другими секторами стендового полигона воспроизводит в виде натурных и имитационных моделей базовые АРМ КВИС:

- АРМ сервера сбора данных (ССД–Ц) – для имитации информационно телекоммуникационного центра сбора данных;
- АРМ сервера сбора данных пункта (ССД–П) – для имитации телекоммуникационного комплекса пункта сбора данных;
- АРМ сервер сбора данных абонента (ССД–А) – для имитации непосредственного предоставления данных абоненту
- АРМ сервера электронной почты (СЭП) – для имитации обмена данными между абонентами КВИС;
- АРМ потребителей информации– для имитации обработки информации в интересах потребителей и расчета данных для выполнения ТЦУ в КВИС.

г) Сектор моделирования средств связи КВИС.

Сектор моделирования средств связи КВИС реализует функции моделирования на основе реального коммуникационного оборудования оперативного взаимодействия и управления между абонентами при выполнении ТЦУ в КВИС и выдаче данных в первичные сети связи (магистральные каналы связи).

д) Сектор планирования и управления КСИ.

В секторе работают основные серверы и средства управления игрой.

е) Сектор оценки эффективности методов, моделей и средств противодействия компьютерным атакам.

В секторе отрабатываются методы, модели и алгоритмы, реализованные в средствах противодействия компьютерным атакам. Сектор оснащен тремя базовыми АРМ:

- оценки эффективности компьютерных атак,
- оценки эффективности противодействия компьютерным атакам,

– оценки устойчивости функционирования КВИС при воздействии атак.

Порядок экспериментальной оценки средств противодействия компьютерным атакам на стендовом полигоне представлен на рисунке 30. Исследования на стендовом полигоне основаны на системно-техническом анализе возможных способов разработки и совершенствования средств противодействия компьютерным атакам. В ходе проведения КИ рассматриваются наиболее реальные атаки для конкретных КВИС. Технологические решения носят комплексный и согласованный характер использования средств противодействия компьютерным атакам, межсетевых экранов, средств защиты информации от несанкционированного доступа и других средств.

Разработанные методы и макеты средств противодействия компьютерным атакам на КВИС позволяют выбрать функции и характеристики средств предупреждения, обнаружения, анализа компьютерных атак и активного противодействия им, по полученным экспериментальным путем результатам оценок.

Рисунок 30 – Порядок экспериментальной оценки средств противодействия компьютерным атакам на стендовом полигоне

Результаты оценок на стендовом полигоне дают возможность для сбора статистики по поиску уязвимостей в КВИС и устранению нештатных ситуаций при воздействии компьютерных атак. Опыт экспериментальных исследований обобщается в виде рекомендаций, в которых систематизированы сведения о последовательности

процедур устранения уязвимых мест в АРМ КВИС, протоколах передачи данных, в программном обеспечении цифрового коммуникационного оборудования.

Предложенные экспериментальные средства стендового полигона, позволяют комплексно оценить эффективность методов обеспечения устойчивости функционирования КВИС, базовой технологии предупреждения и обнаружения компьютерных атак при динамических информационно-вычислительных процессах и условиях применения КВИС в реальном масштабе времени. Разработанные методы и средства могут служить основой для интегральной оценки устойчивости функционирования КВИС.

В целом стендовый полигон представляет собой типовое «ядро» комплекса средств автоматизации, которое при доработках аппаратно-программных средств может быть использовано для разработки базовых технологий создания унифицированных средств в интересах обеспечения устойчивости функционирования КВИС в условиях компьютерных атак.

10 Результаты экспериментальной оценки противодействия компьютерным атакам на критически важные информационные сегменты

В настоящем разделе приведены обобщенные результаты экспериментальной оценки противодействия компьютерным атакам на КВИС [17-21]. Экспериментальные исследования проведены на основе испытаний на стендовом полигоне макетов аппаратно-программных комплексов имитатора компьютерных атак, средств предупреждения и обнаружения компьютерных атак и средств оценки эффективности противодействия компьютерным атакам.

Результаты экспериментальной оценки эффективности противодействия компьютерным атакам представлены в следующей последовательности:

1. Результаты экспериментальной оценки эффективности компьютерных атак нарушителя.
2. Результаты экспериментальной оценки эффективности средств противодействия компьютерным атакам.
3. Результаты экспериментальной оценки эффективности активного противодействия компьютерным атакам.
4. Результаты экспериментальной оценки устойчивости функционирования КВИС в условиях воздействия компьютерных атак.

Эффективность компьютерных атак нарушителя оценивается по следующим показателям:

- вероятности использования уязвимостей КВИС,
- вероятности противодействия сканированию параметров КВИС (обратная величина вероятности сканирования параметров КВИС),
- вероятности создания точек несанкционированного доступа в КВИС,
- вероятности внедрения и распространения атаки,
- коэффициенту преодоления рубежей противодействия.

Оценка возможностей нарушителя по эффективности воздействия компьютерных атак на КВИС по бинарному соотношению «уязвимость КВИС – компьютерная атака» на основе использования разработанных в монографии методов,

показателей и системного анализа результатов моделирования атак характеризуется графическими зависимостями, представленными на рисунках 31 – 34.

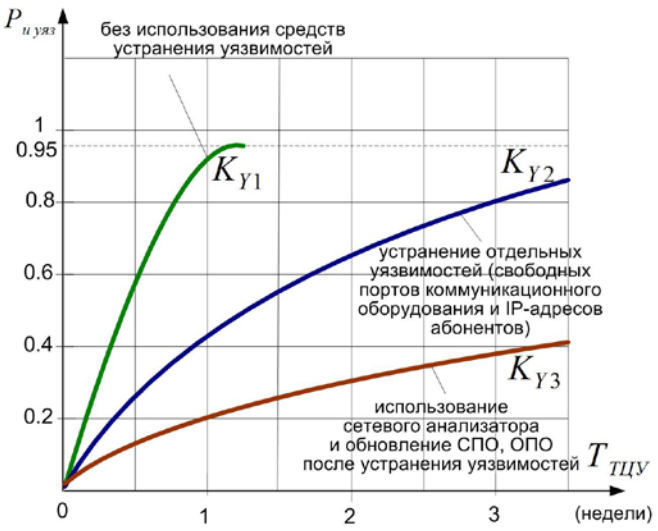


Рисунок 31 – Зависимости вероятности использования уязвимостей КВИС от времени выполнения ТЦУ

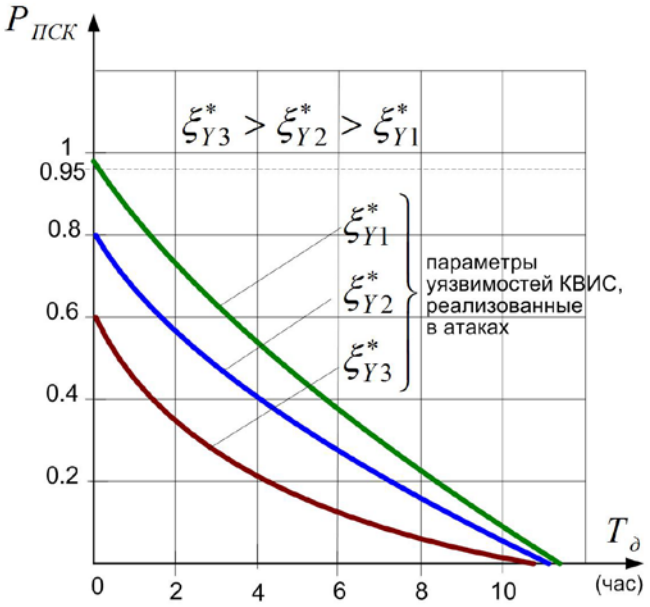


Рисунок 32 – Зависимости вероятности противодействия сканированию параметров КВИС от времени действия атак

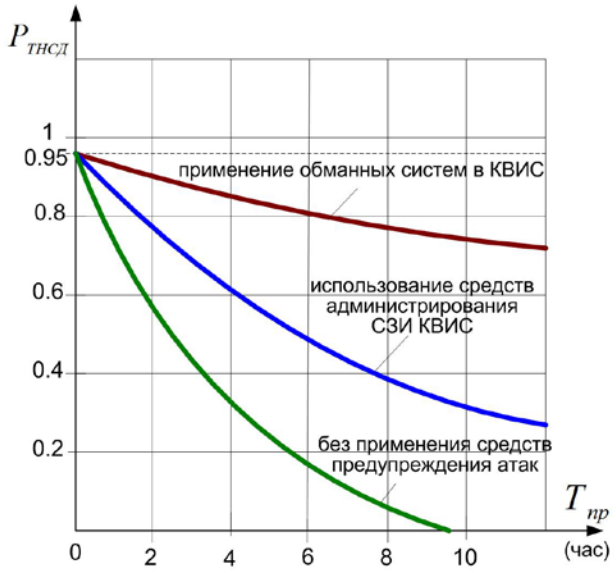


Рисунок 33 – Зависимости вероятности создания точек несанкционированного доступа в КВИС от времени предупреждения атак

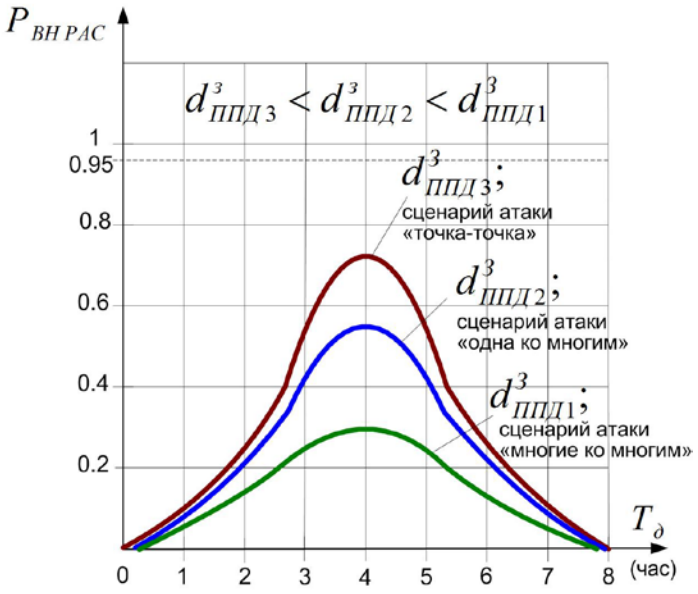


Рисунок 34 – Зависимости вероятности внедрения и распространения атак от времени действия атак

Вид зависимости $P_{и\,уяз}$ на рисунке 31 обусловлен тем, что для варианта $K_{У1}$ не устранены избыточные функции, ошибки и привилегии доступа к системным ресурсам в специальном программном обеспечении КВИС, а также отсутствует разграничение доступа операторов к информационно-вычислительным процессам выполнения ТЦУ. При использовании средств предупреждения атак (например, сетевого анализатора) в

КВИС значение функции, описывающей вероятность использования уязвимостей сегмента при реализации атаки снижается до значения 0.4 за трехнедельный срок выполнения ТЦУ.

На рисунке 32 приведены результаты экспериментов по анализу взаимосвязи ξ^*_{Yi} параметров уязвимостей КВИС, используемых компьютерными атаками, с временем действия атак $T_д$ в виде зависимостей $P_{ПСК}$ вероятности противодействия сканированию параметров КВИС от времени действия атаки. Графики показывают, что при минимальном количестве ξ^*_{Y1} параметров уязвимостей КВИС, используемых компьютерными атаками в течение 2 часов действия атак сохраняется высокий уровень противодействия сканированию параметров КВИС и стойкость средств КВИС, СПКА и СЗИ к вскрытию характеристик структур программ и данных.

На рисунке 33 представлены зависимости $P_{ТНСД}$ вероятности создания точек несанкционированного доступа в КВИС от времени предупреждения атак. Анализ рисунка 33 показывает, что только применение ложных информационных объектов (ложных АРМ КВИС) и технологии маскировки КВИС (устранение демаскирующих признаков критически важных АРМ, дезинформация нарушителя путем внедрения ложных потоков данных и других подобных мер) снижает значение вероятности создания точек несанкционированного доступа в КВИС до 0.7 в течении 10 часов противодействия атакам.

Экспериментальная оценка различных типов компьютерных атак и вариантов построения СПКА и КВИС позволили выявить закономерность между параметрами контроля защищенности протокола передачи данных, сценарием и временем действия атаки и значениями $P_{ВН\,РАС}$ вероятности внедрения и распространения компьютерных атак (рисунок 34). При использовании стандартных протоколов передачи данных $d^{З}_{ППДЗ}$, ввиду их слабой защищенности и уязвимости может быть реализован сценарий атак «многие ко многим» на компоненты КВИС. В этом случае максимальное значение $P_{ВН\,РАС}$ вероятности внедрения и распространения компьютерных атак составляет 0.8. Причиной получения такого значения вероятности является отсутствие в стандартных протоколах передачи данных контроля протоколов передачи данных от транспортного до прикладного уровня модели взаимодействия открытых систем при информационно-логическом взаимодействии абонентов КВИС и реализации ТЦУ.

На рисунке 35 представлена зависимость коэффициента преодоления рубежей противодействия компьютерным атакам от времени действия атак. Рисунок 35

показывает рост относительного числа преодоленных рубежей противодействия атакам $K_{ПРП}$ при увеличении времени действия компьютерных атак и увеличении отношения $\lambda_Y / \lambda_{ПКА}$ интенсивности компьютерных атак λ_Y к интенсивности противодействия атакам $\lambda_{ПКА}$.

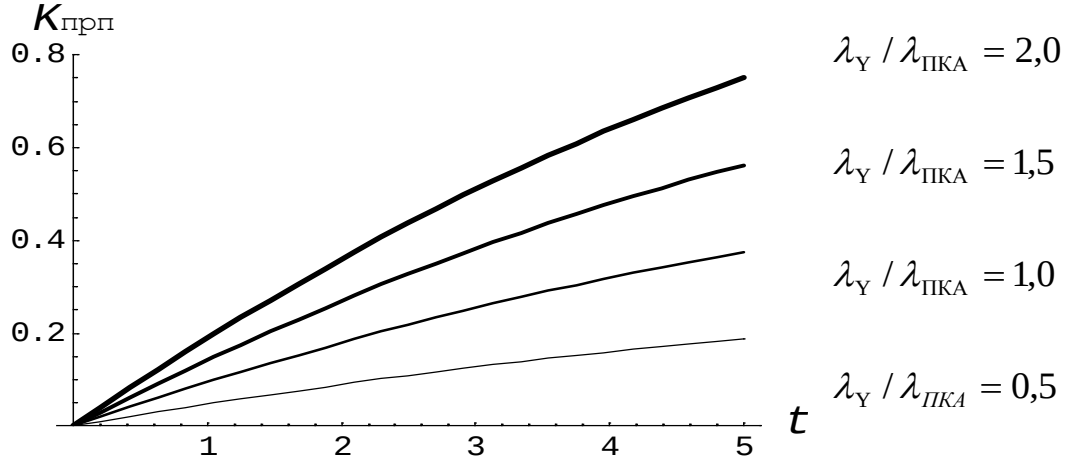


Рисунок 35 – Зависимость коэффициента преодоления рубежей противодействия атакам от времени действия атак при различных значениях отношений $\lambda_Y / \lambda_{ПКА}$ интенсивности компьютерных атак λ_Y к интенсивности противодействия атакам $\lambda_{ПКА}$

Оценка эффективности средств противодействия компьютерным атакам оценивается по бинарному соотношению «компьютерная атака – рубеж противодействия». Например, оценка эффективности средств противодействия компьютерным атакам осуществляется при моделировании воздействия компьютерных атак типа SYN - flood, Smurf и Fraggle.

Из рисунка 36 видно, что при увеличении количества рубежей противодействия атакам до 7 увеличивается вероятность предупреждения, обнаружения и анализа атак до значения $P_{ПОА} = 0.8$ при 5 атаках типа «функциональное поражение». А без встроенных в КВИС компонентов СПКА при более 15 атаках типа «функциональное поражение» или «отказ в обслуживании» они не обнаруживаются, и существует потенциальная опасность функционального поражения КВИС.

На рисунке 37 рассмотрены зависимости вероятности предупреждения, обнаружения и анализа атак от времени выполнения ТЦУ, которые показывают, что при настройке 7 рубежей противодействия атакам на потенциальные атаки после 12

часов выполнения ТЦУ достигается требуемый уровень вероятности предупреждения, обнаружения и анализа атак равный 0.95. Эффективное предупреждение, обнаружение и анализ атак возможны только при условии устранения уязвимостей КВИС, свободных портов коммуникационного оборудования и IP-адресов абонентов КВИС, наличия механизмов гибкого контроля и восстановления информационно-вычислительного процесса в сегменте.

На рисунке 38 для трех вариантов построения средств предупреждения, обнаружения и анализа атак показаны экспериментальные оценки соответствующей вероятности обнаружения атак при увеличении времени их обнаружения. Как можно увидеть из рисунка 6.19, существующие средства защиты информации (например, СЗИ НСД «Аккорд–5»), позволяют обеспечить требуемый уровень вероятности обнаружения атак при работе более одного часа. Только комплексное применение СПКА и СЗИ НСД позволяет найти соотношение между динамикой роста значения вероятностью и временем обнаружения атак. Эффект достигается за счет внедрения в КВИС разработанных в монографии методов предупреждения, обнаружения и анализа атак.

На рисунке 39 представлена диаграмма изменения времени обнаружения атак от уровня их обнаружения, характеризующая прямую взаимосвязь времени обнаружения атак и используемых средств обнаружения атак в КВИС. Анализ рисунка 39 показывает, что высокий уровень обнаружения атак (максимальное обнаружение атак на интервале до 2 минут) достигается при комплексном использовании: СПКА (7 рубежей противодействия), СЗИ НСД «Аккорд–5», межсетевого экрана, антивирусных средств защиты. Кроме того, необходимо чтобы в СПО КВИС была предусмотрена возможность динамически изменять матрицу доступа к ресурсам КВИС, гибко настраивать схемы адресации и правила доступа. При низком уровне обнаружения атак время обнаружения может быть от получаса до суток и более.

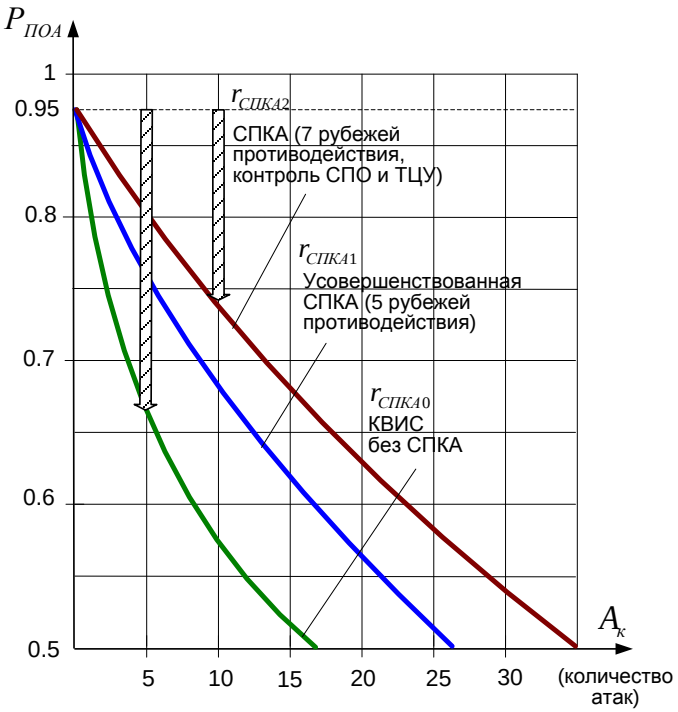


Рисунок 36 – Зависимости вероятности предупреждения, обнаружения и анализа атак от их количества

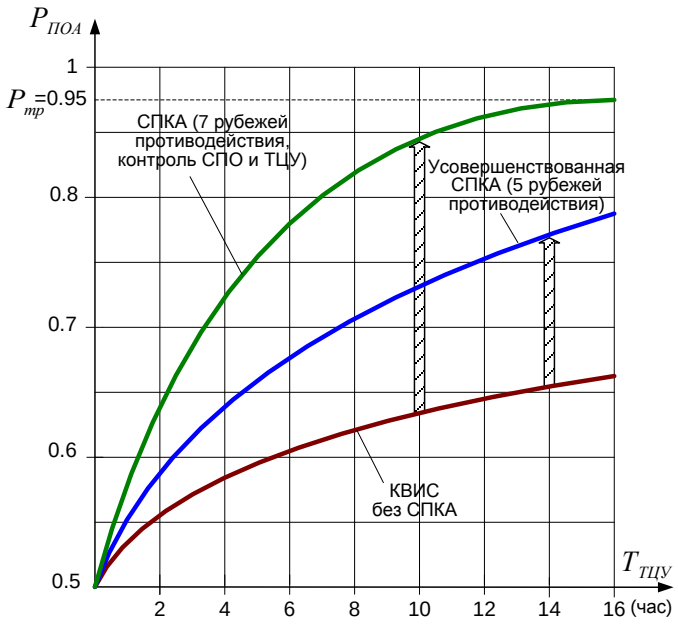


Рисунок 37 – Зависимости вероятности предупреждения, обнаружения и анализа атак от времени выполнения ТЦУ

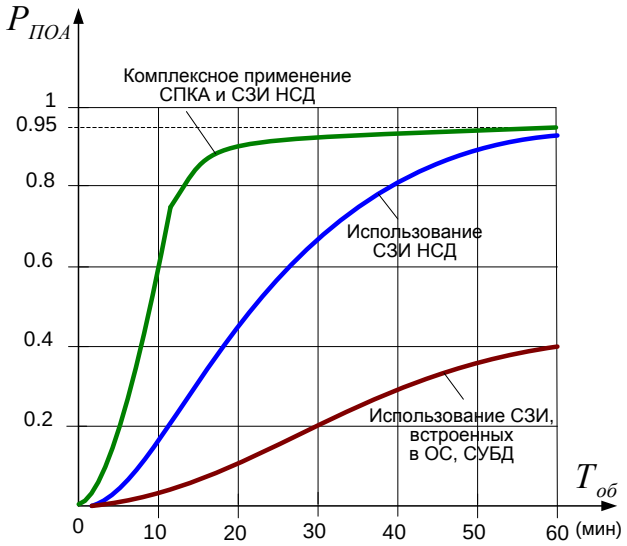


Рисунок 38 – Зависимости вероятности предупреждения, обнаружения и анализа атак от времени их обнаружения

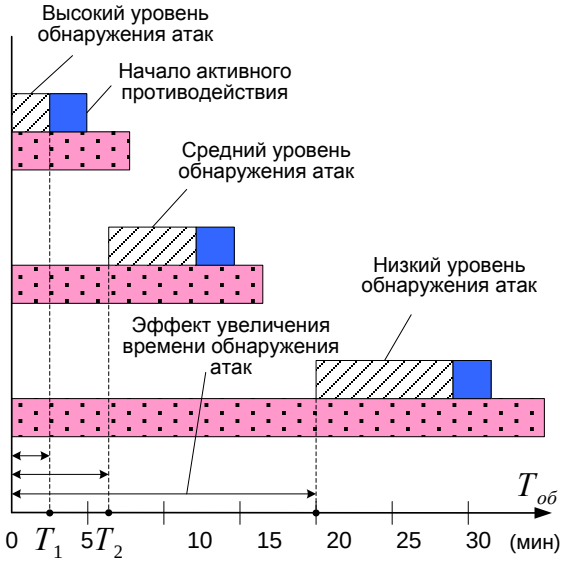


Рисунок 39 – Диаграмма изменения времени обнаружения атак от уровня их обнаружения

На рисунке 40 представлена зависимость коэффициента противодействия атакам от времени действия атак. Анализ рисунка 40 показывает уменьшение относительного числа не преодоленных рубежей противодействия $K_{ПКА}$ при увеличении времени действия компьютерных атак и уменьшении значений отношений количества средств

противодействия атакам $\pi_{\text{П}}$ к числу рубежей противодействия атакам $r^{O}_{СПОКА}$. Рисунок 40 также демонстрирует необходимость применения стороной В максимального числа рубежей противодействия (до 7 рубежей).

Оценка эффективности активного противодействия компьютерным атакам оценивается по бинарному соотношению «источник компьютерной атаки нарушителя – активное противодействие компьютерной атаке в КВИС» при двусторонней модели сторон.

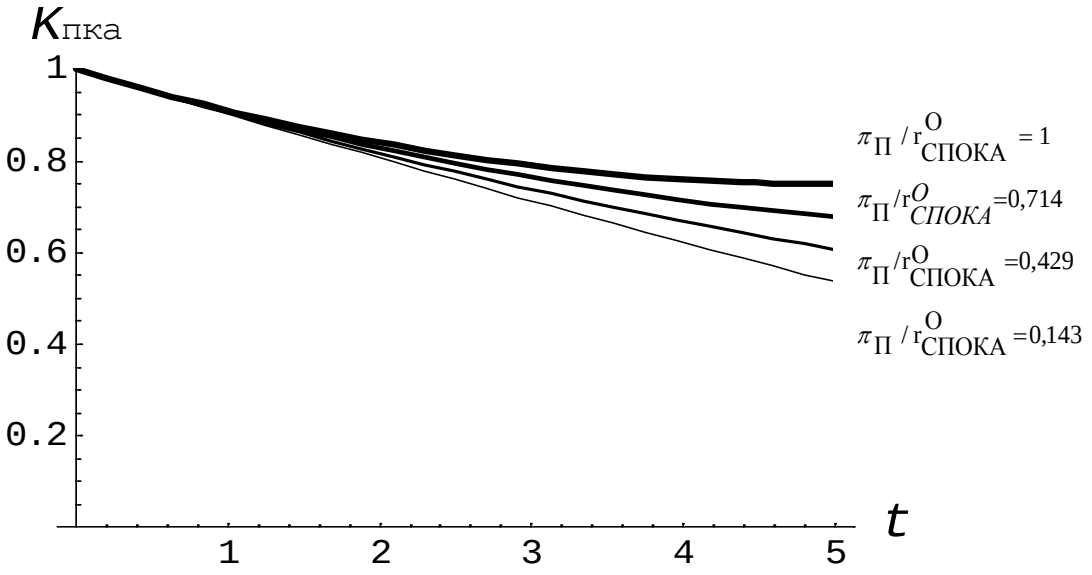


Рисунок 40 – Зависимость коэффициента противодействия компьютерным атакам $K_{ПКА}$ от времени действия атак при различных значениях отношений количества средств противодействия атакам $\pi_{П}$, к числу рубежей противодействия атакам $r^{O}_{СПОКА}$

На рисунке 41 приведены зависимости вероятности отражения компьютерной атаки от количества атак. Как можно заметить из рисунка 41, при увеличении количества атак резко снижается вероятность отражения компьютерной атаки. Эти зависимости демонстрируют, что при небольшом количестве атак в отсутствии комплексного использования методов активного противодействия атакам вероятность отражения атак снижается до значения 0.5.

На рисунке 42 показаны результаты выбора стратегии противодействия атакам на основе игровых методов при двусторонней модели и шести типах атак: сканирование сети КВИС, сканирование портов коммуникационного оборудования,

«отказ в обслуживании», атака использование уязвимостей ОС, атака использование уязвимостей СУБД, навязывание ложных данных. Рисунок 42 демонстрирует полученный средний выигрыш при реализации стратегий противодействия атакам сканирования сети КВИС и использования уязвимостей операционной системы.

Зависимости вероятности достижения информационного превосходства от времени активного противодействия атакам (рисунок 43) показывают необходимость не только реализации семи рубежей противодействия атакам, но и использования в СПКА $D^{r}_{СПОКА2}$ динамически управляемых параметров активного противодействия атакам (блокирования атак, перенаправления на ложный информационный объект, реконфигурации КВИС). При низком значении вероятности достижения информационного превосходства (до 0.7) воздействия компьютерных атак могут привести к преднамеренному нарушению устойчивости функционирования КВИС, существенному ущербу и затратам на восстановление.

На рисунке 44 представлена диаграмма изменения времени активного противодействия атакам от уровня противодействия им. Зависимости наглядно демонстрируют, что при высоком уровне активного противодействия атакам время обнаружения атак должно быть до 5 минут. Если у СПКА низкий уровень активного противодействия атакам, то противодействие может длиться до суток и привести к срыву выполнения ТЦУ.

Оценка эффективности устойчивости функционирования КВИС в условиях воздействия компьютерных атак оценивается по бинарному соотношению «устойчивость функционирования КВИС – противодействие атакам СПКА».

На рисунке 45 представлены графические зависимости для вероятности устойчивости функционирования КВИС в условиях воздействия атак на интервале времени выполнения ТЦУ иллюстрируют три ситуации:

1. Вероятность устойчивости функционирования КВИС в штатном режиме должно обеспечиваться на уровне 0.95.

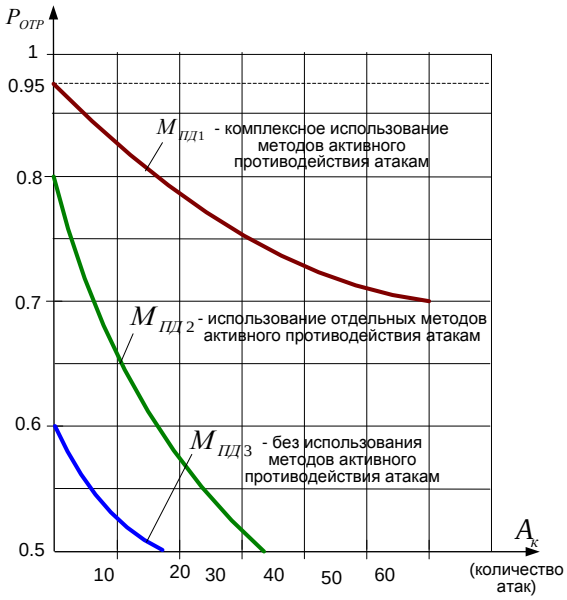


Рисунок 41 – Зависимость вероятности отражения компьютерной атаки от количества атак

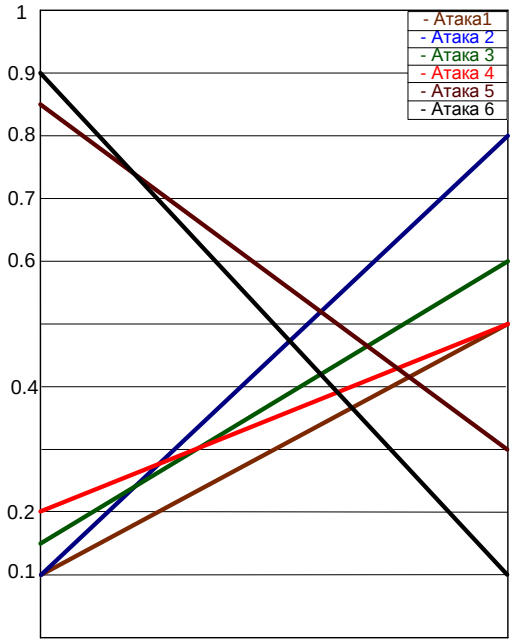


Рисунок 42 – Интерпретация поиска оптимальной стратегии противодействия атакам на основе игры 2x6

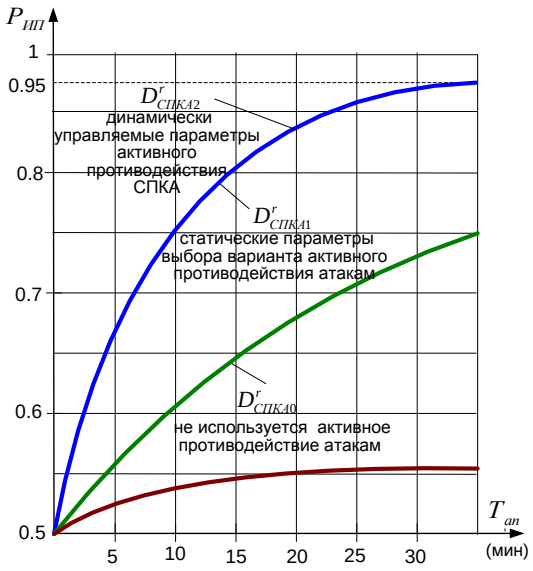


Рисунок 43 – Зависимость вероятности достижения информационного превосходства от времени активного противодействия атакам

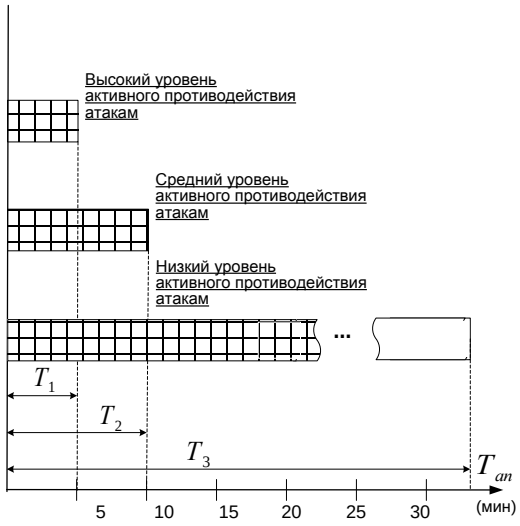


Рисунок 44 – Диаграмма изменения времени активного противодействия атакам от уровня противодействия им

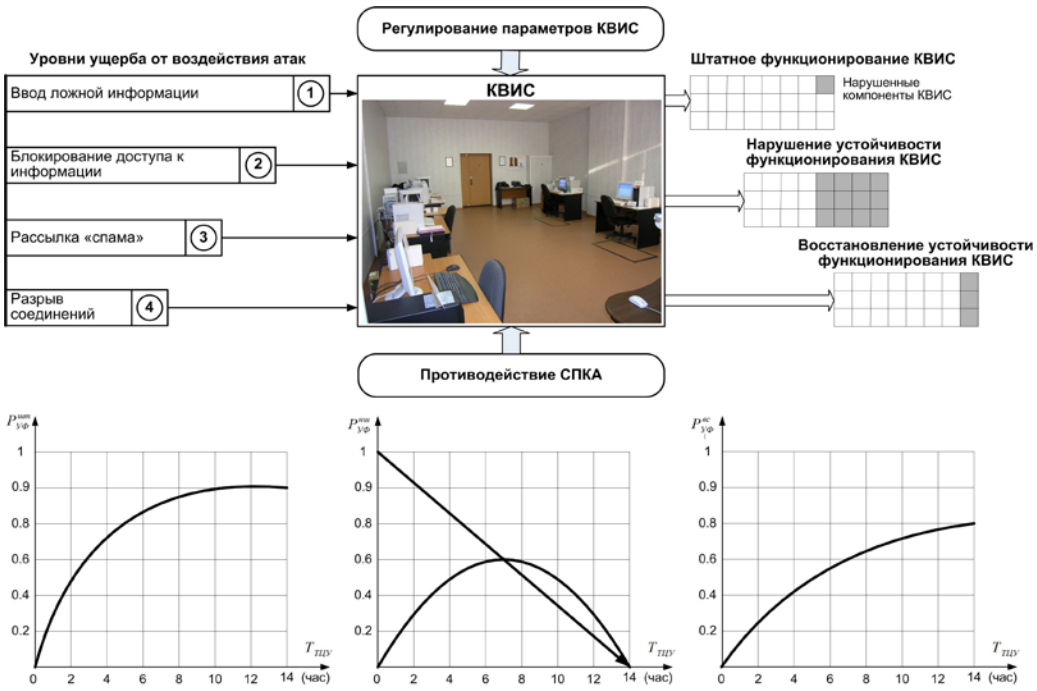


Рисунок 45 – Оценка эффективности устойчивости функционирования КВИС в условиях воздействия компьютерных атак

2. Эффективное воздействие компьютерных атак на КВИС примерно в течении 8 часов может снизить вероятность устойчивости функционирования КВИС до нуля.

3. Максимальное значение вероятности устойчивости функционирования КВИС в условиях массированного воздействия атак может быть достигнуто на уровне 0.8 за счет эффективного применения рубежей противодействия СПКА и динамического регулирования параметров КВИС.

Оценка результатов экспериментов показала, что дополнительное повышение устойчивости функционирования средств сбора, обработки и передачи информации достигается за счет реализации дополнительных требований к функциям противодействия атакам в протоколах передачи данных и коммуникационном оборудовании КВИС, которые позволяют осуществить информационное взаимодействие абонентов через защищенный «туннель» и протокол передачи данных.

Таким образом, результаты оценки показателей противодействия компьютерным атакам на КВИС показывают, что для обеспечения требуемого уровня противодействия атакам и устойчивого функционирования КВИС необходимо предусмотреть разработку СПКА и комплексного использования средств защиты информации на основе предложенных в монографии методов и технологий предупреждения, обнаружения, анализа атак и активного противодействия им.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Метод натурного и имитационного моделирования процессов противодействия компьютерным атакам.
2. Метод экспериментальной оценки эффективности воздействия компьютерных атак.
3. Методы экспериментальной оценки эффективности противодействия компьютерным атакам.
4. Анализ результатов экспериментальной оценки противодействия компьютерным атакам.
5. Метод экспериментальной оценки устойчивости функционирования критически важных информационных систем.
6. Методика оценки ущерба от воздействия компьютерных атак.
7. Стендовый полигон для оценки методов, моделей и средств противодействия компьютерным атакам.
8. Экспериментальная оценка эффективности сценариев противодействия компьютерным атакам на стендовом полигоне.
9. Компьютерные игры оценки устойчивости функционирования критически важных информационных систем.
10. Требования к средствам противодействия компьютерным атакам.

СПИСОК ЛИТЕРАТУРЫ

1. Абчук В.А. и др. Справочник по исследованию операций/Под общ. ред. Ф.А. Матвейчука – М.: Воениздат, 1979. – 368 с.: ил.
2. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М.. Численные методы. – М.: Наука, 1987. – 257 с.
3. Варжапетян А.Г., Глущенко В.В. Системы управления: Исследование и компьютерное проектирование: Учеб. пособие/ А.Г. Варжапетян, В.В.Глущенко. – 2-е изд. – М.: Вузовская книга, 2005. – 328 с.
4. Вентцель Е.С. Элементы теории игр. – М.: Государственное издательство физико-математической литературы, 1961. – 66 с.
5. Вентцель Е.С. Исследование операций. М.: «Советское радио», 1972, 552 с.
6. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. – М.: Наука. – 1998.– 480 с.
7. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003.– 512 с.
8. Волков И.К., Загоруйко Е.А. Исследование операций: Учеб. Для вузов. 2-е изд./Под ред. В.С. Зарубина, А.П. Крищенко. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. – 436 с.
9. Волкова В.Н., Денисов А.А. Основы теории систем и системного анализа. – С. Петербург, изд. СПб ГТУ, 1999.
10. Вязгин В.А., Федоров В.В. Математические методы автоматизированного проектирования: Учеб. Пособие для втузов. – М.: Высш. шк., 1989. – 184 с.
11. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения.
12. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
13. Дорф Р. Современные системы управления/Р.Дорф, Р. Бишоп; Пер. с англ. Б.И. Копылова.- М.: Лаборатория Базовых Знаний, 2004. – 832 с.
14. Дружинин Г.В. Надежность автоматизированных производственных систем. – 4-е изд., перераб. и доп. – М.: Энергоатомиздат, 1986. – 480 с.
15. Климов С.М. Анализ рисков нарушения функционирования информационно – телекоммуникационных космических систем. – М.: Системы безопасности

связи и телекоммуникаций №36, 2000, с. 24-31.

16. Климов С.М., Пальчун Б.П. Методические основы оценки рисков применения программного обеспечения в автоматизированной системе. II Межрегиональная конференция «Информационная безопасность регионов России». Материалы конференции. Том 1. – СПб., 2001, с. 15-20.
17. Климов С.М. Структура методики оценки эффективности средств защиты информации от программно-математических воздействий. Известия ТРТУ. Тематический выпуск. Материалы V Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2003. №4 (33), с. 14-22.
18. Климов С.М. Методика оценки возможного ущерба от нарушения безопасности информации автоматизированной системы. Известия ТРТУ. Тематический выпуск. Материалы V Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2003. №4 (33), с. 84-89.
19. Климов С.М. Методические и технологические основы мониторинга сетевых атак в информационно-телекоммуникационных системах. Известия ТРТУ. Тематический выпуск. Материалы VI Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2004. №4, с. 36-42.
20. Климов С.М. Методы и интеллектуальные средства предупреждения и обнаружения компьютерных атак на критически важные сегменты информационно-телекоммуникационных систем. Известия ТРТУ. Тематический выпуск. Материалы VII Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2005. №4, с. 25-34.
21. Климов С.М. Модель динамических процессов обнаружения компьютерных атак при сохранении устойчивости функционирования критически важных информационных сегментов. Известия ТРТУ. Тематический выпуск. Материалы VIII Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2006. №4, с. 46-55.
22. Климов С.М. Компьютерные игры в защите космической информации. //Военный парад №2(86).2008.
23. Липаев В.В. Программно-технологическая безопасность информационных

систем. - М.: МИФИ, 1997. – 144 с.

24. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. – М.: Мир, 1973.
25. Методы анализа и синтеза структур управляющих систем Б.Г. Волик, Б.Б. Буянов, Н.В. Лубков и др.; Под ред, Б.Г. Волика, – М.: Энергоатомиздат, 1988. – 296 с.
26. Нечипоренко В. И. Структурный анализ систем (эффективность и надёжность). – М.:Сов. радио,1977.-216с.
27. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность/ Петренко С.А., Симонов С.В. – М.: Компания АйТи; ДМК Пресс, 2005. – 384 с.: ил.
28. Половко А.М., Гуров С.В. Основы теории надежности. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2006. – 704 с.
29. Рыжиков Ю.И. Имитационное моделирование. Теория и технологии. – СПб.: КОРОНА принт; М.: Альтекс-А, 2004. – 384 с.: ил.
30. Советов Б.Я. Моделирование систем: Учеб. для вузов/Б.Я. Советов, С.А. Яковлев – 4-е изд., стер. – М. :Высш. шк., 2005. – 343с.
31. Справочник по теории автоматического управления/Под ред. А.А. Красовского. – М.: Наука. Гл. ред. Физ.-мат. Лит., 1987.-712 с.
32. Таха, Хемди А. Введение в исследование операций, 7-е издание.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 912 с.: ил.
33. Теория эксперимента. Налимов В.В. Физико-математическая библиотека инженера, Изд. «Наука». Главная редакция физико-математической литературы, 1971 г., 208 с.
34. Шикин Е.В., Чхартишвили А.Г. Математические методы и модели в управлении: Учеб. пособие. – 3-е изд. – М.: Дело, 2004. – 440 с.
35. Электрические системы. Математические задачи электроэнергетики: Учебник для студентов вузов/Под ред. В.А. Веникова-2-е изд., перераб. И доп.-М.: Высш. школа, 1981. – 288 с.: ил.
36. Эффективность технических систем/Под общ. ред. Уткина В.Ф., Крючкова Ю.В. – М.: Машиностроение, 1988, 328 с.