На правах рукописи

СУПРУН Александр Федорович

ОЦЕНКА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ УЧЕБНО-ТРЕНИРОВОЧНЫХ КОМПЛЕКСОВ НА ФАКУЛЬТЕТАХ ВОЕННОГО ОБУЧЕНИЯ

Специальность 05.13.19: Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание учёной степени
кандидата технических наук

Санкт-Петербург
2007

Работа выполнена в Государственном Образовательном Учреждении
Высшего Профессионального Образования
«Санкт-Петербургский государственный политехнический университет»

Научный руководитель: доктор технических наук, доцент
Матвеев Владимир Владимирович

Официальные оппоненты: доктор технических наук, профессор
Саенко Игорь Борисович

кандидат технических наук, доцент
Кусов Евгений Владимирович

Ведущая организация: Военно-космическая академия
имени А.Ф.Можайского г. Санкт-Петербург

Защита состоится “____” _____ 200 года в _____ часов на заседании диссертационного совета Д 212.229.27 ГОУ ВПО «Санкт-Петербургский государственный политехнический университет» по адресу: 195251, Санкт-Петербург, ул. Политехническая, д.29, ауд.175 гл. здания

С диссертацией можно ознакомиться в фундаментальной библиотеке ГОУ ВПО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан “____” _____ 2007 г.

Ученый секретарь диссертационного совета:

Платонов В.В.

ОБЩАЯ ХАРАКТЕРИСТИКА ДИССЕРТАЦИОННОЙ РАБОТЫ

Актуальность темы. Проблема защиты государственной тайны в учебном процессе образовательного учреждения высшего профессионального образования в современных российских условиях стоит крайне остро.

Одним из основополагающих организационных принципов обеспечения защиты государственной тайны является ограничение и стабилизация состава допущенных лиц, их тщательная предварительная проверка и сохранение определенного контроля за их деятельностью после прекращения контакта с информацией, составляющей государственную тайну. Однако не менее важным является вопрос обеспечения защиты аудиторных и лабораторных помещений от утечки закрытой информации по различным каналам и предотвращение угрозы нарушения конфиденциальности со стороны нарушителя-злоумышленника. Вопросы защиты информации обеспечиваются установленной политикой информационной безопасности.

Контроль за выполнение правил политики информационной безопасности возлагается на должностных лиц. Решение о достаточности проведения технических защитных мер принимается на основе данных мониторинга.

Решению общих проблем обеспечения информационной безопасности посвящены работы А.А. Грушо, П.Д. Зегжды и др., вопросы предупреждения несанкционированного доступа исследованы В.А. Герасименко, Л.М. Ухлиновым и др.

Анализ выполненных исследований показывает, что угрозы безопасности носят комплексный характер, поэтому система защиты информации должна быть комплексной.

Возникает настоятельная потребность в научно-обоснованных, объектно-ориентированных и, желательно, количественно измеримых методах технико-экономической оценки информационной защищенности.

С целью обеспечения безопасности любая организация должна нести определенные затраты. Очевидно, что наиболее благоприятным для организации является такое положение, когда затраты на обеспечение информационной безопасности являются достаточными для безопасного функционирования системы защиты и обеспечиваются при минимальных затратах.

Срок службы системы обеспечения информационной безопасности достаточно продолжителен. На протяжении срока службы несколько раз может измениться состав её технических средств. Исходя из этого, одним из основных вопросов, решаемых лицами, принимающими управленческие решения, является задача рационализации состава технических средств (как варианта системы), обеспечивающих сохранение её эффективности на протяжении жизненного цикла.

Анализ достаточности мер защиты и экономической целесообразности выбранного варианта требует разработки моделей угроз и защиты.

Эти обстоятельства предопределили постановку **актуальной научно-технической задачи -** разработка технологии оценки достаточности мер защиты с использованием технико-экономических показателей.

Цель исследования – разработать методы оценки и обеспечения защищенности Автоматизированного учебно-тренировочного комплекса (АУТК) на основе создания комплекса моделей угроз и защиты при проведении учебного процесса на факультете военного обучения.

Объект исследования – система обеспечения информационной безопасности учебного процесса по закрытым дисциплинам в ГОУ ВПО.

Предмет исследования – методы обеспечения и оценки достаточности защитных мер.

Задачи исследования:

– проанализировать механизм реализации угроз конфиденциальности сведений, используемых в учебном процессе;

– разработать модели угроз;

– обосновать состав и функционирование системы мониторинга;

– предложить комплекс организационных и технических мер защиты;

– разработать методику оценки достаточности мер защиты и обосновать рекомендации по повышению информационной безопасности учебного процесса;

– разработать подход к оценке защищенности АУТК, используемых в учебном процессе.

Методы исследования: системный анализ, структурный синтез, теория вероятностей, исследование операций.

Основные научные результаты, выносимые на защиту:

1. Методика оценки информационной безопасности АУТК.

2. Выявление наиболее существенных угроз безопасности реализации учебного процесса с использованием АУТК.

3. Обоснование комплекса методик оценки достаточности мер защиты с учетом экономических показателей.

4. Разработка рекомендаций по обеспечению требуемого уровня безопасности учебного процесса.

Новизна основных научных результатов состоит в том, что:

– формализованы модели утечки информативных сигналов;

– конкретизирована и уточнена модель нарушителя и формализована логика его действий применительно к АУТК при преодолении системы информационной защиты;

– обоснована структура и разработана математическая модель для оценки эффективности комплексной системы мониторинга;

– предложен новый подход к оценке эффективности подавления радиотехнического канала утечки;

– разработана методика оценки защищенности АУТК, используемых в учебном процессе;

– разработаны методики технико-экономического обоснования вклада различных мер защиты в безопасность учебного процесса с использованием АУТК;

– на основе технико-экономического анализа получены оценки различных мер защиты.

Достоверность основных научных результатов обеспечивается:

– применением апробированных общенаучных и специальных методов исследования;

– реализацией предложенных моделей и методик;

– непротиворечивостью полученных частных количественных оценок практике функционирования существующих элементов систем защиты.

Научная значимость основных научных результатов определяется развитием методологических положений теории обеспечения информационной

безопасности в части формализации процесса защиты от угроз различного характера и вкладом в теорию функционально-стоимостного анализа сложных систем в части оценки неаддитивных параметров.

Практическая значимость состоит в доведении разработанных математических моделей до алгоритмов и расчетных методик, а также в использовании методик для обоснования организационных и технических требований к системе мониторинга и защиты сведений, составляющих государственную тайну, в учебном процессе высшего профессионального образования. Разработаны практические рекомендации по обеспечению защищенности АУТК на факультетах военного обучения.

Практическая значимость работы подтверждена актами реализации разработанных моделей и методов.

Апробация работы. Основные теоретические и практические результаты диссертационной работы докладывались и обсуждались на: научно-методическом семинаре «Проблемы риска в техногенной и социальной сферах» (СПбГПУ 2006 г.), семинаре «Реализация жилищной политики в Ленинградской области в 2006-2007 гг.», научных семинарах кафедры Национальная безопасность ГОУ «СПбГПУ».

Основные научные результаты опубликованы в 11 научных статьях и тезисах докладов на научных конференциях.

Объем и структура. Диссертация состоит из введения, трех глав, заключения и списка использованных источников из 69 наименований.

Содержание работы

Во введении обоснована актуальность темы диссертации, сформулирована цель, определены объект и предмет, а также поставлены задачи исследования, перечислены основные научные результаты и личное участие автора в их получении, дана краткая характеристика содержания работы.

В первом разделе анализируется ресурсное обеспечение процесса подготовки офицеров запаса на факультетах военного обучения ГОУ ВПО. Показано, что в современных экономических условиях требования к уровню подготовки студентов по специальным дисциплинам может обеспечиваться только с использованием автоматизированных учебно-тренировочных ком-

плексов (АУТК) на компьютерной основе. Автором разработана упрощенная концептуальная модель перевода системы обучения из состояния «вербальный учебный процесс» в состояние «использование АУТК» (рис.1).

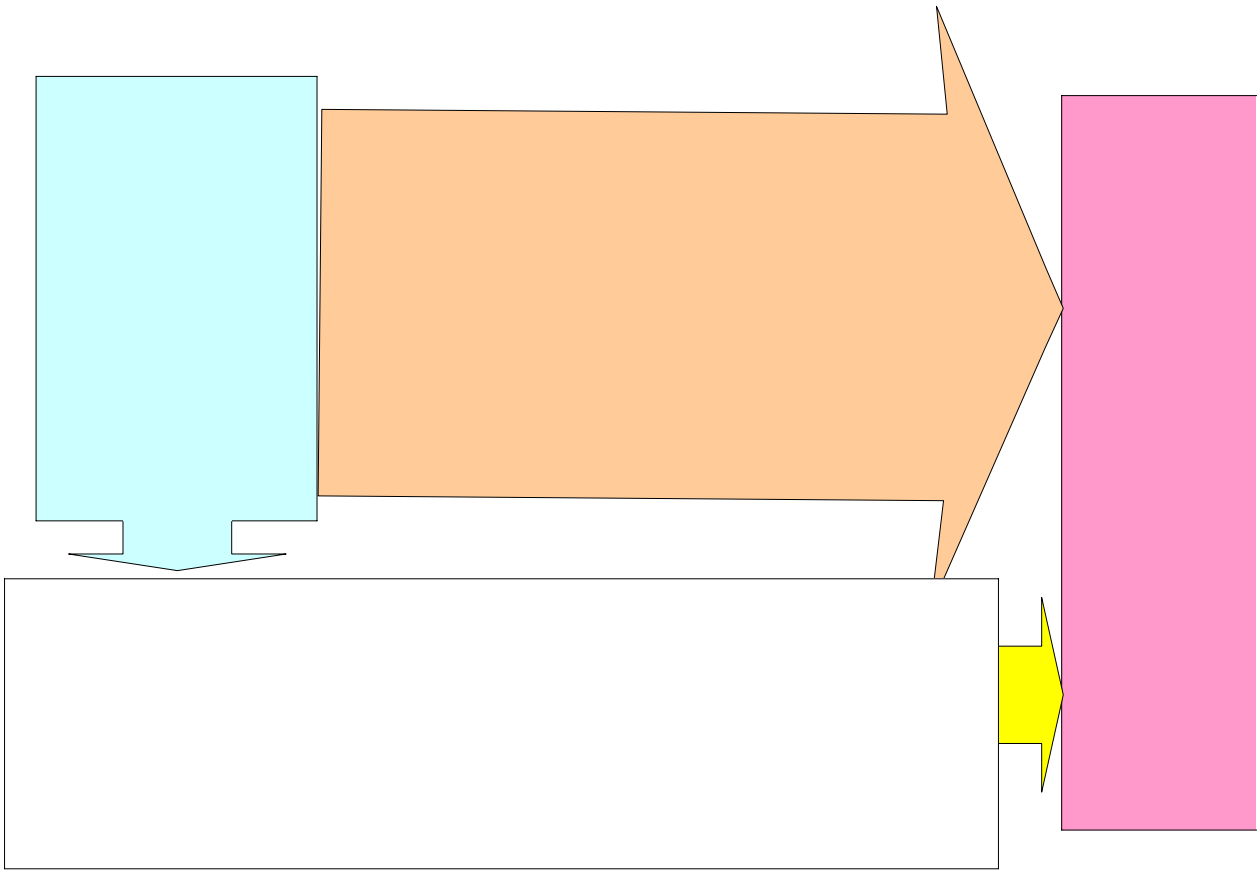


Рис.1 Модель перевода учебного процесса с использованием АУТК

Основным назначением АУТК является формирование у обучаемых представления о принципах работы и формирование навыков по применению реальных образцов вооружения и специальной техники.

Для обеспечения полной имитации всех процессов специального математическое обеспечение АУТК должно содержать фактические данные о характеристиках и возможностях соответствующих образцов специальной техники, поэтому проблема обеспечения информационной безопасности является для АУТК наиболее актуальной.

На основе анализа учебного процесса с использованием образцов военной техники и вооружения и АУТК определены роль и место системы обеспечения информационной безопасности. Определены информационные ресурсы, которые требуют особой защиты.

Проанализированы пути реализации угроз и обеспечения информацион-

ной безопасности, произведена классификация угроз и рассмотрена номенклатура отечественных и зарубежных средств их реализации и защиты.

Выявлены и рассмотрены основные проблемы защиты информации, возникающие при переходе на автоматизированные способы обучения.

Широкая номенклатура средств и способов защиты, используемых при оборудовании новых учебных объектов, различия в количественном составе персонала охраны и средств физической защиты не всегда учитывается при выделении финансовых средств. Опыт показывает, что при финансировании информационной безопасности в ГОУ ВПО принято считать, что все типы угроз считаются равнозначными.

Все это порождает основные противоречия предметной области:

– между существующими ресурсами, то есть допустимыми затратами на защиту информации, и высокими требованиями к информационной защищенности учебного процесса;

– между потребностью в достоверной количественной оценке достаточности защитных мер и возможностями существующего методического аппарата.

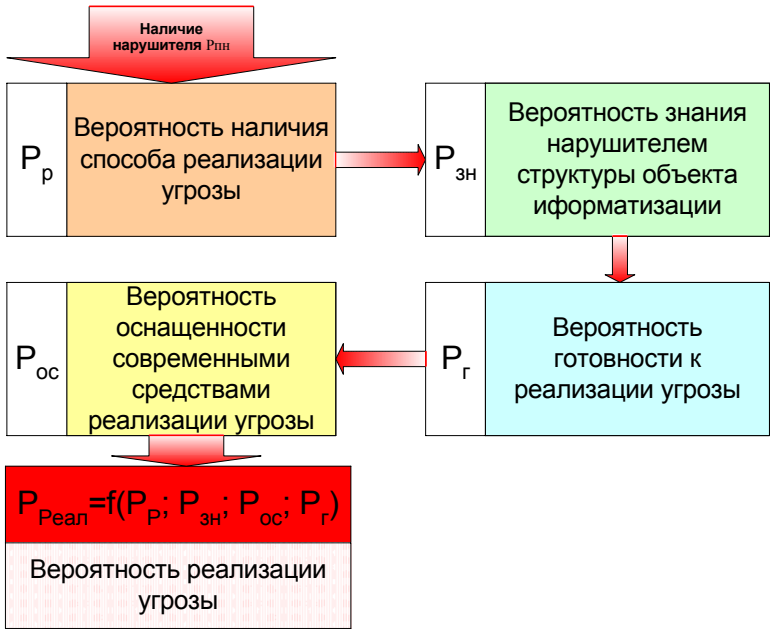
На основе анализа предметной области осуществлена постановка задачи исследования, сущность которой состоит в получении моделей и методик, позволяющих производить оценку достаточности принимаемых мер защиты учебного процесса.

Во втором разделе на основе общего методического подхода к разработке и выбору моделей формализована структура и предложен математический аппарат моделей каналов утечки конфиденциальной информации, используемой в учебном процессе ФВО ГОУ ВПО, и методов защиты информации.

С использованием информационно-логической схемы функционирования типового объекта информатизации произведена «увязка» понятий «объект-угроза – способы защиты».

В диссертационной работе разработан алгоритм учета факторов, определяющих облик нарушителя, формализована его вероятностная модель (рис.2), логика действий и математическая модель реализации угрозы конфиденциальности с учетом преодоления систем защиты.

Не подвергая ревизии существующую государственную систему контроля выполнения правил обеспечения политики информационной безопасности, обоснована необходимость наличия на типовом объекте комплексной системы мониторинга.



В общем случае мониторинг должен обеспечить выявление «брешей» в системе защиты, позволить оценить вероятность утечки конфиденциальной информации по всей совокупности каналов и дать оценку достаточности (эффективности) защитных мероприятий.

Рис.2 Структура модели нарушителя

Возможность утечки сигнала, несущего информацию конфиденциального характера (наличие «бреши» в системе защиты) предлагается оценивать с использованием математической модели вида:

$$D_{U_1} \vee D_{U_2} \vee \ldots \vee D_{U_j} \vee \ldots \vee D_{U_y} \rangle R_k ,$$

где D_{Uy} – дальность распространения информационного сигнала j-го канала; R_k – радиус контролируемой (охраняемой) зоны.

Вероятность реализации угрозы конфиденциальности $P_{\text{ут}}$ может быть рассчитана по формуле:

$$P_{\text{ут}} = 1 - \prod_{\text{j}=1}^{\text{y}} \prod_{i=1}^{I} \left(1 - P_{j.i}\right),$$

где $P_{j.i}$ – вероятность утечки информации по *j*-му каналу в *i*-м диапазоне.

Задача, стоящая перед комплексной системой защиты, может считаться выполненной при выполнении условия:

$$\frac{U_n}{U_{n_1}}(R_k) \wedge \frac{U_n}{U_{n_2}}(R_k) \wedge ... \wedge \frac{U_n}{U_{n_j}}(R_{jk}) \wedge \frac{U_n}{U_{y_2}}(R_k) \rangle 1,$$

где U_n, U_{n_j} – потенциалы полей подавления и излучения соответственно.

Данный математический аппарат модели комплексной системы мониторинга позволяет количественно оценить вероятность утечки информации по всей совокупности каналов и достаточность мер защиты.

Разработаны структура и математическая модель для оценки вероятности утечки информативного сигнала и действенности мер защиты.

С использованием методического аппарата методов исследования операций разработана математическая модель для оценки эффективности подавления технического канала утечки информативного сигнала. Сущность её заключается в том, что на основе факторного (параметрического) закона подавления радиотехнического канала утечки информативного сигнала за счет ПЭМИ, получен координатный закон подавления:

$$G(R) = \int_0^\infty G(X) \cdot f(X_R) \mathrm{dx},$$

который устанавливает зависимость между вероятностью подавления и расстоянием от точки размещения источника поля подавления ($f(X_R)$ – функция плотности распределения параметра поля подавления на расстоянии R). Вид координатного закона подавления (RPG) представлен на рис. 3.

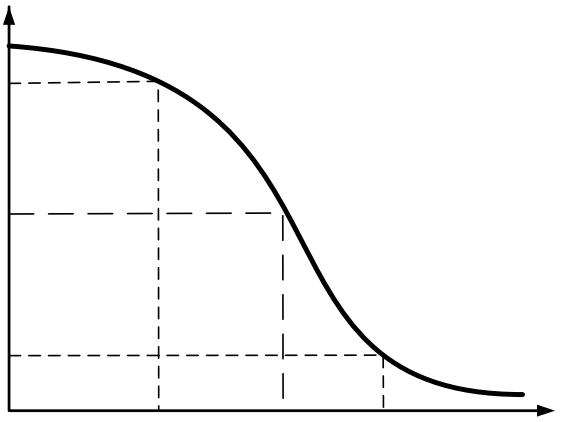
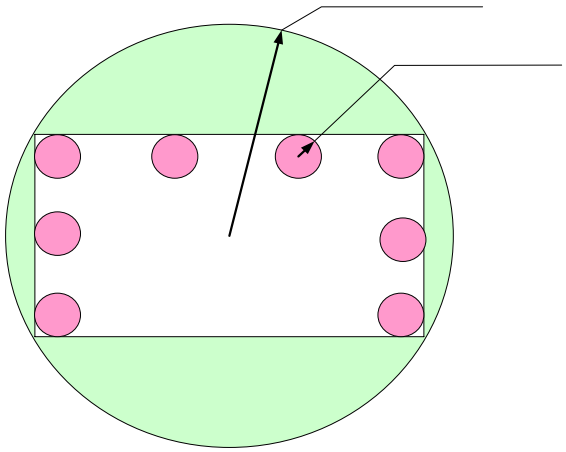


Рис. 3 Координатный закон подавления

На расстояниях $R \le R_Q$ $G(R) = 1$, что соответствует зоне безусловного подавления; при $R_Q < R \le R_{без}$ находится зона вероятного подавления, и при $R > R_{без}$ – «зона безопасности» подавляемого канала.

Основными числовыми характеристиками КЗП являются площадь ($S_{\text{п}}$) и радиус приведенной зоны подавления (рис.4) т.е. зоны, в которой каналы утечки информации подавляются достоверно.



На данном рисунке зона возможного перехвата информационного сигнала от совокупности технических средств – источников ПЭМИ аппроксимирована прямоугольником. В зависимости от степени компактности расположения таких средств, она может быть представлена в виде эллипса или круга.

Рис. 4 Графическое представление модели подавления ПЭМИ

Вполне очевидно, что потенциал поля подавления должен быть таким, чтобы

$$\mathrm{d}S_{\text{п}} = G(R)\mathrm{d}S = 2\pi R \cdot G(R)\mathrm{d}R,$$

$$S_{\text{п}} = 2\pi \int_0^{\infty} R\,G(R)\mathrm{d}R,$$

$$R_{\text{П}} = \sqrt{2\int_0^{\infty} R\,G(R)\mathrm{d}R}$$

Радиус приведенной зоны с точностью 2...3% равен расстоянию, на котором $G(R) = 0{,}5$. Это расстояние принимается за радиус подавления.

Практическое значение КЗП заключается в том, что расчет вероятности подавления сводится к расчету вероятности накрытия зоной подавления приведенной зоны распространения информативного сигнала.

<u>В третьем разделе</u> проведены исследования работоспособности предложенной модели и разработанных методик оценки достаточности защитных мероприятий по обеспечению информационной безопасности учебного процесса на ФВО.

Проанализировано содержание организационных и технических мер обеспечения информационной безопасности. Раскрыто содержание понятия «комплексная защита информации» применительно к организации учебного процесса на Факультете военного обучения (рис.5).

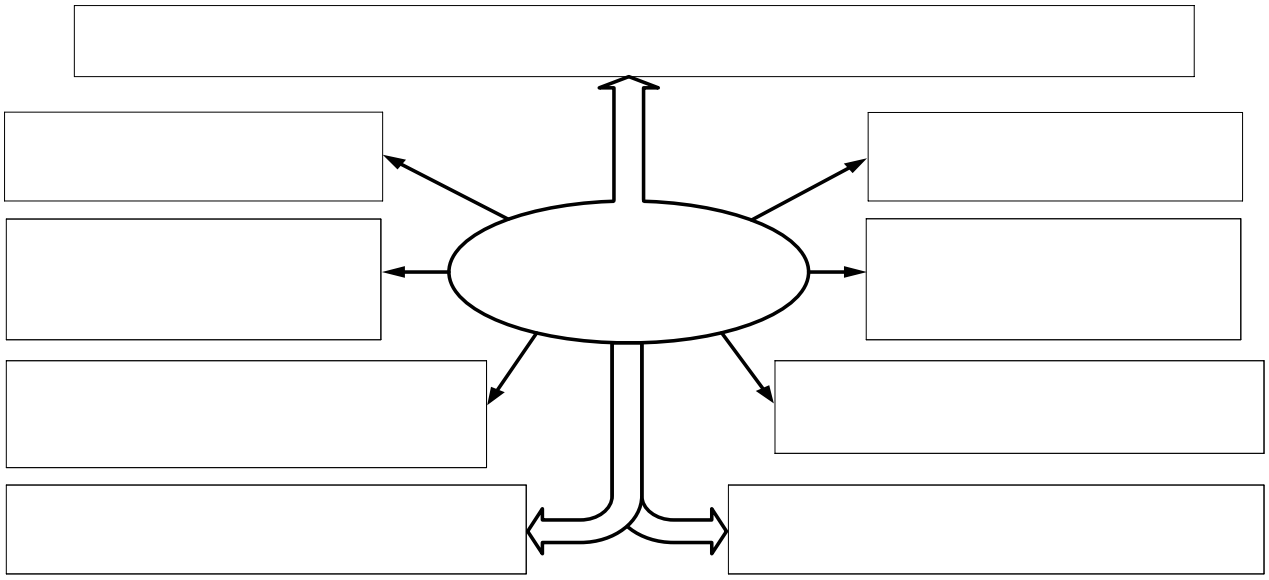


Рис.5 Схема комплексной системы обеспечения информационной безопасности учебного процесса

Принцип комплексности предполагает обеспечение защиты всех форм учебного процесса: лекционных и практических занятий, проведение тренировок с использованием АУТК.

Для достижения цели функционирования для каждой формы обучения устанавливается требуемая вероятность сохранения

$$P_c(\tau_\phi) = \prod_i P_c(t_i), \quad \tau_\phi = \sum_i t_i ,$$

где τ_ϕ – продолжительность функционирования; t_i – длительность i-го этапа функционирования; $P_c(t_i)$ – вероятность сохранения конфиденциальности на i-м этапе.

Комплексная защита предполагает наличие активной и пассивной компоненты. Показатель защищенности в этом случае описывается при помощи выражения:

$$P_{сз}(T) = 1 - \left[\left(1 - P^a_{сз}\right) \cdot \left(1 - P^n_{сз}(T)\right)\right],$$

где $P^a_{сз}, P^n_{сз}$ – вероятности сохранения, обеспечиваемые активной и пассивной защитой, соответственно.

На основе разработанной модели мониторинга степени защищенности потенциальных каналов утечки информации, предложен метод обоснования структуры Комплексной системы мониторинга (КСМ) и состава аппаратных средств, учитывающий экономический фактор. Схема алгоритма представлена на рис. 6.

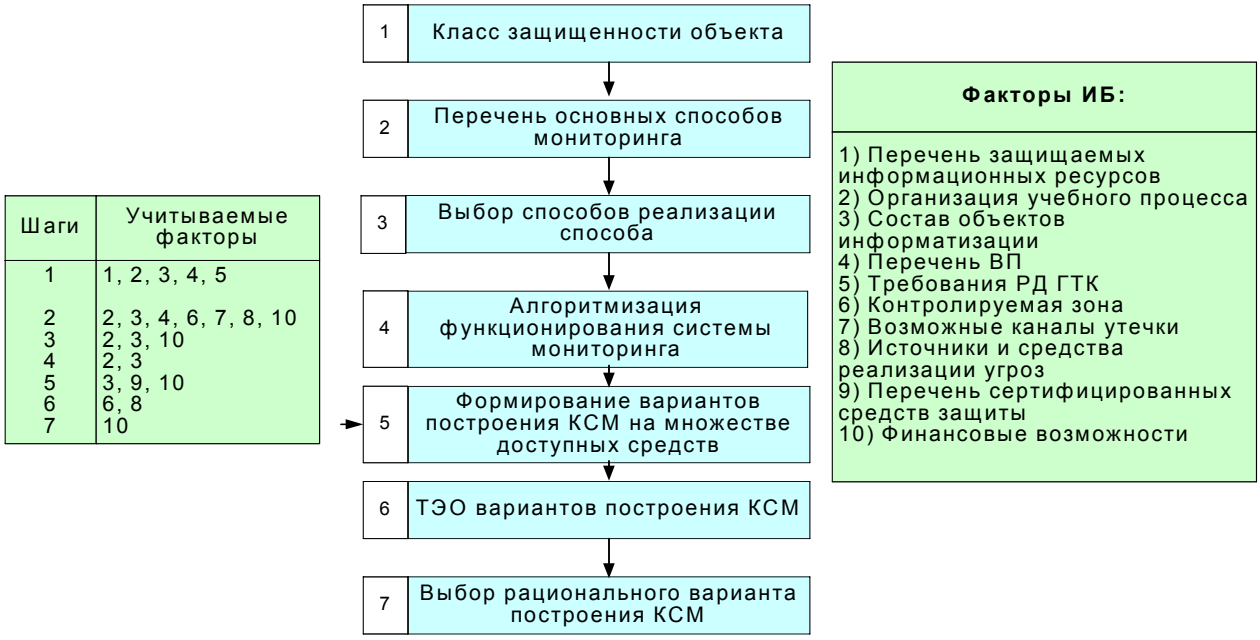


Рис.6 Схема алгоритма разработки КСМ

Практика показала, что реально существуют три основных варианта создания КСМ:

1) внедрение готовой системы («коробочный» вариант №1);

2) внедрение упрощенной системы, разработанной конкретно для заданного объекта с его управленческой структурой и элементами защиты (вариант № 2);

3) интегрированная надстройка над оперативными информационными системами, действующими в структуре управления и существующими системами (вариант №3).

Каждый из путей имеет свои достоинства и недостатки, определяющие возможность их внедрения в состав существующей системы мониторинга, сроки создания КСМ, требуемый уровень контроля надежности защиты (эффективность КСЗИ) и располагаемые финансовые ресурсы.

Технико-экономическое обоснование создания КСМ произведено путем сравнительной оценки вариантов по критерию «эффектив-

ность/стоимость» с учетом реализуемости на основе разрабатываемых, существующих и сертифицированных отечественных элементов и систем-прототипов.

Результаты технико-экономической оценки приведены в таблице.

Результаты технико-экономической оценки

№ п/п	Оцениваемые параметры	Вариант создания КСЗИ		
		№1	№2	№3
1.	Стоимость выполнения работы по созданию КСМ	Максимальная	Средняя	Минимальная
2.	Среднегодовая стоимость эксплуатации системы	Сопоставимы		
3.	Затраты на проведение мероприятий по мониторингу	Сопоставимы		
4.	Затраты на нормативно-техническое обеспечение	Максимальн.		Сопоставимы
6.	Сравнительный ориентировочный интегральный показатель стоимости (анализ доступных открытых источников, экспертные оценки)	1.0	0.6…0.4	0.4…0.2
7.	Относительный уровень эффективности КСМ	1.0	0.9…0.8	0.8…0.7
8.	Уровень контроля в наибольшей степени соответствующий требованиям руководящих документов	1.0	0.8…0.7	0.6…0.4
9.	Сравнительные относительные сроки создания КСМ на новом объекте	1.0	0.7…0.5	0.6…0.3

В работе предлагается рассматривать комплексную систему мониторинга в качестве составной части комплексной системы обеспечения информационной безопасности учебного процесса на ФВО**.** Предложена технология оценки достаточности мер защиты, включающая:

– методику определения степени опасности угрозы конфиденциальности информации, с использованием которой проведен практические вычисления по ранжированию технических каналов утечки информации;

– методику оценки эффективности защиты от утечки информации за счет ПЭМИ.

Анализ показал, что с достаточной для практики точностью задача оценки эффективности защиты данного канала утечки может быть решена графическим способом. Сущность его заключается в том, что, используя технические средства мониторинга побочных электромагнитных излучений и наводок (ПЭМИН), применительно к конфигурации определяются излучающие «точки» и радиусы распространения информативного сигнала. Получен-

ные инструментальным методом зоны излучения наносятся на план выделенного помещения. Зона возможного распространения информативных сигналов аппроксимируется одной их фигур (квадрат, эллипс, круг).

Из состава номенклатуры доступных средств защиты выбираются (один или несколько экземпляров) удовлетворяющих требованиям по ТТХ и стоимости.

Определяются размеры зон подавления, а затем с использованием стандартных процедур или методом прямого перебора находятся рациональные точки установки источника полей подавления, при которых обеспечивается выполнение условия

$$S_{\text{п}} = \sum_{j}^{y} \frac{S_{\text{п j}}}{\text{S}_{\text{и}}} \geq 1 ,$$

где: $S_{\text{п j}}$, $\text{S}_{\text{и}}$ – площади приведенных зон подавления и излучения соответственно.

Варианты различных оценок представлены на рис. 7.

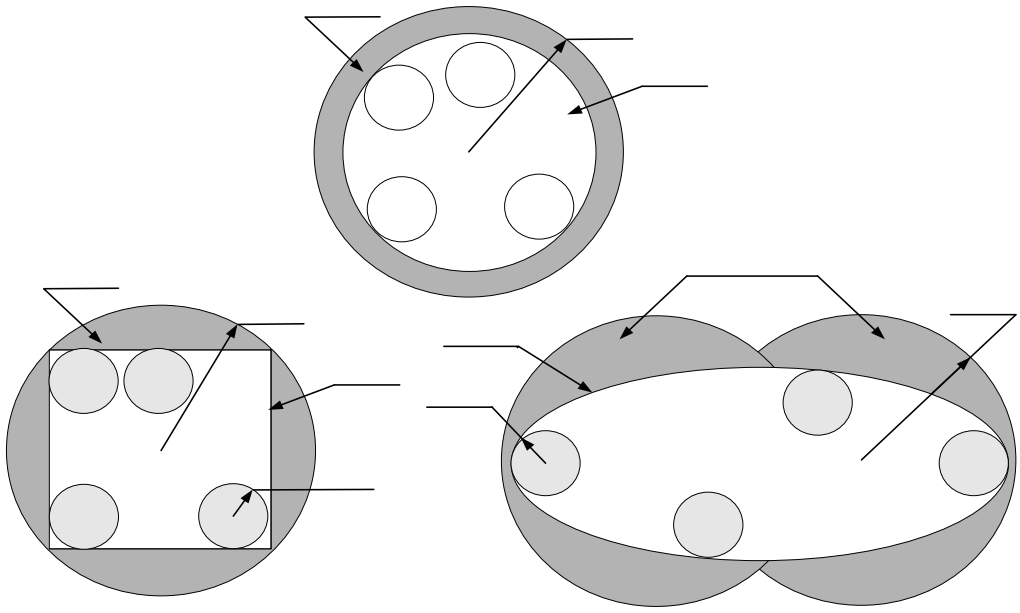


Рис. 7. Варианты оценки эффективности защиты технического канала

На основе практических данных определены оценки достаточности мер обеспечения информационной безопасности и вклада различных защитных мероприятий (рис. 8).

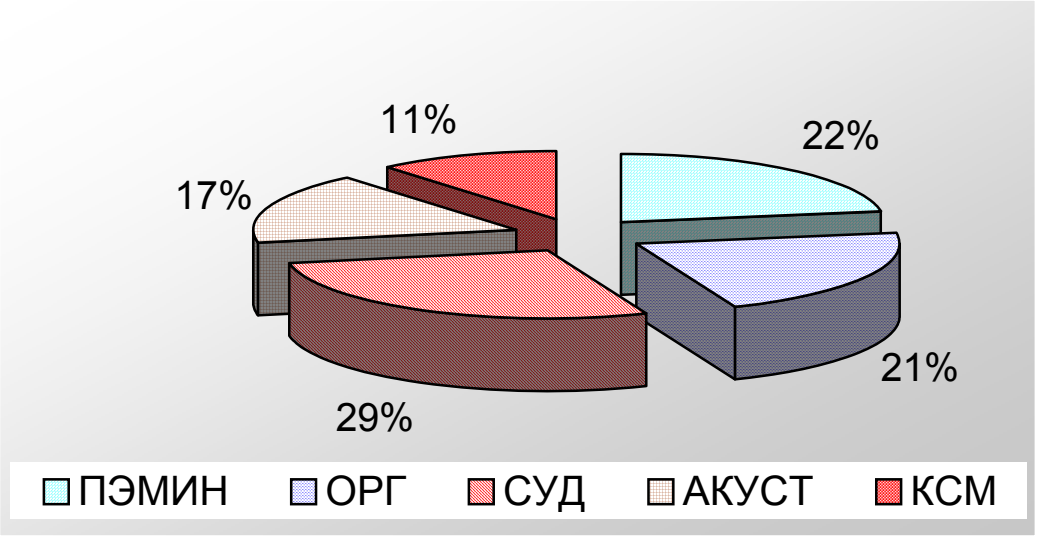


Рис.8 Вклад отдельных защитных мероприятий в создание защищенной среды проведения учебного процесса

На основе предложенной модели и методик разработаны и обоснованы практические рекомендации по повышению уровня защищенности учебного процесса по специальным дисциплинам с использованием компьютерной тренажерной техники и макетов вооружения и военной техники.

Заключение включает перечисление решенных задач, полученные научные результаты, отмечается их новизна и достоверность, теоретическая и практическая значимость, апробация и публикация, внедрение и реализация, сделан вывод о достижении цели исследования.

В работе получены следующие основные научные результаты:

– на основе формализованного представления учебного процесса на факультетах военного обучения Государственных образовательных учреждений высшего профессионального образования проанализированы критические информационные ресурсы и обоснованы реальные угрозы конфиденциальности информации;

– проанализированы пути реализации угроз конфиденциальности сведений, используемых в учебном процессе;

– разработаны модели угроз, система мониторинга, предложены рекомендации для организационных и технических мер защиты;

– предложена методика оценки достаточности мер защиты;

– проведены вычислительные эксперименты, подтвердившие работоспособность модельного и методического ряда;

– по результатам количественных оценок и качественного анализа выданы научно-обоснованные рекомендации по повышению информационной безопасности учебного процесса с использованием АУТК.

Основные научные работы, опубликованные по теме диссертации

Публикации в изданиях по перечню ВАК Минобрнауки РФ

1. Супрун А.Ф., Матвеев В.В., Ермилов В.В. Организационные и технические меры защиты учебного процесса по специальным дисциплинам на факультетах военного обучения. /А.Ф. Супрун// Проблемы информационной безопасности. Компьютерные системы.- СПб: Изд-во СПбГПУ, 2006.-№ 3.- С. 101-107. (№ 726 по перечню ВАК РФ)

Статьи и тезисы докладов

2. Супрун А.Ф., Матвеев В.В. Обоснование моделей каналов утечки информации. /А.Ф. Супрун// Материалы конференции в рамках XXXV Недели науки СПбГПУ.- СПб: Изд-во СПбГПУ, 2006.- С. 126-132.

3. Супрун А.Ф., Матвеев В.В. Алгоритм учета факторов, определяющих категорию нарушителя информационной безопасности в структуре органа муниципального управления. /А.Ф.Супрун// Материалы семинара «Реализация жилищной политики в Ленинградской области в 2006-2007гг.: Изд-во СПб, 2006.- С. 93-95.

4. Супрун А.Ф. О защите информации в экономической системе управления мегаполисом. /А.Ф. Супрун// Материалы семинара «Реализация жилищной политики в Ленинградской области в 2006-2007гг.»: Изд-во СПб, 2006.- С. 95-97.

5. Супрун А.Ф. Кляхин В.Н., Матвеев В.В., Копачева М.В. Один из подходов к формированию модели носителя угрозы информационной безопасности в управленческих структурах различного уровня. /А.Ф. Супрун// Материалы X Всероссийской конференции по проблемам науки и высшей школы. «Фундаментальные исследования в технических университетах.» Национальная безопасность.: Изд-во НП «Стратегия будущего» СПб, 2006.- Т. 2. Часть 2.- С. 162-167.

6. Супрун А.Ф., Матвеев В.В. Разработка структуры, графа и математической модели защиты технических каналов утечки./А.Ф. Супрун// Материалы XXXV Недели науки СПбГПУ.: Изд-во СПбГПУ, 2006.- С. 18-22.

7. Супрун А.Ф. Необходимость и способы защиты информации в учебном процессе факультетов военного обучения. Проблемы риска в техногенной и социальной сферах./А.Ф. Супрун// Материалы конференции. Вып.4.: Изд-во СПбГПУ, 2005.- С. 103-112.

8. Матвеев В.В., Супрун А.Ф. Рекомендации по обеспечению информационной безопасности учебного процесса на ФВО ГОУ ВПО. Проблемы риска в техногенной и социальной сферах. ./А.Ф. Супрун// Материалы конференции. Вып.4. :Изд-во СПбГПУ, 2005.- С. 34-39.

9. Матвеев В.В., Супрун А.Ф. Новый вызов политике информационной безопасности. /А.Ф.Супрун// Материалы VIII Всероссийской конференции по проблемам науки и высшей школы. Фундаментальные исследования в технических университетах. Национальная безопасность. 26-27 мая 2004. Т. 2. Часть 1.: Изд-во СПбГПУ, 2004.- С. 29-36.

10. Супрун А.Ф., Каверзнева Т.Т. Проблемы вибрационной защиты. /А.Ф. Супрун// Сборник трудов Второй Всероссийской научно-практической конференции с международным участием «Новое в экологии и безопасности жизнедеятельности». 20-22 мая 1997 г. Т.3.: Изд-во МЦЭНТ СПб, 1997.- С. 190-193.

11. Супрун А.Ф., Захаров С.Г. Человек и его безопасность в условиях электромагнитных излучений. /А.Ф.Супрун//: Изд-во СПбГТУ, 1996.-С.10-53.