

замечание – большое количество таких пулов сильно загрузит оперативную память.

Заключение

После применения данного способа оптимизации удалось получить ~ + 6.6 fps. Главной характеристикой такого подхода оптимизации является повышение стабильности fps, что видно из рис. 4–5.

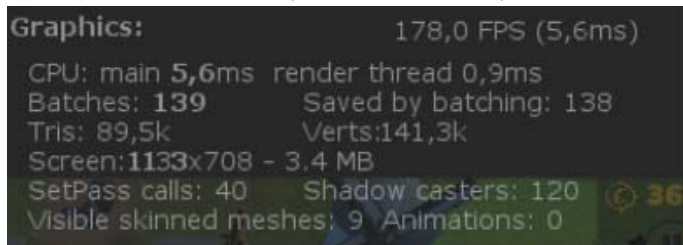


Рис. 4. До использования пула



Рис. 5. После использования пула

Список литературы

1. Документация компании разработчика движка Unity3D [Электрон. ресурс]. – Режим доступа: <https://docs.unity3d.com>.
2. Alexander Shvets «Dive Into Design Patterns».
3. [http://it.mmcs.sfedu.ru/wiki/Пул_объектов_\(Object_Pool\)](http://it.mmcs.sfedu.ru/wiki/Пул_объектов_(Object_Pool)).

ПО ПРОЕКТИРОВАНИЮ КСЗИ ДЛЯ ОБЪЕКТА ЗАЩИТЫ



Тихомиров Александр Олегович

Студент 5-го курса направления «Информационная безопасность автоматизированных систем», Московского политехнического университета



Гневшев Александр Юрьевич

Старший преподаватель кафедры «Информационная безопасность» Московского политехнического университета

Аннотация. Данная статья посвящена проблеме разработки комплексной системы защиты информации для объекта защиты, а конкретнее оптимизации данного процесса. Проанализированы зарубежные и отечественные аналоги. Разработан подбор элементов защиты информации при проектировании комплексной системы защиты информации для объекта защиты. Сформирована база знаний уязвимостей и необходимых рекомендаций по защите информации на объекте.

Ключевые слова: КСЗИ, уязвимость, объект защиты, угроза, средство защиты, помещение, ПО, технические средства защиты, жизненный цикл.

Annotation. This article is devoted to the problem of developing an integrated information security system for a protected object, and more specifically to optimizing this process. Foreign and domestic analogues are analyzed. The selection of information security elements in the design of an integrated information security system for a protected object has been developed. A knowledge base of vulnerabilities and necessary recommendations for protecting information at the facility has been formed.

Keywords: CSIS, vulnerability, object of protection, threat, means of protection, premises, software, technical means of protection, life cycle.

Введение

Комплексная система защиты информации (КСЗИ) – совокупность организационных и инженерно-технических мероприятий, которые направлены на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа.

Система – выполняет определенную функцию и обеспечивает выполнение функций отдельных компонентов.

Главная цель создания системы защиты информации – ее надежность. Но компоненты ЗИ, с одной стороны, являются составной частью системы, с другой – сами организуют систему, осуществляя защитные мероприятия.

Предпроектная стадия:

1. Разработка ТЭО (технически экономического обоснования) на этом этапе анализируется деятельность объекта и готовятся исходные данные для ТЭО. Главное – обоснование целесообразности и необходимости создания проекта, ориентировочный выбор защищаемых каналов (и их обоснование), определение объема и состав работ о создании СЗИ, а также определённые сметы и сроков работы. P.S. принцип экономичности – ИБ не дороже информации, принцип рациональности – минимизации затрат на меры защиты.

2. Разработка технического задания, на этом этапе происходит разработка и обоснование требований к структуре СЗИ и обеспечение совместимости и взаимодействия всех средств. Главное – сбор и подготовка исходных данных, определение состава системы, плана её создания и оценка затрат. Разработка ТЗ происходит после ТЭО.

Стадия проектирования

1. Эскизный проект, в случаях, когда большой и сложный по устройству объект.

2. Разработка технического проекта. На этом этапе разрабатываются и обосновываются все проектные решения. Разработан и обоснован выбранный вариант проекта; уточнены перечни технических средств, порядок и сроки их поставки. В техническом проекте могут рассматриваться 2–3 варианта решения поставленной задачи по созданию системы защиты. Все варианты должны сопровождаться расчетом эффективности, на основе которого могут быть сделаны выводы о рациональном варианте. При создании системы защиты небольшого или простого объекта этап технического проектирования может быть исключен, как и этап эскизного проектирования.

3. Разработка рабочего проекта имеет своей целью детализировать проектные решения, принятые на предыдущем этапе.

Именно на стадии проектирования будет возможность использовать разработанное ПО проектирования КСЗИ для объекта защиты в целях оптимизации процесса выбора решения, расчёта эффективности и экономических затрат.

Цель

1. Разработать программу по проектированию КСЗИ для объекта защиты

Задачи

1. Провести сравнительный анализ зарубежных и отечественных аналогов. Оценить востребованность разрабатываемого ПО.

2. Разработать подбор элементов защиты информации при проектировании комплексной системы защиты информации для объекта защиты.

3. Сформировать базу знаний уязвимостей и необходимых рекомендаций по защите информации на объекте.

Сравнительный анализ зарубежных и отечественных аналогов

и оценка востребованности разработанного ПО

При помощи Интернет-ресурсов и всевозможной литературы был проведен поиск зарубежных и отечественных аналогов разработанного ПО проектирования КСЗИ для объекта защиты. В результате поисков существующих разработанных аналогов найдено не было, так как подобного ПО не существует на рынке ни за рубежом, ни у отечественного производителя.

На данный момент при проектировании комплексной системы защиты информации вся оценка уязвимостей объекта защиты, рекомендации по решению, подбор оборудования и материалов для улучшения защищенности помещения производится вручную специалистом по ИБ. Этот подход не является оптимальным, по причине трудоемкости и затрат времени, а также не исключён человеческий фактор ошибки в расчётах или же подбор не оптимального оборудования и материалов по параметрам цена/качество.

Полностью исключить специалиста в области информационной безопасности из процесса проектирования КСЗИ нельзя, но можно существенно сократить затраты времени на разработку.

Развитие КСЗИ во времени отражает такая категория, как жизненный цикл (ЖЦ) – одно из базовых понятий методологии проектирования ИС.

Жизненный цикл КСЗИ – это непрерывный процесс, который начинается с момента принятия решения о необходимости создания системы и заканчивается в момент ее полного изъятия из эксплуатации (обычно в результате морального устаревания).

Процесс создания и сопровождения системы представляется как некоторая последовательность этапов и выполняемых на них процессов. Для каждого этапа определяются состав и последовательность выполняемых работ, получаемые результаты, методы и средства, необходимые для выполнения работ, роли и ответственность участников и т.д. Такое формальное описание ЖЦ позволяет спланировать и организовать процесс коллективной разработки и обеспечить управление этим процессом.

В жизненном цикле выделяют следующие стадии:

- 1) разработка требований;
- 2) проектирование;
- 3) реализация и тестирование;
- 4) внедрение;
- 5) сопровождение.

Жизненный цикл носит итеративный характер: реализованные этапы ЖЦ, начиная с самых ранних, циклически повторяются в соответствии с новыми требованиями и изменениями внешних условий. На каждом этапе ЖЦ формируется набор документов и технических решений, которые являются исходными для последующих решений.

Наибольшее распространение получили три модели ЖЦ:

- каскадная модель, в которой переход на следующий этап означает полное завершение работ на предыдущем этапе. Основным недостатком этого подхода является существенное запаздывание с получением результата;
- поэтапная модель с промежуточным контролем – итерационная модель разработки системы с циклами обратных связей между этапами, допускающие возвраты к предыдущему этапу. В результате каждый из этапов может растянуться на весь период разработки;
- спиральная модель, в которой каждый виток спирали соответствует созданию работоспособного фрагмента или версии системы. Это позволяет уточнить требования, цели и характеристики проекта, определить качество разработки, спланировать работы следующего витка спирали и в результате выбрать оптимальный вариант системы, удовлетворяющий требованиям заказчика, и довести его до реализации. Основная проблема – определение момента перехода на следующий этап.

ПО проектирования КСЗИ для объекта защиты можно использовать при любом жизненном цикле КСЗИ. Так как использование данного ПО имеет следующие преимущества и недостатки, представленные в табл. 1.

Таблица 1

Преимущества и недостатки ПО проектирования КСЗИ для объекта защиты

Преимущества	Недостатки
<ul style="list-style-type: none"> • База нормативных показателей звукоизоляции • Автоматическое сравнение показателей • Вычисление и предоставление информации о имеющихся не соответствиях нормам • Предоставление рекомендуемого оборудования и материалов от партнеров для устранения уязвимостей • Примерный расчёт экономических затрат 	<ul style="list-style-type: none"> • Обучение сотрудника использованию ПО • Ввод исходных данных после первичного анализа объекта защиты

Разработать подбор элементов защиты информации при проектировании комплексной системы защиты информации для объекта защиты

Для обеспечения защиты информации в помещении необходимо провести анализ звукоизоляции помещения. Сравнив звукоизоляцию объекта защиты с нормативными показателями стен, окон и дверей на рис. 1–3 ниже.

№ п/п	Элементы конструкций	Примечание	Звукоизоляция (дБ) на частотах, Гц				
			250	500	1000	2000	4000
1	Кирпичная кладка	0,5 кирпича	40	42	48	54	60
		1,0 кирпича	44	51	58	64	65
		1,5 кирпича	48	55	61	65	65
		2,0 кирпича	52	59	65	70	70
		2,5 кирпича	55	60	67	70	70
2	Стена (0,5 кирпича, гипсолитовые плиты толщиной 8 мм, обои)	Без отверстий	38	49	57	59	52
		С незаделанными отверстиями для воздухопровода	36	46	52	53	50
		С незаделанными отверстиями под электропроводку	35	44	51	62	48
3	Железобетонная плита	40 мм	36	35	38	47	53
		100 мм	40	44	50	55	60
		160 мм	47	51	60	63	-
		200 мм	44	51	59	65	65
		300 мм	50	58	65	69	69
		400 мм	55	61	67	70	70
		800 мм	61	68	70	70	70
4	Межэтажное перекрытие из бетонных плит	Незаделанные щели между плитами, сколот угол одной из плит	43	40	39	57	40
5	Стена из шлакоблоков	220 мм	42	48	54	60	63
6	Перегородка из древесно-стружечной плиты	20 см	26	26	26	26	26

Рис. 1. Нормативные показатели стен

№ п/п	Конструкция	Примечание	Звукоизоляция (дБ) на частотах, Гц				
			250	500	1000	2000	4000
1	Одинарное остекление	3 мм	17	22	28	31	32
		4 мм	23	26	31	32	32
		6 мм	22	26	30	27	25
2	Двойное остекление с воздушным промежутком	57 мм (толщина 3 мм)	20	32	41	49	46
		90 мм (толщина 3 мм)	29	38	44	50	48
		170 мм (толщина 3 мм) (с прокладками)	33	36	38	38	38
		57 мм (толщина 4 мм)	31	38	46	49	35
		90 мм (толщина 4 мм)	33	41	47	48	36
		100 мм (толщина 4 мм) (с герметизацией)	35	39	47	46	52
		200 мм (толщина 4 мм) (с прокладками)	36	41	47	49	55
300 мм (толщина 4 мм) (с прокладками)	39	43	47	51	55		
3	Стеклопакет	Толщина 98 мм (с прокладками)	40	42	45	48	50

Рис. 2. Нормативные показатели окон

№ п/п	Конструкция	Примечание	Звукоизоляция (дБ) на частотах, Гц				
			250	500	1000	2000	4000
1	Обыкновенная филеичатая дверь	Без прокладок	14	16	22	22	20
		С прокладками	19	23	30	33	32
2	Глухая щитовая дверь толщиной 40 мм, облицованная с двух сторон фанерой толщиной 4 мм	Без прокладок	23	24	24	24	23
		С прокладками	27	32	35	34	35
3	Типовая дверь	Без прокладок	23	31	33	34	36
		С прокладками	30	33	35	39	41
4	Щитовая дверь из древесноволокнистых плит толщиной 4 – 6 мм с воздушным зазором 50 мм, заполненным стекловатой	Без прокладок	26	30	31	28	29
		С прокладками	30	33	36	32	30
5	Дверь звукоизолирующая облегченная	Одинарная	30	39	42	45	43
		Двойная с зазором более 200 мм	42	55	58	60	60
6	Дверь звукоизолирующая тяжелая	Одинарная	36	45	51	50	49
		Двойная с зазором более 300 мм	46	60	60	65	65
		Двойная с облицовкой тамбура	58	65	70	70	70

Рис. 3. Нормативные показатели дверей

Проведя сравнительный анализ вводных данных звукоизоляции объекта защиты и нормативных показателей. Выявим необходимость замены или установки средств защиты информации для стен, окон или дверей.

Сформировать базу знаний уязвимостей и необходимых рекомендаций по защите информации на объекте

Перед определением необходимости использования СЗИ определяются источники канала утечки информации. Пример смотри в табл. 2.

Эти данные в разрабатываемом ПО будут заполняться, посредством тестового бланка, наличие того или иного технического оборудования или объектов в помещении будут говорить об источниках каналов утечки информации на объекте защиты.

На основе полученных данных приводятся несколько возможных вариантов рекомендаций по реализации защиты информации на объекте защиты.

Таблица 2

Каналы утечки информации

Источник канала утечки информации	Наименование канала утечки информации	Краткое описание
• Телефонные линии • Радиотелефон	Электроакустический, ПЭМИН	• Утечка информации за счет акустоэлектрического преобразования в приемнике линии радиотрансляции; • Утечка информации за счет модуляции полезным сигналом ЭМ-полей, образующихся при работе бытовой техники
• Динамик оповещения • Пожарный извещатель	Электроакустический, ПЭМИН	• Утечка информации за счет акустоэлектрического преобразования в приемнике линии радиотрансляции • Утечка информации за счет модуляции полезным сигналом ЭМ-полей, образующихся при работе бытовой техники
ПЭВМ с полной конфигурацией	ПЭМИН	• Утечка информации за счет модуляции полезным сигналом ЭМ-полей, образующихся при работе бытовой техники.
Проектор	Электроакустический, ПЭМИН	• Утечка информации за счет акустоэлектрического преобразования в приемнике линии радиотрансляции • Утечка информации за счет модуляции полезным сигналом ЭМ-полей, образующихся при работе бытовой техники.
Система отопления и вентиляции	Электроакустический	• Утечка информации за счет акустоэлектрического преобразования в приемнике линии радиотрансляции;
Стены смежных помещений	Акустический	• Мембранный перенос энергии речевых сигналов через перегородки за счет слабого затухания сигнала на низких частотах.
Дверь	Акустический	• Мембранный перенос энергии речевых сигналов через перегородки за счет малой массы и слабого затухания сигнала.
Телевизор	Электроакустический, ПЭМИН	• Утечка информации за счет акустоэлектрического преобразования в приемнике линии радиотрансляции; • Утечка информации за счет модуляции полезным сигналом ЭМ-полей, образующихся при работе бытовой техники.
Аппаратное оборудование	НСД	• Утечка информации за счет несанкционированного доступа с помощью различных средств к ЭВМ
Пожарный ИП и громкоговоритель	Акустоэлектрический	• Утечка информации за счет акустоэлектрического преобразования в приемнике линии радиотрансляции;
Окна	Акуствибрационный	Утечка информации за счет акуствибрационного преобразования на конструкционных объектах;

Товар	Устройство защиты аналоговых телефонных аппаратов "Корунд"	Устройство защиты МП-1А	Устройство защиты от НСД МП-8 "Сигма-РА"
Изображение			
Цена	1750	4600	9900
Модель	"Корунд"	Устройство защиты МП-1А	Устройство защиты от НСД МП-8 "Сигма-РА"
Производитель			
Наличие	Есть на складе	Есть на складе	Есть на складе
Рейтинг	 На основе 0 отзывов.	 На основе 0 отзывов.	 На основе 0 отзывов.
Краткое описание	Устройство защиты "Корунд" предназначено для исключения утечки информации через абонентскую линию аналоговых АТС и защиты от подслушивания речи людей или прослушивания любых других звуков с использ...	Устройство защиты аналоговых телефонных аппаратов. Сертификат ФСТЭК. Устройство МП-1А предназначено для защиты телефонного аппарата, находящегося в режиме ожидания вызова, от утечки чер...	Устройство защиты аналоговых телефонных аппаратов от НСД. Устройство МП-8 «Сигма-РА» предназначено для защиты телефонного аппарата, находящегося в режиме ожидания вызова, от утечки через него ...
Вес	0.00кг	0.00кг	0.00кг
Размеры (Д x Ш x В)	0.00мм x 0.00мм x 0.00мм	0.00мм x 0.00мм x 0.00мм	0.00мм x 0.00мм x 0.00мм

Рис. 4. Варианты защиты телефонной линии

Опираясь на каналы утечки информации предоставляются рекомендации по установке средств защиты информации. Например, если дверь в помещение не удовлетворяет нормативному показателю звукоизоляции, её необходимо заменить. ПО предоставляет несколько вариантов.

Также будет предоставляться ссылка на сайт для покупки рекомендованного оборудования. База знаний рекомендаций собирается из необходимых средств для защиты объекта.

В базе хранятся не только возможные варианты рекомендуемого оборудования, но и их характеристика (см. рис. 4).

Заключение

Проведя сравнительный анализ зарубежных и отечественных аналогов было выявлено их отсутствие. Данное ПО будет востребовано среди специалистов по информационной безопасности, так как

оно оптимизирует работу над технической защитой объекта.

Описан алгоритм подбора средств защиты информации, опирающийся на нормативные показатели звукоизоляции помещения и защиту других возможных каналов утечки информации.

Сформирована база знаний рекомендаций по защите каналов утечки информации.

Список литературы

1. Гришина Н.В. Организация комплексной системы защиты информации / Н.В. Гришина.
2. Моделирование комплексной системы защиты информации [Электрон. ресурс]. – Режим доступа: <https://studfile.net/preview/8103080/> (дата обращения: 15.03.2020).
3. Грибунин В.Г. Комплексная система защиты информации на предприятии / В.Г. Грибунин, В.В. Чудовский.

ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ: СТРУКТУРНЫЙ АНАЛИЗ



Златковская Евгения Михайловна

Студентка 4-го курса по профилю «Корпоративные информационные системы» Московского политехнического университета

Аннотация. В статье рассматривается задача повышения эффективности управления информационно-управляющих систем, а именно повышение эффективности процесса принятия, обработки и выполнения заявок технической поддержки пользователей при обеспечении электронного документооборота.

Ключевые слова: образование, документооборот, электронный документооборот, менеджмент, информационная система.