МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_8_»_08_____2023 г.

Организация аудита информационной безопасности

Методические указания по выполнению практических работ по дисциплине «Организация аудита информационной безопасности» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Организация аудита информационной безопасности: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 29 с.: Библиогр.: с. 29.

Содержат сведения по вопросам формирования у студентов знаний по основам организации аудита информационной безопасности, а также развития в процессе обучения системного мышления, необходимого для решения задач управления в области информационной безопасности.

Методические указания по выполнению практических работ по дисциплине «Организация аудита информационной безопасности» предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции
Подписано в печать . Формат 60x84 1/16.
Усл. печ.л. . Уч. –изд.л. .Тираж 50 экз. Заказ .
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Практическая работа №1
на тему: «Определение класса государственной информационной системы (ГИС)».

Цель работы:

определение класса государственной информационной системы (ГИС).

Требования к выполнению задания:

Ознакомиться и изучить основные принципы разработки организационно-правовых аспектов деятельности службы защиты информации.

Задание:

Выбрать самостоятельно организацию и информационную систему в ней сделать описание системы и провести ее классификацию.

Ход работы:

1**Определение уровня защищенности персональных данных.**

Текст классификации формируется строго с формулировками из ПП №1199.

Тип угроз:

− определяется в Модели угроз и дублируется в Акте определения возможностей.

Итоговый уровень защищенности персональных данных определяется по следующей схеме:

НЕ работники	**угрозы 1 типа**	**угрозы 2 типа**	**угрозы 3 типа**	**Работники**
	Угрозы с НДВ ОС	**Угрозы с НДВ СПО**	**Угрозы БЕЗ НДВ**	
специальные категории	**1УЗПДн**			специальные категории
специальные категории персональных данных **более** чем 100000		**1УЗПДн**		
специальные категории персональных данных **менее** чем 100000		**2УЗПДн**		специальные категории
специальные категории персональных данных **более** чем 100000			**2УЗПДн**	
специальные категории персональных данных **менее** чем 100000			**3УЗПДн**	специальные категории
биометрические	**1УЗПДн**			биометрические
биометрические		**2УЗПДн**		биометрические
биометрические			**3УЗПДн**	биометрические
иные категории	**1УЗПДн**			иные категории
иные категории персональных данных **более** чем 100000		**2УЗПДн**		
иные категории персональных данных **менее** чем 100000		**3УЗПДн**		иные категории
иные категории персональных данных			**3УЗПДн**	

НЕ работники	угрозы 1 типа	угрозы 2 типа	угрозы 3 типа	Работники
более чем 100000				
иные категории персональных данных **менее** чем 100000			**4УЗПДн**	иные категории
общедоступные	**2УЗПДн**			общедоступные
общедоступные персональные данные **более** чем 100000		**2УЗПДн**		
общедоступные персональные данные **менее** чем 100000		**3УЗПДн**		общедоступные
общедоступные			**4УЗПДн**	общедоступные

Определение класса защищенности

п.1.1. – в большинстве случаев будет персональные данные (но могут быть несколько видов информации, по количеству видов информации ограниченного доступа)

п.1.2. – расставляется по 1 плюсу в каждом столбце в нужной строке, в соответствии с экспертной оценкой для конкретной системы. Соответствие:

существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять **возложенные на них функции**	**Высокая**
умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять **хотя бы одну из возложенных на них функций**	**Средняя**
незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) оператор (обладатель информации) могут выполнять возложенные на них функции **с недостаточной эффективностью** или выполнение функций возможно только **с привлечением дополнительных сил и средств**	**Низкая**

п.1.3. – оценка общего УЗ (уровня значимости информации) – он устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации. Соответствие:

хотя бы для **одного** из свойств безопасности информации (конфиденциальности, целостности, доступности) определена **высокая степень ущерба**	УЗ 1

хотя бы для **одного** из свойств безопасности информации (конфиденциальности, целостности, доступности) определена **средняя степень ущерба** и нет ни одного свойства, для которого определена высокая степень ущерба	УЗ 2
для **всех** свойств безопасности информации (конфиденциальности, целостности, доступности) определены **низкие степени ущерба**	УЗ 3
обладателем информации (заказчиком) и (или) оператором степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) **не может быть определена**, но при этом информация **подлежит защите** в соответствии с законодательством Российской Федерации	УЗ 4

При обработке в ИС двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) УЗ определятся отдельно для каждого вида информации.

п.1.4. – оценка масштаба системы из трёх возможных. Варианты:

Информационная система имеет:	**Если она:**
федеральный масштаб	функционирует на территории Российской Федерации (в пределах федерального округа) **и** имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях
региональный масштаб	функционирует на территории субъекта Российской Федерации и имеет сегменты **в одном или нескольких** муниципальных образованиях **и (или)** подведомственных и **иных** организациях
объектовый масштаб	функционирует **на объектах одного** федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации **и не имеет** сегментов в территориальных органах, представительствах, филиалах, подведомственных и **иных** организациях

п. 1.5. – присвоение класса защищенности информационной системы по табличке сопоставления УЗ и масштаба. Соответствие:

Уровень значимости информации	**Масштаб информационной системы**		
	Федеральный	**Региональный**	**Объектовый**
УЗ 1	**К1**	**К1**	**К1**
УЗ 2	**К1**	**К2**	**К2**
УЗ 3	**К2**	**К3**	**К3**
УЗ 4	**К3**	**К3**	**К4**

Сравнение получившихся значений по первой и второй классификации.

В случае, если определенный в установленном порядке уровень защищенности персональных данных выше, чем установленный класс защищенности государственной информационной системы, то осуществляется повышение класса защищенности до значения, обеспечивающего выполнение требований к ПДн. Соответствие:

Меры защиты информации предусмотренные классом защищенности ИС	Обеспечивают уровень защищенности персональных данных
К1	1, 2, 3 и 4
К2	2, 3 и 4
К3	3 и 4
К4	4

Примечание: Если есть подсистемы, использовать нижеприведенную структуру документа. Сегменты – объединения маленьких ИСПДн (Баз Данных) по общему функционалу и единому классу.

В связи с наличием в информационной системе <наименование ИСПДн><название организации> отдельных сегментов:

– ***<маркированный список названий систем>***

целесообразно проводить классификацию отдельных сегментов и всей системы в целом.

Классификация сегмента <наименование сегмента ИСПДн><название организации>

Данный сегмент включает в себя следующие информационные системы персональных данных:

– ***<маркированный список названий маленьких ИСПДн>.***

Определение класса защищенности

В соответствии с Приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» комиссия установила следующее: ***<классификация по стандартной схеме>.***

Определение уровня защищенности персональных данных

В соответствии с Постановлением Правительства Российской Федерации №1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» комиссия установила следующее: ***<классификация по стандартной схеме>.***

Затем (соблюдая очередность систем и ту же структуру текста) провести классификацию каждого заявленного сегмента. И только в конце общий класс системы:

Классификация ИСПДн <наименование ИСПДн><название организации>

На основании полученных данных и в соответствии с Постановлением Правительства Российской Федерации №1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в информационной системе персональных данных <наименование ИСПДн><название организации> реализуемые меры защиты информации для информационной системы класса защищенности **К1** обеспечивают **1** уровень защищенности персональных данных.

Вопросы

1. Какие исходные данные необходимы для проведения классификации?
2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какова специфика проведения классификации?
4. Каковы суть и содержание нормативной основы организации ЗСИ?
5. Что такое государственная информационная система (ГИС)?
6. Каково определение класса ГИС?
7. Какие критерии определяют класс ГИС?
8. Каковы основные функции и задачи ГИС?
9. Какая роль ГИС в государственном управлении?
10. Какие примеры ГИС существуют в разных странах?
11. Каковы требования к безопасности ГИС?
12. Какие стандарты и нормативы применяются при создании ГИС?
13. Каков процесс разработки и внедрения ГИС?
14. Какие технические средства используются в ГИС?
15. Каковы основные преимущества использования ГИС?
16. Какие вызовы и проблемы могут возникнуть при работе с ГИС?
17. Каковы перспективы развития ГИС в будущем?
18. Какие организации отвечают за развитие и поддержку ГИС?
19. Каковы основные принципы эффективного управления ГИС?

Список дополнительной литературы:

1. Справочно-поисковая система «Консультант Плюс»;
2. Справочно-поисковая система «Гарант»

Практическая работа №2
на тему: «Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации».

ЦЕЛЬ РАБОТЫ

Разработать структуру государственных стандартов Российской Федерации в области информационной безопасности и защиты информации.

ЗАДАНИЕ НА ПРАКТИЧЕСКУЮ ПАБОТУ Ознакомиться с принципами системного подхода при создании структуры ГОСТ и ИСО.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Произвести поиск всех существующих государственных и международных стандартов в области информационных технологий, информационной безопасности и защиты информации. При нахождении – вносить в универсальный каталогизатор дисков, файлов, папок, а также любых нефайловых элементов wincatalog[1].

Пример заполнения приведен на рисунке 1.

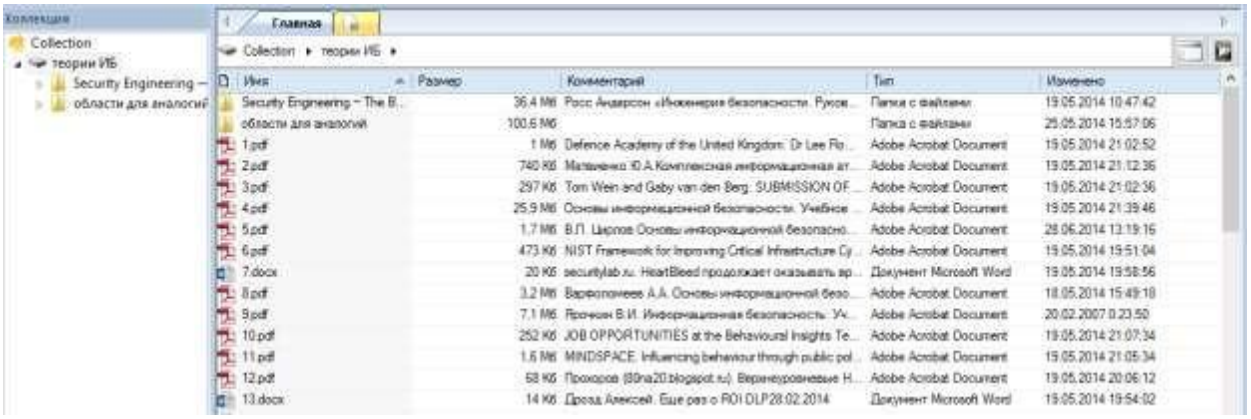


Рис.1 – Пример внесения документов в универсальный каталогизатор

2. При заполнении присваивать теги, которые описывают данный документ или область его применения, для последующей группировки.

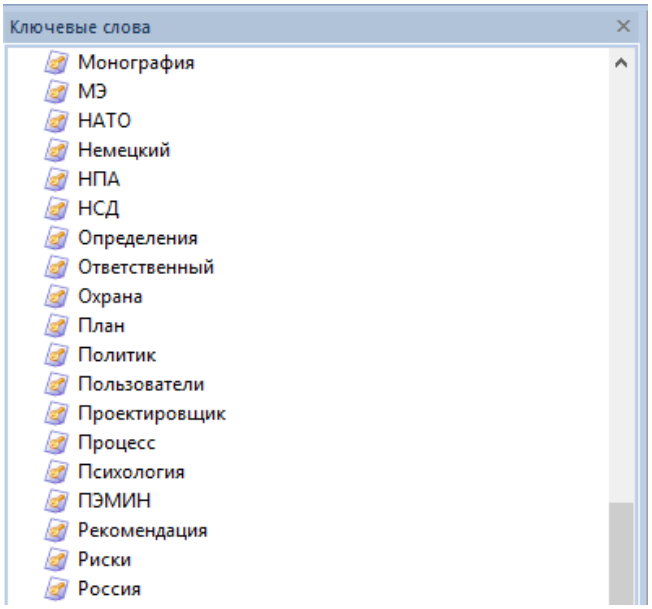


Рис.2 – Пример создания списка тегов

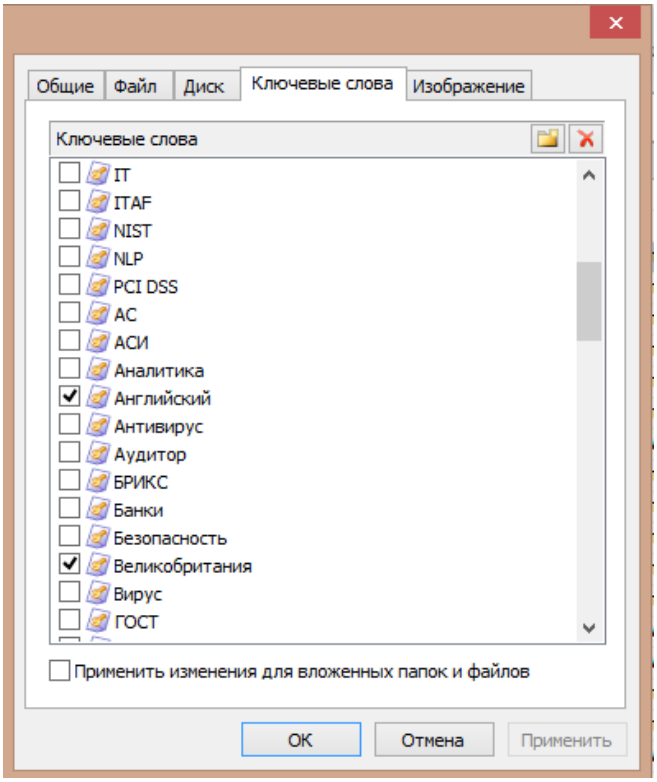


Рис.3 – Пример присваивания тегов документу

3. После заполнения системы тегов – необходимо графически их представить с помощью программы FreeMind[2] или аналога.

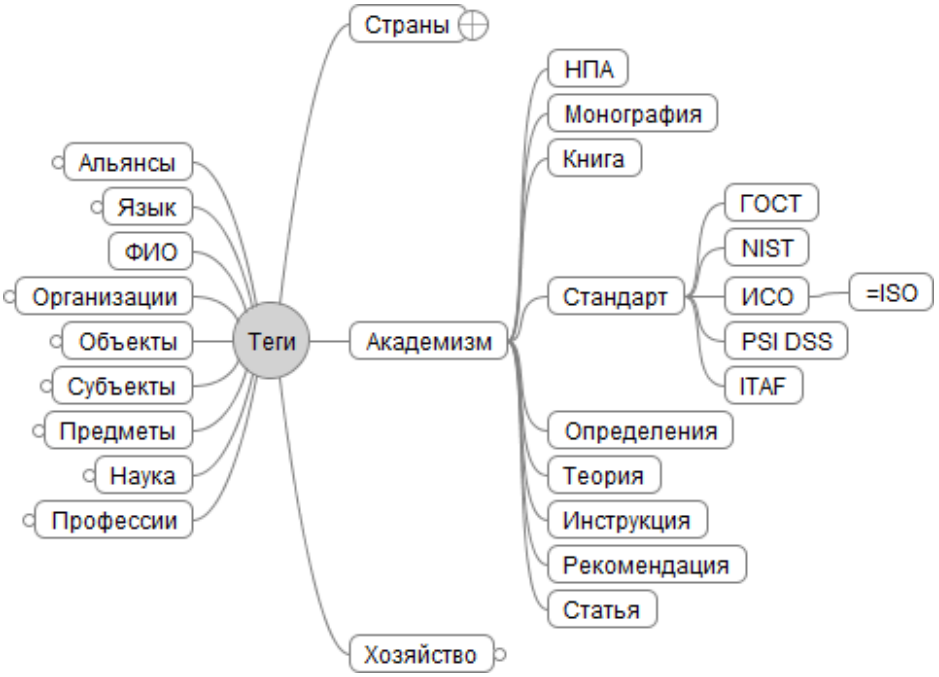


Рис.4 – Пример графического представления тегов

4. На основе полученных данных - заполнить таблицу с перечнем найденных ГОСТ и ИСО по приведенному примеру:

Таблица 1 – Список стандартов

№п/п	Номер стандарта	Статус
Защита сетей общего пользования		
1.	ГОСТ Р 53110-2008	Действует
2.	ГОСТ Р 53111-2008	Действует
3.	ГОСТ Р 53109-2008	Действует
Оценка безопасности автоматизированных систем		
4.	ГОСТ Р ИСО/МЭК ТО 19791-2008	Действует
5.		

5. Составить отчет. В отчете должны быть представлены четко видные и понятные скрины экрана при выполнении работы и оформленная таблица.

6. Найти нужно как можно больше стандартов. Заполнить таблицу №1

Контрольные вопросы

1. Дать полное определение ГОСТ
2. Дать полное определение ИСО
3. Как проводится сертификация средств защиты информации?
4. Что показывают характеристики данного средства защиты?
5. Какая основная информация содержится в сертификате?
6. Какова роль государственных и международных стандартов в области информационной безопасности и защиты информации?
7. Какие организации отвечают за разработку стандартов в Российской Федерации в области информационной безопасности?
8. Какими принципами руководствуются при разработке стандартов в области информационной безопасности?
9. Какие основные направления стандартизации существуют в области информационной безопасности?
10. Каков процесс разработки и утверждения государственных стандартов в Российской Федерации?
11. Какие международные стандарты используются в Российской Федерации в области информационной безопасности?
12. Какие правовые акты регулируют разработку и использование стандартов в области информационной безопасности?
13. Какие органы осуществляют контроль за соблюдением стандартов в области информационной безопасности?
14. Какие требования предъявляются к сертификации и аккредитации по стандартам информационной безопасности?
15. Какие последствия могут возникнуть при нарушении требований стандартов в области информационной безопасности?
16. Какие преимущества имеют организации, которые следуют государственным и международным стандартам в области информационной безопасности?
17. Как происходит адаптация международных стандартов в Российской Федерации?
18. Какие изменения произошли в стандартизации информационной безопасности в Российской Федерации за последние несколько лет?
19. Каковы требования к документированию и систематизации стандартов в области информационной безопасности?
20. Какая роль участия экспертов и специалистов в разработке структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации?

Список дополнительной литературы

1. Справочно-поисковая система «Консультант Плюс» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.consultant.ru/
2. Справочно-поисковая система «Гарант»[Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.garant.ru/
3. Справочно-поисковая система«Федеральное агентство по техническому регулированию и метрологии» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.gost.ru/wps/portal/
4. Справочно-поисковая система«Международная организация по стандартизации» [Электронный ресурс]:- Электрон. дан. - Режим доступа: www.iso.org

Практическая работа №3
на тему: «Техническое задание на создание информационной системы и системы защиты информации».

Цель работы

Целью данной лабораторной работы является Решение ситуационных задач (кейсов).

Задание:

В Курской области создается Комитет Курской области по контролю успеваемости учащихся образовательных организациях Курской области (выделяется часть функций из комитета образования и науки).

В рамках комитета создается автоматизированная система внутренней работы. Все сотрудники должны иметь автоматизированные рабочие места.
Структура комитета:
Руководитель – 1
Заместитель руководителя по внутренней работе – 1
Заместитель руководителя по контролю успеваемости – 1
Отдел кадров – 1
Бухгалтерия – 2
Отдел контроля успеваемости – 5
Отдел автоматизации деятельности – 1

Должен быть создан банк данных успеваемости, при этом имеется разработчик специального ПО, который реализует интерфейсную часть по необходимым требованиям с учетом выбранной аттестуемым СУБД. СУБД интегрируется с порталом госуслуг. Ввод данных осуществляется путем выгрузки данных из действующей системы Аверс по каналу связи.

Руководитель и заместители должны иметь доступ ко всей информации и Интернет, отдел контроля – только к ИС контроля, бухгалтерия и отдел кадров – только к ресурсу кадров и бухгалтерии, а так же к АС бюджетная система и закупки.

Деятельность бухгалтерии – стандартная, база данных 1С совмещена с отделом кадров.

Комитет занимает 8 помещений на 1 этаже (схема составляется самостоятельно), возможен прием посетителей.

Примерный бюджет на всю информатизацию и защиту информации 2,5 млн. руб.

Разрешаются любые уточняющие вопросы по электронной почте, при этом отметки о ходе работы и отметки о переписке должна быть внесена в ЖИРУ.

Необходимо:

Требования к отчету:

Отчет должен содержать:

1. титульный лист;
2. цель работы;
3. перечень документов для создания и оформления информационных систем;
4. ТЗ на создание информационной системы и системы защиты информации.
5. модель угроз и модель нарушителя;
6. смета на технические средства обработки информации, закупку лицензионного ПО, средств защиты информации, коммутационное оборудование (СКС, установку и монтаж не включать);
7. доклад;
8. выводы по проделанной работе.

Вопросы:

1. Где необходима электронная подпись документов?
2. Какие могут быть альтернативные наборы вариантов решения?
3. Как определялась схема рассадки людей?
4. Какой перечень документов по которым готовился?
5. Каковы основные разделы, которые должны быть включены в техническое задание на создание информационной системы и системы защиты информации?
6. Какие требования к функциональности информационной системы следует указать в техническом задании?
7. Какие требования к безопасности информации должны быть учтены в техническом задании?
8. Какие требования к архитектуре и инфраструктуре информационной системы следует указать в техническом задании?
9. Каким образом определяются требования по доступу и авторизации пользователей в техническом задании?
10. Какие методы шифрования и защиты данных следует описать в техническом задании?
11. Какие требования по резервному копированию и восстановлению информации следует указать в техническом задании?
12. Каким образом определяются требования к мониторингу и аудиту информационной системы в техническом задании?
13. Какие требования к защите от внешних угроз (например, взлом, вирусы) следует указать в техническом задании?
14. Каким образом определяются требования к защите от внутренних угроз (например, несанкционированный доступ персонала) в техническом задании?
15. Какие требования к системе мониторинга и обнаружения инцидентов следует указать в техническом задании?

16. Какие требования к обучению и осведомленности пользователей информационной системы следует описать в техническом задании?

17. Какие требования к физической безопасности информационной системы следует указать в техническом задании?

18. Каким образом определяются требования к резервному питанию и защите от сбоев электроснабжения в техническом задании?

19. Какие требования к документированию и отчетности о безопасности информационной системы следует описать в техническом задании?

Список дополнительной литературы:

3. Справочно-поисковая система «Консультант Плюс»;
4. Справочно-поисковая система «Гарант»;

Практическая работа №4
на тему: «Основные методы управления информационной безопасностью в ГИС».

Цель работы

Целью данной лабораторной работы является оценка показателей качества функционирования комплексной системы защиты информации на предприятии, расчет защищенности от физического проникновения и от несанкционированного доступа в локальную сеть.

Постановка задачи

1. **План предприятия и назначение помещений:**
   1- проходная;
   2- помещение охраны;
   3- операторская;
   4- операторская;
   5- бухгалтерия;
   6- кабинет директора;
   7- приемная;
   8- библиотека;
   9- комната для переговоров.

В соответствии с описанием помещений составить собственную графическую схему.

1. Перечень информации, циркулирующей на предприятии

Перечень информации	*Возможные потери, руб*
Плановая документация	100000
Информационно-справочная и справочно-аналитическая документация	150000
Отчетная документация	80000
Документация по обеспечению кадрами	50000
Финансовая документация	1000000
Материально-техническое снабжение	50000
Договорная документация	200000

2. Параметры локальной сети и список сотрудников

Параметры локальной сети:
Количество компьютеров – 7;
Сеть на витой паре Ethernet 100Мбит;
Персонал состоит из постоянного и переменного состава
1) Постоянный:

- генеральный директор;
- зам. директора;
- юрист;
- секретарь;
- администратор сети и безопасности;
- сотрудники – 3 человека;
- программист;
- охранники – 3 человека;

- уборщицы – 2 человека.

2) Переменный состав:

- группа поиска – 3 человека;
- бухгалтер;
- электрик-телефонист;
- заказчики.

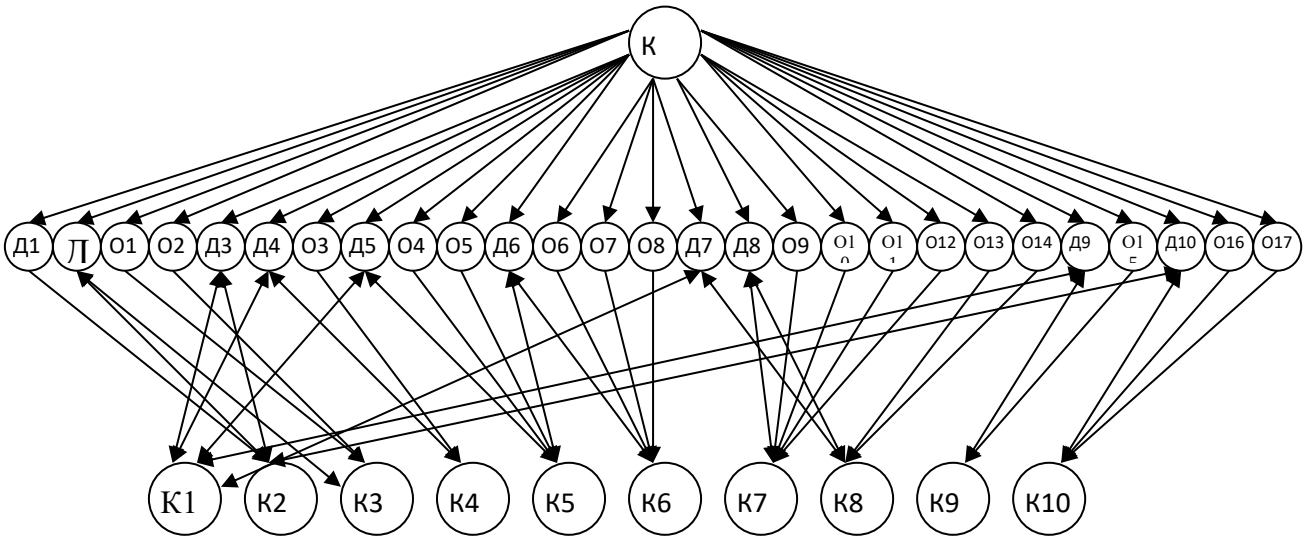
3. Перечень угроз с учетом возможных потерь

№	*Угроза*	*Объект угрозы*	*Опасность угрозы в баллах от 1 до 100*	*Возможные потери*
1	Утечка за счет структурного звука в стенах и перекрытиях	Переговоры	20	50 тыс.
2	Съем информации с плохо стертых дискет	Информация на дискетах	40	Незначительные
3	Программно-аппаратные закладки в ПЭВМ	Информация в локальной сети	50	90 тыс.
4	Радио-закладки в стенах и мебели	Секретные переговоры	70	90 тыс.
5	Съем информации по системе вентиляции	Разговоры	40	Незначительные
6	Лазерный съем акустической информации с окон	Секретные переговоры	70	90 тыс.
7	Производственные и технологические отходы	Служебная и профессиональная тайны	20	Незначительные
8	Компьютерные вирусы, логические бомбы и т.п	Информация в локальной сети	50	90 тыс.
9	Съем информации за счет наводок и навязывания	Секретные переговоры, информация в локальной сети	80	90 тыс.
10	Дистанционный съем видеоинформации	персонал, клиенты	40	50 тыс.
11	Съем акустической информации с использованием диктофонов	Разговоры, переговоры	70	50 тыс.
12	Хищение носителей информации	Документированная информация, информация на НЖМД	40	90 тыс.
13	Высокочастотный канал утечки в бытовой технике	переговоры	30	незначительные
14	Съем информации направленным микрофоном	Переговоры, разговоры	30	50 тыс.
15	Внутренний канал утечки (обслуживающий персонал, несанкционированное копирование);	Информация на НЖМД, документированная информация, переговоры	80	90 тыс.
16	Утечка за счет побочного излучения терминалов	Компьютерная информация, разговоры	40	90 тыс.
17	Съем информации с телефонного уха	Телефонные переговоры	50	незначительные
18	Визуальный съем с дисплея и принтера	Различная информация	20	незначительные
19	Утечка по линиям связи	переговоры	80	50 тыс.
20	Утечка по цепям заземления	Различная информация	20	незначительные
21	Утечка по цепи электропитания	Переговоры	40	50 тыс.

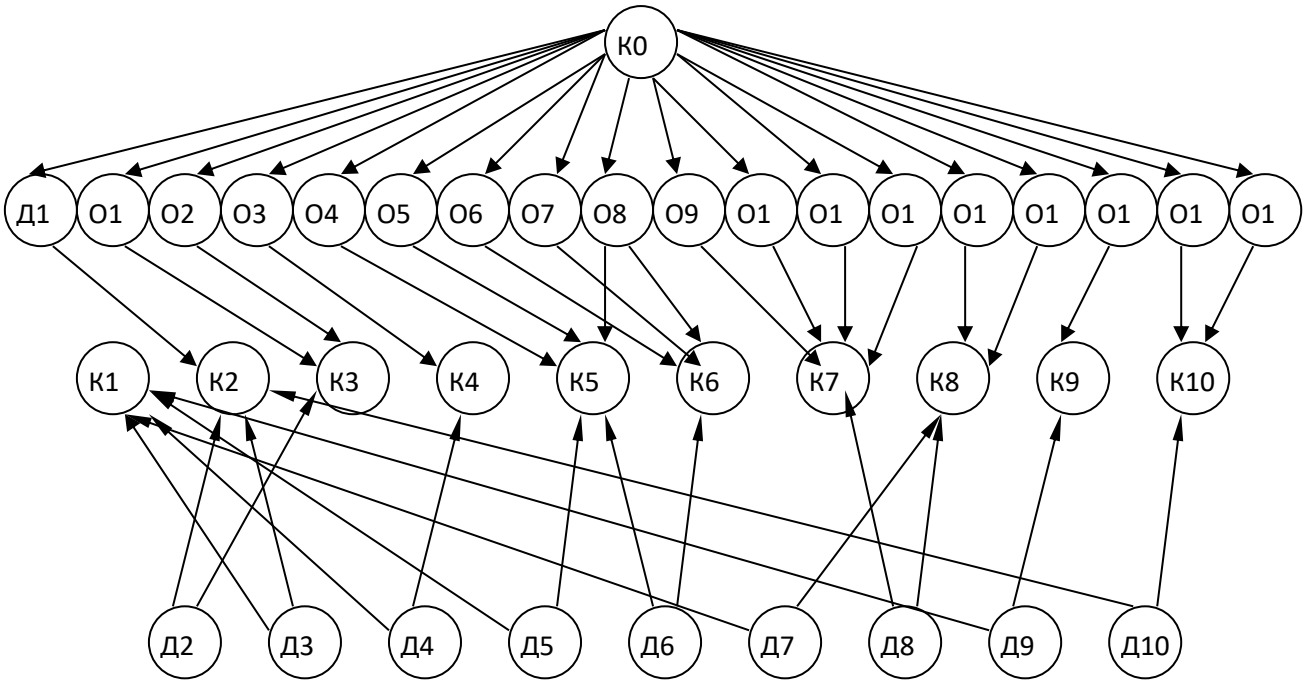
2. Расчет защищенности от физического проникновения

2.1. **Для поставленной задачи рассчитать вероятность доступа в помещения предприятия** (для построения графов можно воспользоваться программой *Deadlock*)

Пример. Помещение имеет 10 комнат, включая коридор (обозначим буквой «К»), 17 окон (обозначим буквой «О») и 10 дверей (обозначим буквой «Д»). Построенный для данного здания граф имеет следующий вид, при этом помещением 0 считаем внешнюю среду.



Для наглядности вынесем переходы, доступ к которым невозможен из внешней среды отдельно.



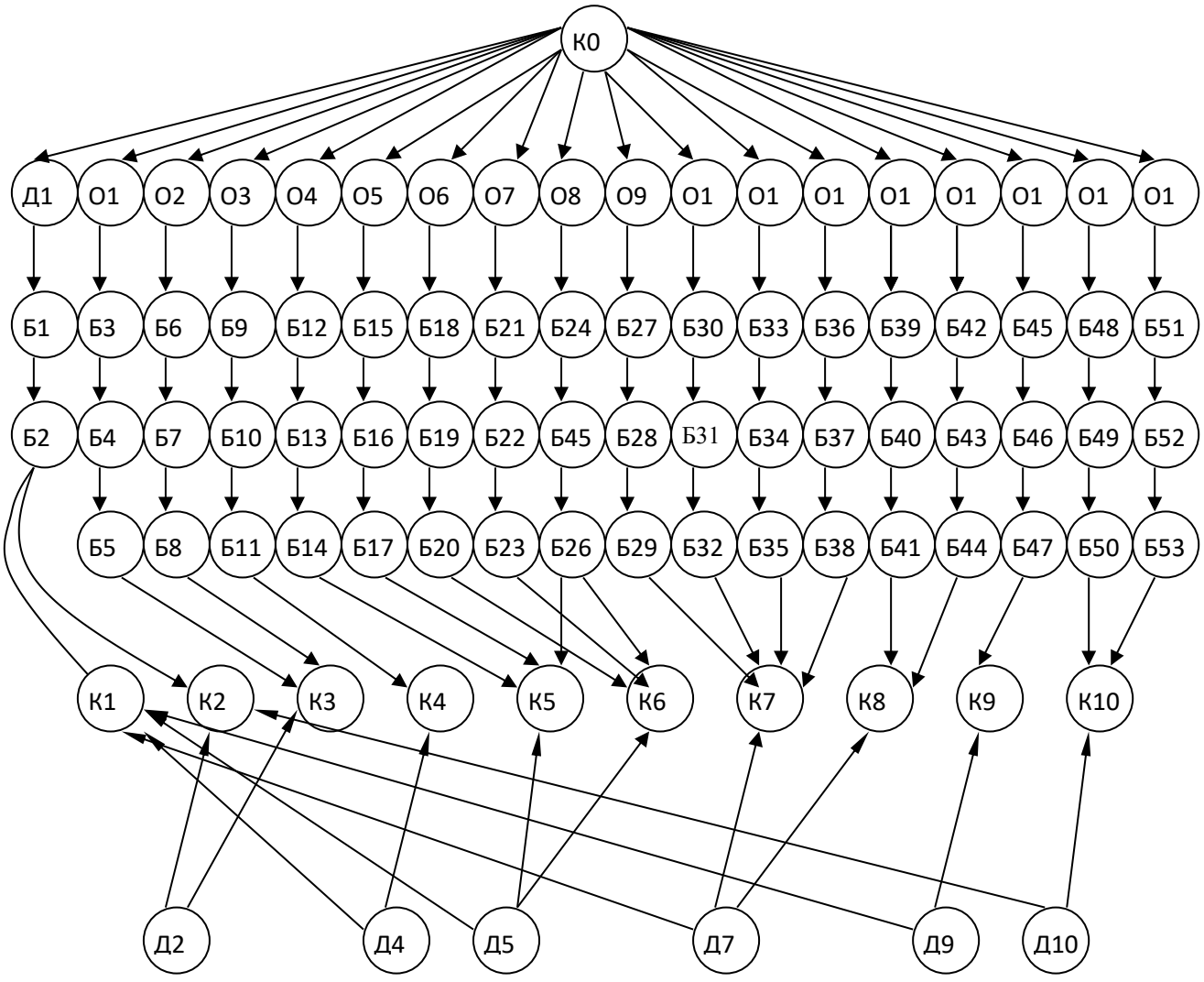
Данный граф представляет собой схему переходов между помещениями предприятия. При построении графа не учитывались возможные средства защиты от проникновения. При

появлении таких средств они будут представлять собой дополнительные вершины. В нашем случае на окнах имеются следующие средства защиты:

- решетки;
- жалюзи;
- датчики разбития стекла.

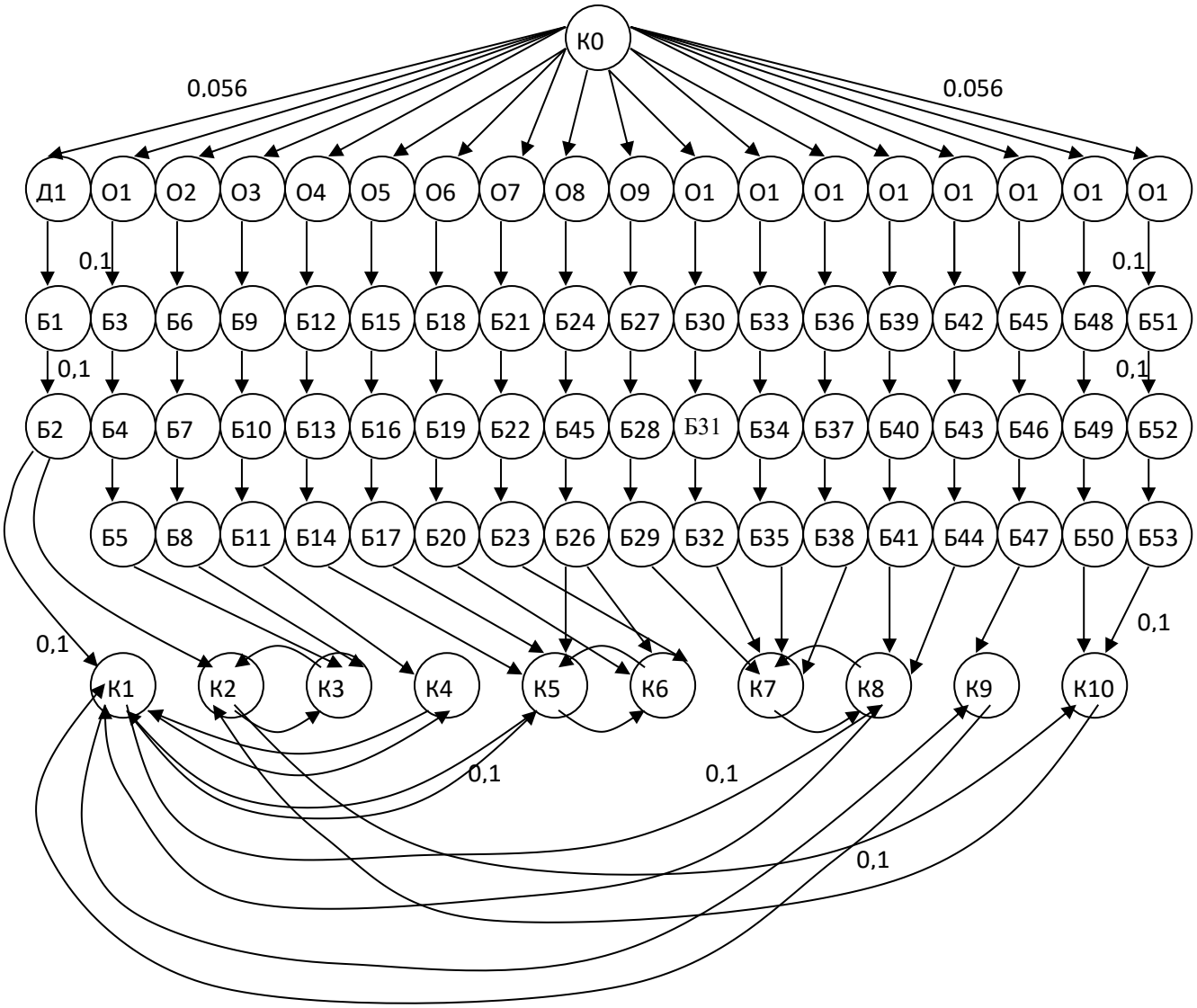
А на входной двери имеется замок и дверь бронирована.

Поэтому появляются три барьера (обозначим их буквой «Б») от Б1 до Б53. В том случае, если на двери нет замка, то соответствующую ей вершину можно удалить из графа, соединив соответствующие комнаты между собой непосредственно. Вершины, соответствующие этим двум комнатам, можно объединить в одну вершину, поскольку доступ в одну из комнат равносилен доступу в другую. Таким образом, из графа исключаются вершины Д3, Д6, Д8.



Каждой дуге ставится в соответствие ее вес – вероятность совершения данного перехода. При этом двунаправленные дуги распадаются на две. Путь проникновения нарушителя в какое-либо помещение представляет собой путь в графе. Начальной точкой пути всегда считаем вершину К0. Все переходы, начинающиеся в вершине К0, примем равновероятными, поскольку нам неизвестно, по какому пути пойдет преступник. При этом сумма всех этих вероятностей равна вероятности возникновения соответствующей угрозы, в нашем случае – физического проникновения. В нынешних условиях вероятность

попытки проникновения можно принять равной 1. Таким образом, вес дуг, начинающихся в К0 равен 0.056. Для упрощения расчетов в лабораторной работе примем вероятность совершения всех остальных переходов равными 0,1.
С учетом сказанного выше граф примет следующий вид:



Каждой вершине можем приписать вероятность попадания в данную вершину. Эту вероятность можем рассчитать по формуле:

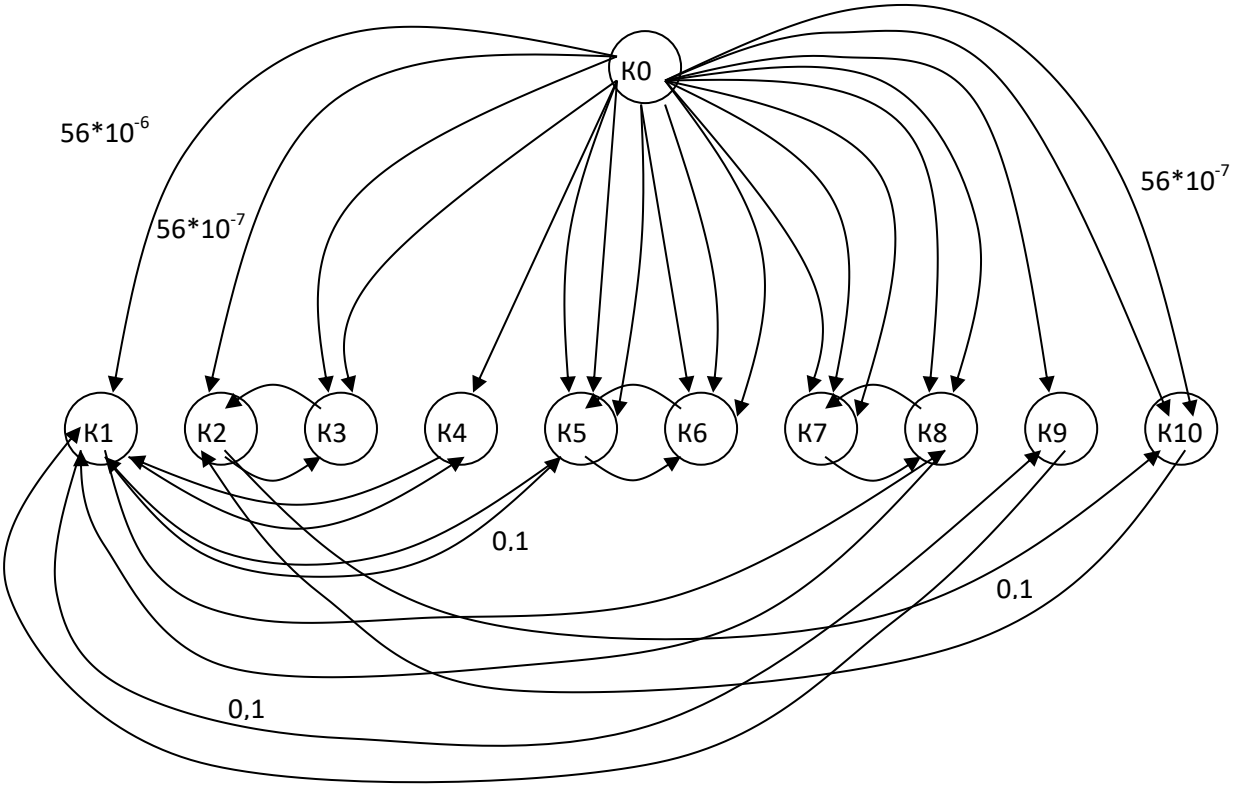
$$p_i = \sum_{j=1}^{n} v_j \cdot p_j \,, \qquad (1)$$

где v_j – вес *j*-й дуги;

p_j – вероятность нахождения преступника в соседнем состоянии (соседней вершине) *j*,

n – число соседних состояний (вершин).

Если в графе присутствует вершина, переход в которую возможен только из одной вершины и из которой выходит только одна дуга, то такую вершину можно исключить, заменив ее дугой с весом, равным произведению весов входящей и исходящей дуги. Исключив, таким образом, все такие вершины, получим новый граф.



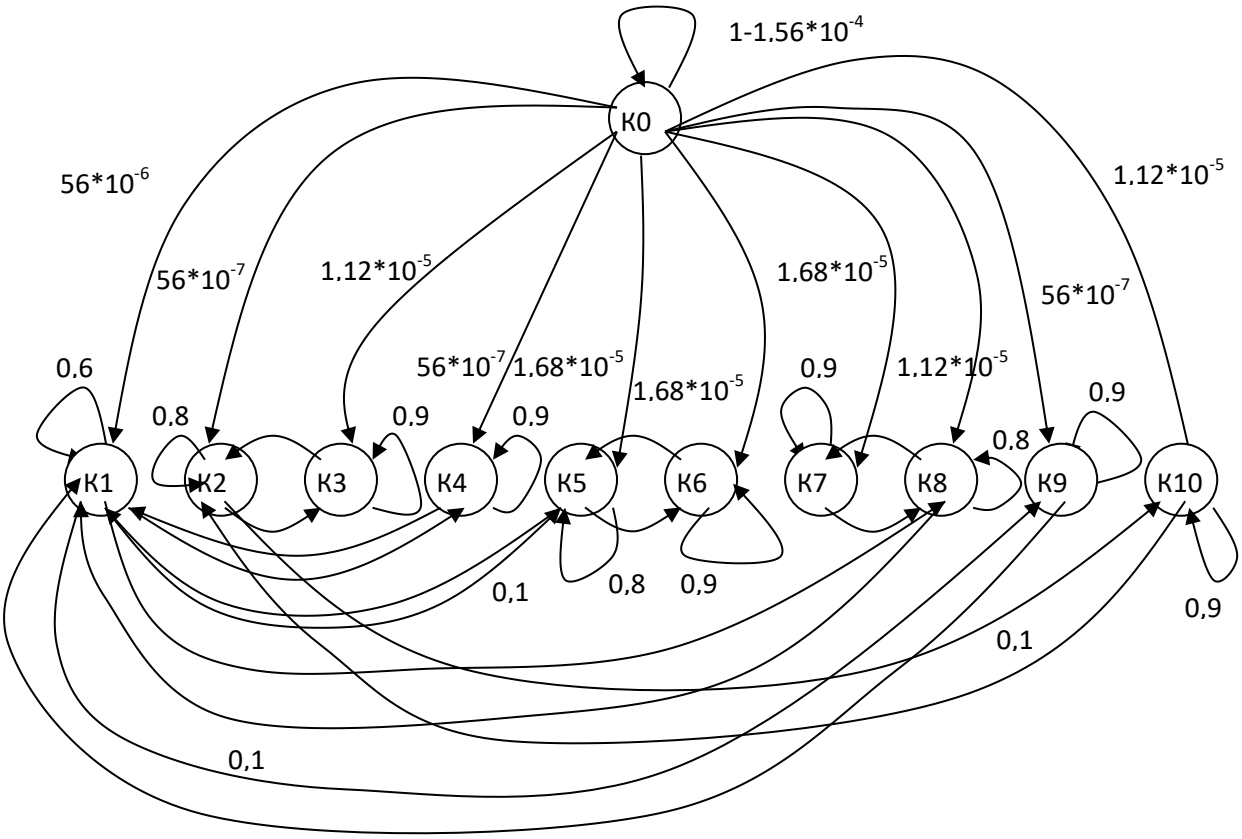
Если из одной вершины в другую ведут более одной дуги, все эти дуги можно заменить одной с весом, равным сумме весов этих дуг. Составим систему уравнений Колмогорова-Чепмена для определения вероятностей доступа в помещения. Для этого добавим в граф дуги, ведущие из каждой вершины в саму себя, с весом, равным:

$$v_i = 1 - \sum_{j=1}^{n} v_j \,, \qquad (2)$$

где v_j – вес *j*-й дуги, входящей в данную вершину;

n – количество дуг, входящих в вершину *i*.

В результате получим следующий граф:



Для данного графа матрица смежности будет иметь следующий вид:

	К0	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10
Из К0	0,999844	$56*10^{-6}$	$56*10^{-7}$	$1,12*10^{-5}$	$56*10^{-7}$	$1,68*10^{-5}$	$1,68*10^{-5}$	$1,68*10^{-5}$	$1,12*10^{-5}$	$56*10^{-7}$	$1,12*10^{-5}$
Из К1	0	0,6	0	0	0,1	0,1	0	0	0,1	0,1	0
Из К2	0	0	0,8	0,1	0	0	0	0	0	0	0,1
Из К3	0	0	0,1	0,9	0	0	0	0	0	0	0
Из К4	0	0,1	0	0	0,9	0	0	0	0	0	0
Из К5	0	0,1	0	0	0	0,8	0,1	0	0	0	0
Из К6	0	0	0	0	0	0,1	0,9	0	0	0	0
Из К7	0	0	0	0	0	0	0	0,9	0,1	0	0
Из К8	0	0,1	0	0	0	0	0	0,1	0,8	0	0
Из К9	0	0,1	0	0	0	0	0	0	0	0,9	0
Из К10	0	0	0,1	0	0	0	0	0	0	0	0,9

Расчет вероятности доступа в помещения

$k := 0, 1 .. 126 \qquad A := (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$

$$B_k := \begin{pmatrix} 0.999844 & 0.000056 & 0.0000056 & 0.0000112 & 0.0000056 & 0.0000168 & 0.0000168 & 0.0000168 & 0.0000112 & 0.0000056 \\ 0 & 0.6 & 0 & 0 & 0.1 & 0.1 & 0 & 0 & 0.1 & 0.1 \\ 0 & 0 & 0.8 & 0.1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.1 & 0.9 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 & 0.9 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 & 0 & 0.8 & 0.1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.1 & 0.9 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 & 0 & 0 & 0 & 0.9 & 0.1 & 0 \\ 0 & 0.1 & 0 & 0 & 0 & 0 & 0 & 0.1 & 0.8 & 0 \\ 0 & 0 & 0.1 & 0 & 0 & 0 & 0 & 0 & 0 & 0.9 \end{pmatrix}^k$$

$$C1 := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C2 := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C3 := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C4 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C5 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

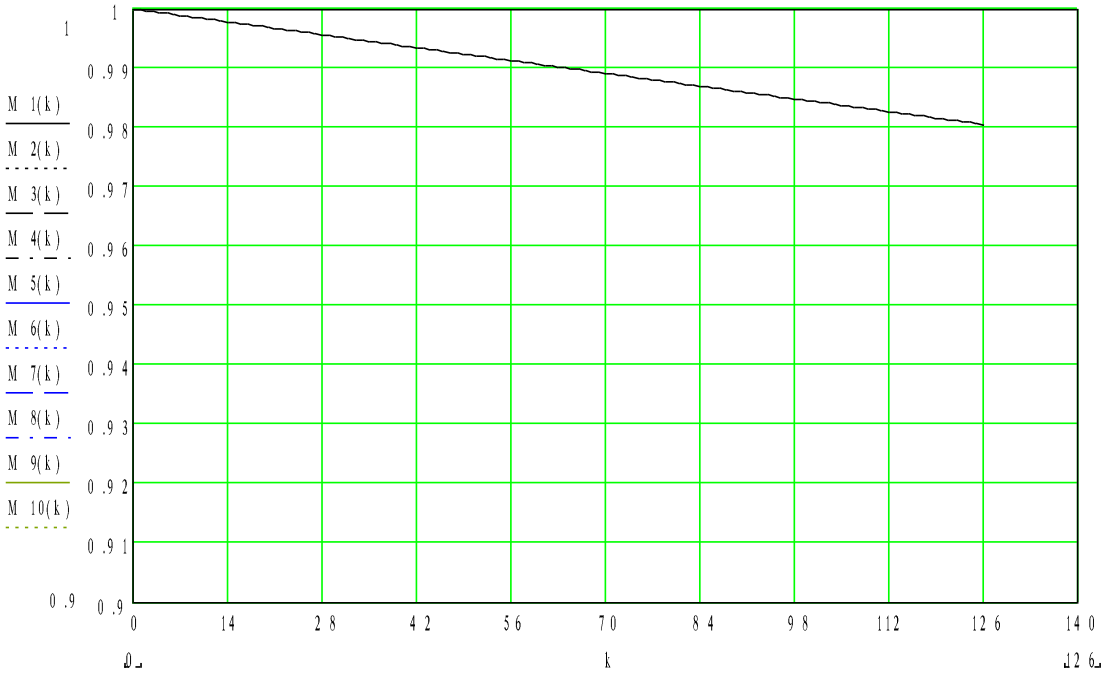
$$C6 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C7 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C8 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad C9 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad C10 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

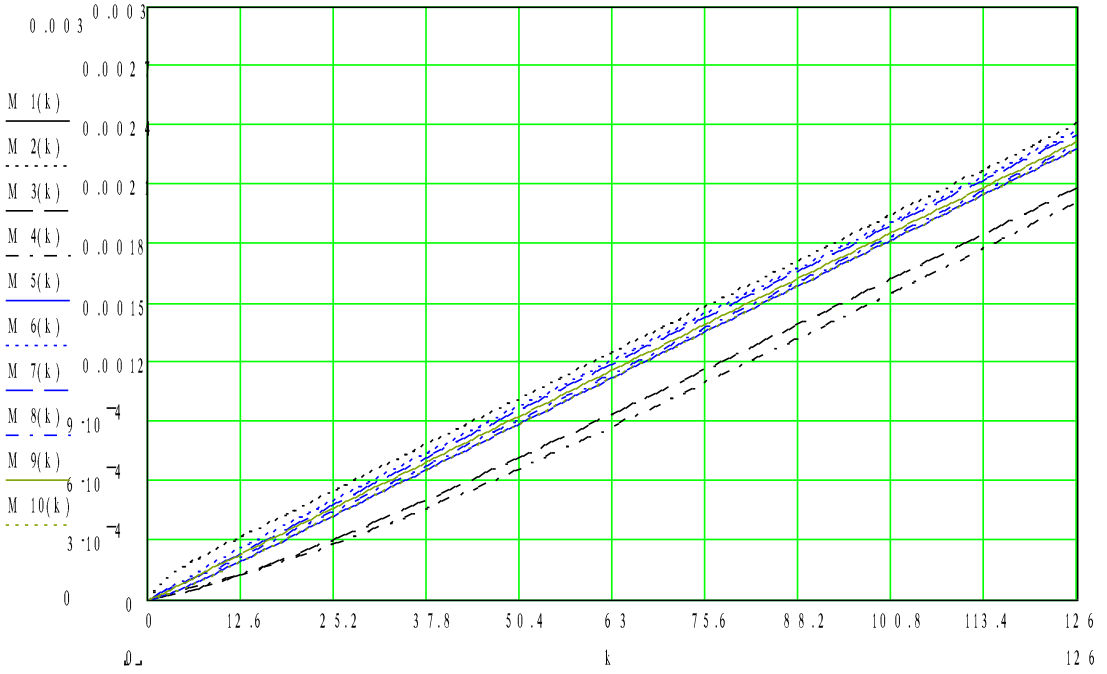
$P1_k := A \cdot B_k \cdot C1 \quad P2_k := A \cdot B_k \cdot C2 \quad P3_k := A \cdot B_k \cdot C3 \quad P4_k := A \cdot B_k \cdot C4 \quad P5_k := A \cdot B_k \cdot C5$

$P6_k := A \cdot B_k \cdot C6 \quad P7_k := A \cdot B_k \cdot C7 \quad P8_k := A \cdot B_k \cdot C8 \quad P9_k := A \cdot B_k \cdot C9 \quad P10_k := A \cdot B_k \cdot C10$

$M1(k) := (P1_k)_{0,0} \quad M2(k) := (P2_k)_{0,0} \quad M3(k) := (P3_k)_{0,0} \quad M4(k) := (P4_k)_{0,0} \quad M5(k) := (P5_k)_{0,0}$

$M6(k) := (P6_k)_{0,0} \quad M7(k) := (P7_k)_{0,0} \quad M8(k) := (P8_k)_{0,0} \quad M9(k) := (P9_k)_{0,0} \quad M10(k) := [(P10)_k]_{0,0}$

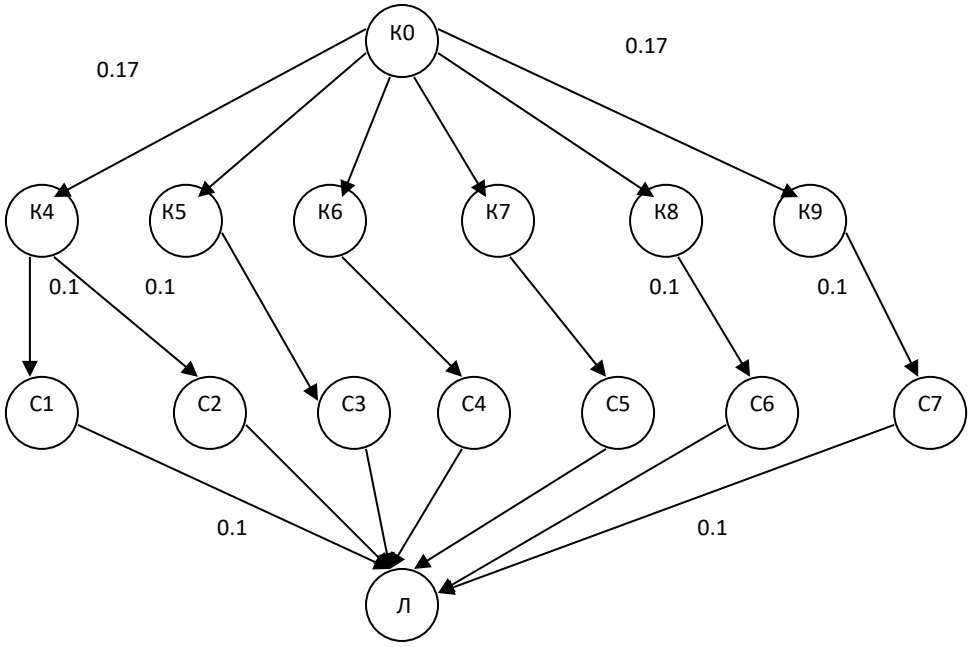

M 1(k)
M 2(k)
M 3(k)
M 4(k)
M 5(k)
M 6(k)
M 7(k)
M 8(k)
M 9(k)
M 10(k)
1
0.99
0.98
0.97
0.96
0.95
0.94
0.93
0.92
0.91
0.9
0
14
28
42
56
70
84
98
112
126
140
k


M 1(k)
M 2(k)
M 3(k)
M 4(k)
M 5(k)
M 6(k)
M 7(k)
M 8(k)
M 9(k)
M 10(k)
0.003
0.0027
0.0024
0.0021
0.0018
0.0015
0.0012
9·10⁻⁴
6·10⁻⁴
3·10⁻⁴
0
0
12.6
25.2
37.8
50.4
63
75.6
88.2
100.8
113.4
126
k

3. Расчет защищенности от НСД к локальной сети предприятия

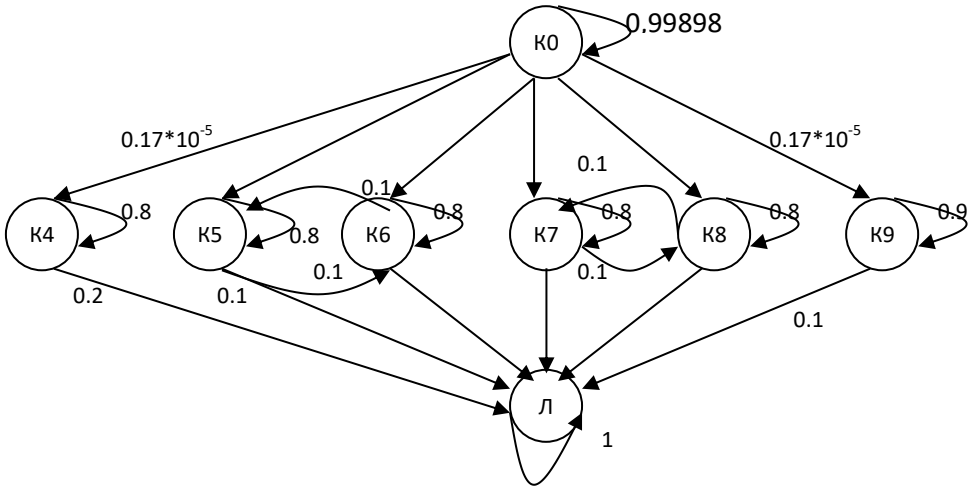
3.1. Для поставленной задачи рассчитать защищенность от НСД ЛВС.

Пример. Граф будет иметь следующий вид:



Будем считать: К0- внешняя среда, К4..К9 – комнаты, С- компьютеры, Л- локальная сеть предприятия.

Граф, преобразованный с учетом исключения вершин с одной входной и одной выходной дугой, имеет вид:



Матрица смежности будет иметь следующий вид:

	К0	К4	К5	К6	К7	К8	К9	Л
из К0	0.99898	$0.17*10^{-5}$	$0.17*10^{-5}$	$0.17*10^{-5}$	$0.17*10^{-5}$	$0.17*10^{-5}$	$0.17*10^{-5}$	0
из К4	0	0.8	0	0	0	0	0	0.2
из К5	0	0	0.8	0.1	0	0	0	0.1
из К6	0	0	0.1	0.8	0	0	0	0.1
из К7	0	0	0	0	0.8	0.1	0	0.1
из К8	0	0	0	0	0.1	0.8	0	0.1
из К9	0	0	0	0	0	0	0.9	0.1
из Л	0	0	0	0	0	0	0	1

Расчет вероятности НСД к локальной сети предприятия

$k := 0, 1 .. 126 \qquad A := (1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)$

$$B_k := \begin{pmatrix} 0.99898 & 0.00017 & 0.00017 & 0.00017 & 0.00017 & 0.00017 & 0.00017 & 0 \\ 0 & 0.8 & 0 & 0 & 0 & 0 & 0 & 0.2 \\ 0 & 0 & 0.8 & 0.1 & 0 & 0 & 0 & 0.1 \\ 0 & 0 & 0.1 & 0.8 & 0 & 0 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0.8 & 0.1 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0.1 & 0.8 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.9 & 0.1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}^k$$

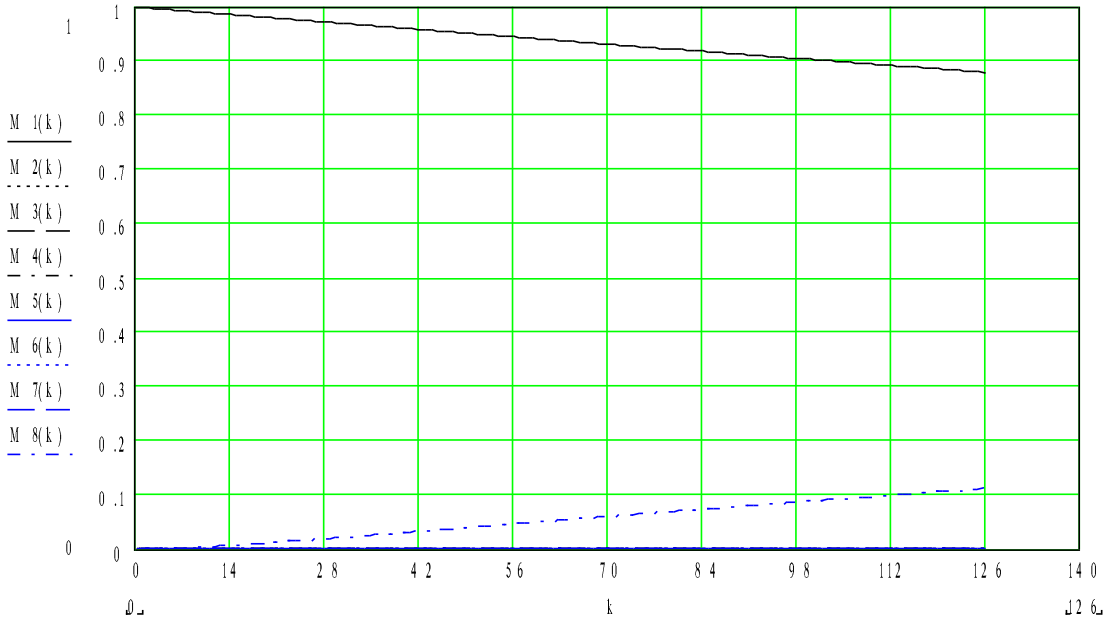
$$C1 := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C2 := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C3 := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C4 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C5 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C6 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad C7 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad C8 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

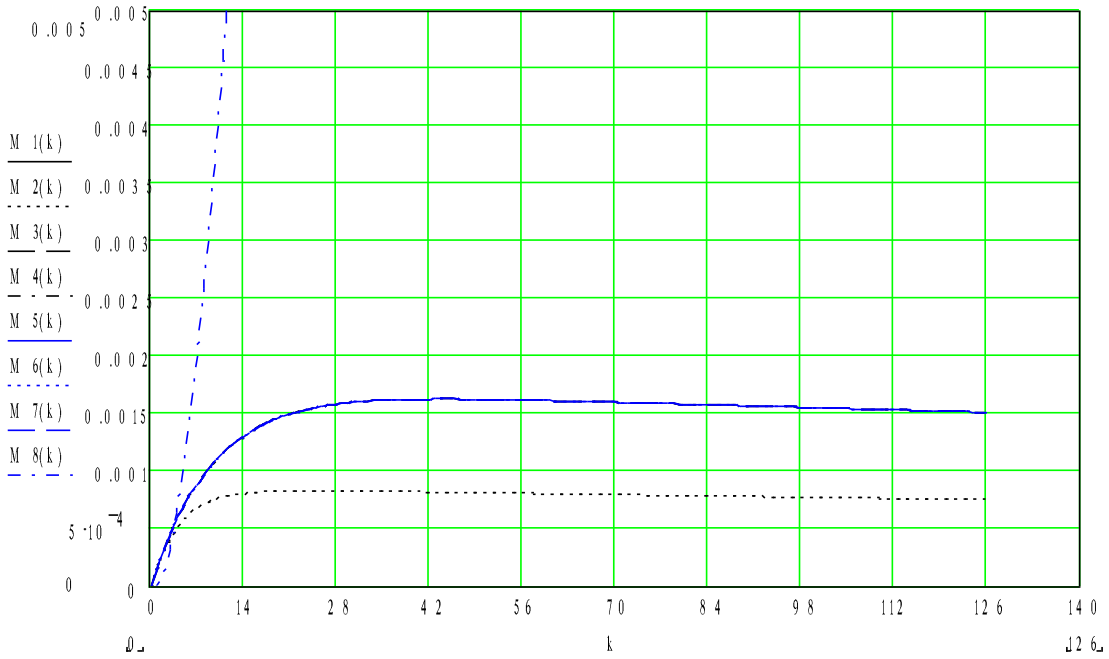
$P1_k := A \cdot B_k \cdot C1 \qquad P2_k := A \cdot B_k \cdot C2 \qquad P3_k := A \cdot B_k \cdot C3 \qquad P4_k := A \cdot B_k \cdot C4$

$P5_k := A \cdot B_k \cdot C5 \qquad P6_k := A \cdot B_k \cdot C6 \qquad P7_k := A \cdot B_k \cdot C7 \qquad P8_k := A \cdot B_k \cdot C8$

$M1(k) := (P1_k)_{0,0} \qquad M2(k) := (P2_k)_{0,0} \qquad M3(k) := (P3_k)_{0,0} \qquad M4(k) := (P4_k)_{0,0}$

$M5(k) := (P5_k)_{0,0} \qquad M6(k) := (P6_k)_{0,0} \qquad M7(k) := (P7_k)_{0,0} \qquad M8(k) := (P8_k)_{0,0}$





3.2. По полученным графикам сделать выводы о качестве функционирования комплексной системы защиты информации на рассматриваемом предприятии.

Контрольные вопросы:

1. Что такое плановая документация?
2. Что такое информационно-справочная и справочно-аналитическая документация?
3. Что такое отчетная документация?
4. Что такое документация по обеспечению кадрами?
5. Что такое финансовая документация?
6. Что такое материально-техническое снабжение?

7. Какие основные методы управления информационной безопасностью применяются в геоинформационных системах (ГИС)?
8. Какова роль политики безопасности в управлении информационной безопасностью ГИС?
9. Какие методы аутентификации и авторизации используются для обеспечения безопасности в ГИС?
10. Как осуществляется контроль доступа к данным и ресурсам в ГИС?
11. Какие меры предпринимаются для защиты от несанкционированного доступа к геоинформационным данным?
12. Как происходит мониторинг и обнаружение инцидентов безопасности в ГИС?
13. Какие методы шифрования используются для защиты данных в ГИС?
14. Какие меры предпринимаются для защиты от вредоносного программного обеспечения (вирусов, троянов) в ГИС?
15. Как осуществляется резервное копирование и восстановление данных в случае сбоя или потери информации в ГИС?
16. Как обеспечивается физическая безопасность серверов и другого оборудования ГИС?
17. Какой подход используется для обучения пользователей ГИС по вопросам информационной безопасности?
18. Как осуществляется контроль за действиями пользователей в ГИС с целью предотвращения несанкционированных действий?
19. Какие меры предпринимаются для защиты передачи данных между компонентами системы ГИС?
20. Как обеспечивается защита от утечки конфиденциальной информации в ГИС?
21. Как происходит оценка и аудит системы безопасности ГИС для обнаружения уязвимостей и недостатков?

Список литературы

1. Корнилова, А. А. Защита персональных данных : учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2020. – 119 с. – URL: https://biblioclub.ru/index.php?page=book&id=611314 (дата обращения: 04.05.2023). – Режим доступа: по подписке. – Текст : электронный.
2. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 140 с. – URL: https://biblioclub.ru/index.php?page=book&id=612162 (дата обращения: 04.05.2023). – Режим доступа: по подписке. – Текст : электронный.
3. Информационная безопасность в цифровом обществе : учебное пособие / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=611084 (дата обращения: 04.05.2023). – Режим доступа: по подписке. – Текст : электронный.
4. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Ч. 1. - 150 с. – Текст : электронный.
5. Аудит информационной безопасности органов исполнительной власти : учебное пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, М. В. Рудановский. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 100 с. – URL: https://biblioclub.ru/index.php?page=book&id=93259 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.