



ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ИНДИВИДУАЛЬНЫХ ЗАДАНИЙ И ПРЕЗЕНТАЦИЙ



Оформление титульного листа и оглавления

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»
ИНЖЕНЕРНО-ЭКОНОМИЧЕСКИЙ ИНСТИТУТ

Кафедра безопасности и информационных технологий

Направление подготовки бакалавриата
10.03.01-«Информационная безопасность»

ДОКЛАД

Тема: «Программное обеспечение для расчета систем видеонаблюдения»

Выполнил студент группы ИЭ-05-21 Иванов И.И.
Проверил доцент, к.т.н., доцент Петров П.П.
Оценка: _____ дата _____

Москва 2020 г.

Оглавление

Введение	3
1. АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РАСЧЕТА СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ	4
1.1. Современное программное обеспечение для расчета систем видеонаблюдения	4
1.2. Выводы	8
2. МЕТОДИКА РАБОТЫ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ ДЛЯ РАСЧЕТА СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ	9
2.1. Программное обеспечение JVSG - IP Video System Design Tool	9
2.2. Программное обеспечение VideoCad	14
2.3. Программное обеспечение CCTV Design Lens Calculator	18
2.4. Программное обеспечение CAD5D	22
2.5 Выводы	24
Заключение	27
Список используемых источников	30

2

Оформление докладов

Пример оформления таблицы и рисунка

21

использованием информационных технологий и обеспечить возможность выполнения основных бизнес - целей объекта.

Распространенная практика свидетельствует о том, что система управления рисками должна быть интегрирована в систему управления жизненным циклом информационной технологии (табл. 1).

Таблица 1. Управление рисками на различных стадиях жизненного цикла информационной технологии

Фаза жизненного цикла информационной системы	Соответствие фазе управления рисками
1. Предпроектная стадия ИС (определение целей и задач и их документирование)	Выявление основных классов рисков для данной ИС, вытекающих из целей и задач, концепция обеспечения ИБ
2. Проектирование ИС	Выявление рисков, специфичных для данной ИС (вытекающих из особенностей архитектуры ИС)
3. Создание ИС: поставка элементов, монтаж, настройка, отладка и конфигурирование	До начала функционирования ИС должны быть идентифицированы и приняты во внимание все классы рисков
4. Функционирование ИС	Периодическая переоценка рисков, связанная с изменениями внешних условий и в конфигурации ИС
Прекращение функционирования ИС (информационные и вычислительные ресурсы более не используются по назначению и утилизируются)	Соблюдение требований информационной безопасности по отношению к выходящим информационным ресурсам

Далее приведем пример практической реализации рассмотренных нами методик. Для этого сначала определим понятие риска информационной безопасности.

(Слайд № 36). Риск информационной безопасности ($R_{инб}$) определим, как функцию трех переменных: вероятности существования угрозы информационной безопасности ХС (P_v), вероятности существования незащищенности (уязвимости) информационной системы ХС ($P_{ин}$), и вероятности потенциального воздействия на информационную систему ХС ($P_{воз}$).

$$R_{инб} = E(P_v; P_{ин}; P_{воз}) \quad (1)$$

Если любая из этих переменных приближается к нулю, то риск приближается к нулю, следовательно, для расчета величины риска информационной безопасности справедливым будет выражение 2.

$$R_{инб} = P_v \times P_{ин} \times P_{воз} \quad (2)$$

Естественно, что выражение 2 справедливо для случая, когда переменные являются количественными величинами. Если же переменные – качественные величины, операция умножения становится не применимой. Таким образом, величина $R_{инб}$, рассчитанная в соответствии с выражением 2, в сущности, является *вероятностью несения ХС некоторых потерь*.

7

VideoCAD - многофункциональный и удобный инструмент, предназначенный для профессионального проектирования систем видеонаблюдения и контроля, моделирование видеоборудования и видеоизображений.

Для расчета систем видеонаблюдения, программы VideoCAD позволяет (рис. 7):
 рассчитать для нанесения на план объекта реальные размеры горизонтальных проекций зоны обзора, зоны обнаружения человека, зоны опознавания человека и зоны чтения автомобильного номера;

рассчитать и смоделировать глубину резкости каждой видеокамеры в проекте;

рассчитать, сколько % от размера экрана, пикселей, ТВ линий, миллиметров (двойное в случае английского формата измерений) будет занимать изображение на мониторе любого объекта в зоне обзора;

вычислить по графикам спектрального распределения мощности излучения и измерять практически спектральную эффективность источников света для различных сенсоров видеокамер;

рассчитать длину и электрические параметры кабелей.

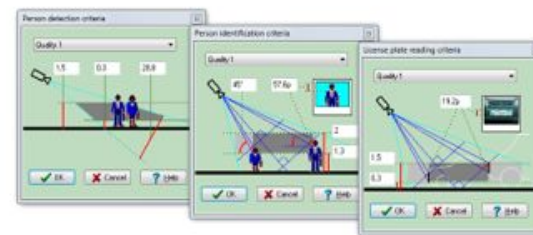


Рисунок 7. Возможности программы VideoCAD

По завершении расчетов программа автоматически формирует итоговый документ, в котором отображается расчетное количество технических средств для создания системы видеонаблюдения.



Заключение

1. Изучены общие сведения о программном обеспечении для расчета систем видеонаблюдения. Установлено, что программы для проектирования систем видеонаблюдения должны помочь разработчику в выполнении расчётов используется информация, взятая из различных областей: строительные конструкции и материалы, электротехника, слаботочные системы, оптика, электроника и многие другие.

2. Рассмотрены несколько конкретных программных обеспечений для расчета систем видеонаблюдения: JVSG - IP Video System Design Tool; VideoCad; CCTV Design Lens Calculator; CAD5D. Это показывает различные функции каждой программы в расчете системы видеонаблюдения.



Список используемых источников

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Невский А.Ю., Баронов О.Р. Система обеспечения информационной безопасности хозяйствующего субъекта: учебное пособие. – М.: Издательский дом МЭИ, 2009.
3. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. № 583.
4. Программа проектирования видеонаблюдения VideoCAD/
http://www.cctvcad.com/rus/programma_proektirovaniya_videonabludeniya.html.
5. CCTV Design Lens Calculator — для проектирования видеонаблюдения
[/https://markevich.by/programmnye-sredstva/cctv-design-lens-calculator-programma-dlya-proektirovaniya-videonablyudeniya.html](https://markevich.by/programmnye-sredstva/cctv-design-lens-calculator-programma-dlya-proektirovaniya-videonablyudeniya.html).
6. Проектирование видеонаблюдения с помощью программы CAD5D
<https://cad5d.ru/videonablyudenie/>.



ОФОРМЛЕНИЕ ПРЕЗЕНТАЦИЙ

**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»
ИНЖЕНЕРНО-ЭКОНОМИЧЕСКИЙ ИНСТИТУТ**

Кафедра безопасности и информационных технологий

**Направление подготовки бакалавриата
10.03.01- «Информационная безопасность»**

ДОКЛАД

**АНАЛИЗ КЛАССИФИКАЦИИ КОНСТРУКТИВНЫХ
ТРЕБОВАНИЙ К ДВЕРЯМ И ПРОЧИМ ЗАЩИТНЫМ
КОНСТРУКЦИЯМ ПО УСТОЙЧИВОСТИ К КРИМИНАЛЬНОМУ
ОТКРЫВАНИЮ И ВЗЛОМУ**

**Студент группы ИЭ-41-21
Иванов Иван Иванович**

Москва-2021



Роль дверей и замков в защите информации

Сколько способов вскрытия замков существует и какая квалификация взломщиков?

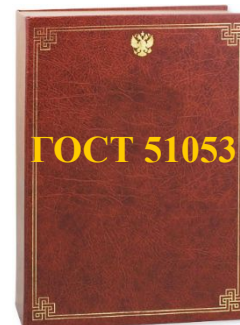
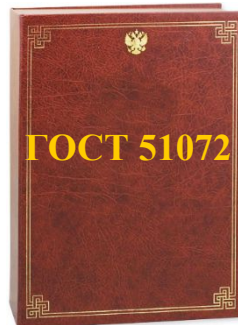
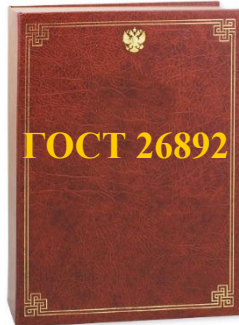
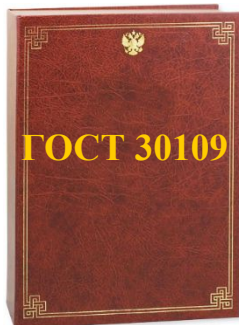




- 1. Двери. Классификация, устройство, требования**
- 2. Дверные замки. Конструкция, классификация, требования**



ДВЕРИ. КЛАССИФИКАЦИЯ, УСТРОЙСТВО, ТРЕБОВАНИЯ



- **ГОСТ 30109** «Двери деревянные. Методы испытаний на сопротивление взлому»;
- **ГОСТ 26892** «Двери деревянные. Методы испытания на сопротивление ударной нагрузке, действующей в направлении открывания двери»;
- **ГОСТ Р 51072** «Двери защитные. Общие технические требования и методы испытаний на устойчивость к взлому, пулестойкость и огнестойкость»;
- **ГОСТ Р 51053** «Замки сейфовые. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому»;
- **и другие**

На основании этих документов в зависимости от категории прочности по сопротивлению взлому двери дифференцируются по назначению

Рама с заполнением
минеральной ватой

2й уплотнитель
(в нащельнике рамы)

Панель изнутри
(МДФ 18мм)

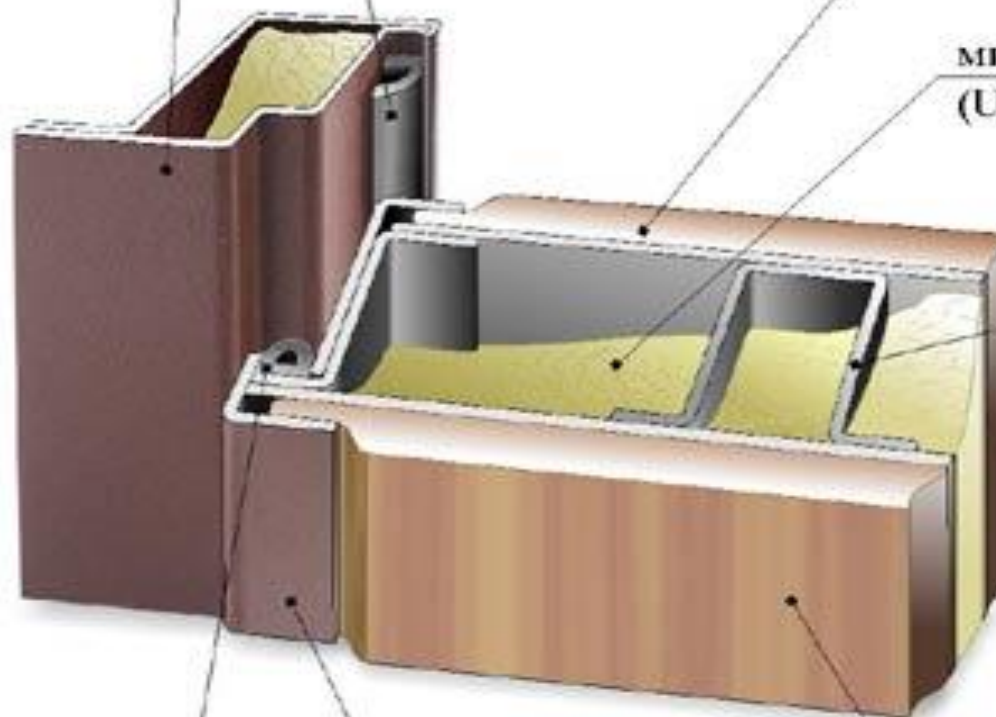
минеральная вата
(URSA)

Ребра
жесткости

1й уплотнитель
(на дверном полотне)

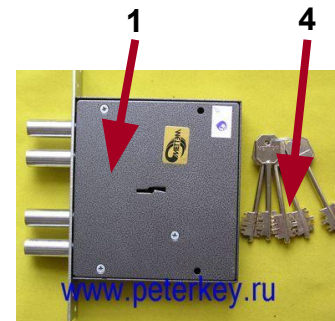
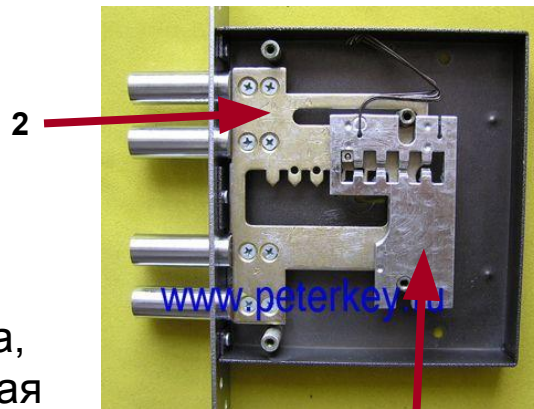
Дверное полотно

Панель снаружи
(МДФ 18мм)



Механический замок состоит из:

- 1 - корпуса;
- 2 - ригеля (засова);
- 3 - сувальды;
- 4 - ключа;
- 5 - запорной планки

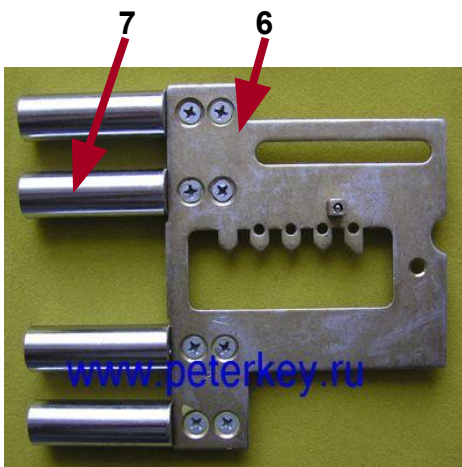
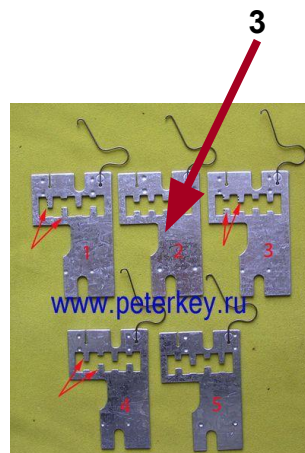


Ригель – деталь замка, непосредственно запирающая дверь

Ключ – деталь, управляющая механизмом замка

Состоит из **головки** (6), на которую воздействует ключ и одной или нескольких **задвижек** (7)

Ключ ставит **сувальды** и пружины в такое положение, чтобы стало возможным передвижение **ригеля**



Сувальд – деталь замка, толкающая **ригель** под воздействием **ключа**. Конструкция, конфигурация и количество подпружиненных сувальд образуют «секрет» ключа



1. Функционал дверей и замков, в соответствии с ГОСТ 30109, должен затруднить доступ:

- ❖ **квалифицированного взломщика на 30 мин.;**
- ❖ **неквалифицированного взломщика – на 1 час**

2. Технические характеристики дверей и замков должны соответствовать уровню защиты конфиденциальной информации и требованиям ГОСТ 51072

3. Стоимость дверей и замков должна быть сопоставима со стоимостью конфиденциальной информацией



1. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. «Основы управления информационной безопасностью». Учебное пособие для вузов.-2-е изд., испр. - М.: Горячая линия - Телеком, 2014. – 244 с.: Серия «Вопросы управления информационной безопасностью. Выпуск 1»

2. Новиков В.К. «Организационно - правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации)». Учебное пособие.- М.: Горячая линия - Телеком, 2015. - 176 с.

3. Бузов Г.А. «Защита информации ограниченного доступа от утечки по техническим каналам». - М.: Горячая линия - Телеком, 2016. - 586 с.



ДОКЛАД

**АНАЛИЗ КЛАССИФИКАЦИИ КОНСТРУКТИВНЫХ
ТРЕБОВАНИЙ К ДВЕРЯМ И ПРОЧИМ ЗАЩИТНЫМ
КОНСТРУКЦИЯМ ПО УСТОЙЧИВОСТИ К КРИМИНАЛЬНОМУ
ОТКРЫВАНИЮ И ВЗЛОМУ**

СПАСИБО ЗА ВНИМАНИЕ !!!

**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»
ИНЖЕНЕРНО-ЭКОНОМИЧЕСКИЙ ИНСТИТУТ**

Кафедра безопасности и информационных технологий

**Направление подготовки бакалавриата
10.03.01- «Информационная безопасность»**

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

**ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В
РАСПРЕДЕЛЕННЫХ, РАЗНОРОДНЫХ И
РАЗНОКАТЕГОРИЙНЫХ СИСТЕМАХ**

**Выполнил студент группы ИЭ-05-21
Руководитель работы доцент, к.т.н., доцент**

**Иванов И.И.
Петров П.П.**

Москва-2021



Актуальность работы –

Цель исследования –

Задачи исследования –

Границы исследования –



Выпускная квалифицированная работа состоит из глав и приложений

В первой главе исследовалось

Во второй главе исследовалось

В первом приложении представлен анализ

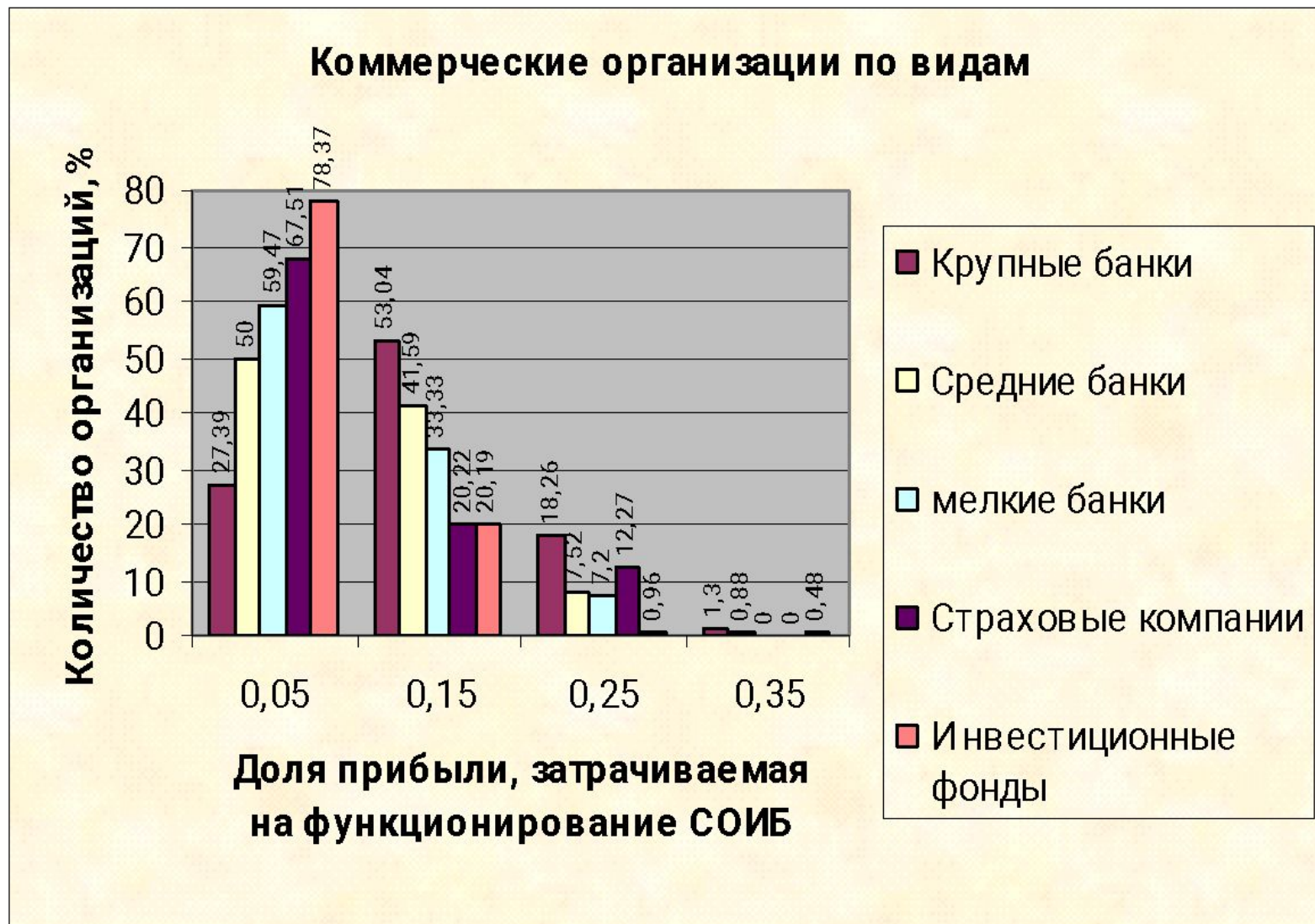
Во втором приложении представлены результаты

Пример оформления таблицы

Затраты коммерческих финансовых организаций на функционирование СОИБ

Доля затрачиваемой прибыли		Количество организаций					
X	X _{сред}	Все организации, %	Крупные банки, %	Средние банки, %	Мелкие банки, %	Страховые компании, %	Инвестиционные фонды, %
0,0	0,05	56,68	27,39	50,00	59,47	67,51	78,37
0,1	0,15	33,36	53,04	41,59	33,33	20,22	20,19
0,2	0,25	9,46	18,26	7,52	7,2	12,27	0,96
0,3	0,35	0,50	1,30	0,88	0,00	0,00	0,48
0,4 – 1,0	0,45 -0,95	0,00	0,00	0,00	0,00	0,00	0,00
Сумма		100%	100%	100%	100%	100%	100%
Мат.ожидание		10,38%	14,35%	10,93%	9,77%	9,48%	7,36%

Пример оформления графика





Пример оформления формулы

Показатель совокупной стоимости владения СОИБ
рассчитывается по формуле:

$$\text{ТСО} = \text{Пр} + \text{Кр}_1 + \text{Кр}_2 \quad (1)$$

где:

Пр - прямые затраты;

Кр₁ - косвенные затраты первой группы;

Кр₂ - косвенные затраты второй группы



1. IP-решения рекомендуется применять для крупных объектов, включающих более 16 камер. Системы IP-видеонаблюдения будут оптимальным решением, если на объекте уже имеется сеть с высокой пропускной способностью, особенно если камеры будут распределены по большой площади объекты, где приоритетом для системы видеонаблюдения является качество и четкость записанного изображения, а стоимость установки и обслуживания являются вторичными

2. HD аналоговые технологии CCTV (AHD, HD-CVI и HD-TVI) применяются для видеонаблюдения малого и среднего масштаба, для небольших систем видеонаблюдения состоящими из 16 и менее камер и одного DVR, для частного сектора, а также для малых и средних коммерческих и промышленных зданий



1. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. «Основы управления информационной безопасностью». Учебное пособие для вузов.-2-е изд., испр. - М.: Горячая линия - Телеком, 2014. – 244 с.: Серия «Вопросы управления информационной безопасностью. Выпуск 1»

2. Новиков В.К. «Организационно - правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации)». Учебное пособие.- М.: Горячая линия - Телеком, 2015. - 176 с.

3. Бузов Г.А. «Защита информации ограниченного доступа от утечки по техническим каналам». - М.: Горячая линия - Телеком, 2016. - 586 с.




ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

**ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В
РАСПРЕДЕЛЕННЫХ, РАЗНОРОДНЫХ И
РАЗНОКАТЕГОРИЙНЫХ СИСТЕМАХ**

СПАСИБО ЗА ВНИМАНИЕ !!!



1. Национальный стандарт Российской Федерации ГОСТ Р 57321.1 «Менеджмент знаний. Менеджмент знаний в области инжиниринга. Часть 1. Общие положения, принципы и понятия»
2. Федеральный закон №149 от 7.07.2006г. «Об информации, информационных технологиях и о защите информации»
3. Конституция Российской Федерации
4. Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «Стратегия национальной безопасности Российской Федерации»
5. Указ Президента РФ от 05.12.2016 № 646 «Доктрина информационной безопасности Российской Федерации»
6. Указ Президента РФ от 09.05.2017 № 203 «Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы»
7. Основные направления научных исследований в области обеспечения информационной безопасности российской федерации. (Утверждены секретарем совета безопасности российской федерации 31 августа 2017 г.)
8. Постановление Правительства Российской Федерации № 244 от 02.03.2017 г. «О совершенствовании требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики и внесении изменений в некоторые акты правительства российской федерации»
9. Приказ Минэнерго Российской Федерации № 1015 от 06.11.2018 г. «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования»



СЕМИНАР № 1
СУЩНОСТЬ ИНФОРМАЦИИ

СПАСИБО ЗА ВНИМАНИЕ !!!