МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине
«Управление информационной безопасностью»
для студентов направления подготовки
10.04.01 Информационная безопасность

Методические указания к лабораторным работам

Практическое занятие № 1. Инициация и предварительное планирование проекта

Цель работы: изучить основные процессы инициации и предварительного планирования проекта.

Теоретическая часть Инициация проекта. Началу каждого проекта должны предшествовать маркетинговые исследования, проработка целесообразности выполнения, переговоры с заказчиками, инвесторами и другими потенциальными участниками проекта. Эту стадию проекта обычно называют *инициацией.* Основная цель процессов инициации - сделать запуск проекта управляемым. Так, решение о запуске проекта должно быть ответственным, сознательным и приниматься теми, кто имеет на это право. Для того чтобы лица, принимающие решение о запуске проекта, могли принять адекватное решение, они должны обладать информацией обо всех аспектах проекта. Например, инвестора прежде всего будут интересовать гарантии эффективного использования его капиталовложений, схемы финансовых потоков, размеры и сроки получения прибыли. Заказчика будут интересовать цели и продукт проекта, сроки его выполнения и стоимость. Менеджера высокого ранга наряду с этим будут интересовать сведения о необходимых для проекта технологиях, специалистах и ресурсах, а также о порядке их использования.

Предварительное планирование проекта. Предварительное планирование проекта может быть начато еще на стадии его инициации, т. к. уже тогда следует оценить цикл выполнения проекта. По существу для этого и нужен предварительный план. Конечно, на этой стадии план не может быть детальным и точно определять многие важные для проекта даты, но он уже должен формировать оценки для этих дат. Понятие оценки в управлении проектами является одним из наиболее важных. Оценка некоторого показателя представляет собой его значение, определенное с доступной в данный момент (на данной стадии) проекта точностью. Очевидно, что оценка любого показателя может изменяться с течением времени, а точность такой оценки быстро убывает по мере роста срока, отделяющего текущую дату от предполагаемого момента, в который для данного показателя можно будет определить фактическое значение.

Оборудование и материалы: для выполнения данной лабораторной работы необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, MS Project.

Указания по технике безопасности: к выполнению лабораторных работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения лабораторной работы необходимо выполнить следующее:

1.Изучить рекомендуемую литературу.

2.Создайте файл графика реализации проекта с помощью Консультанта.

3.Определите опорные даты проекта.

4.Установите для файла проекта режимы работ.

5.Введите свойства файла проекта.

6.Построить модели бизнес-процессов предметной области.

7.Ответить на контрольные вопросы.

8.Оформить отчет.

Содержание отчета: отчет по лабораторной работе должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию:

Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1.Что такое проект?

2.Перечислить основные этапы проекта.

3.Дайте краткую характеристику методов сетевого планирования и управления.

4.Охарактеризуйте метод критического пути.

5.В чем отличие метода PERT от метода CPM.

Список литературы, рекомендуемый к использованию по данной теме:

1. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 206 с.

2. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. 113 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 139 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 186 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 145 с.

Практическое занятие № 2. Определение состава задач проекта

Цель работы: Изучить способы определения состава задач проекта.

Теоретическая часть

Определение состава задач с оценкой продолжительности их выполнения. Технически перечень задач (работ) может быть создан «вручную» или путем переноса данных из любого файла, например, баз данных Foxpro или Access, документа Word, таблицы Excel. Независимо от способа создания принципиально важна ориентация перечня работ на особенности конкретного проекта. В укрупненном графике каждой из фаз проекта, может соответствовать одна работа. Объемы работ на этой стадии будут определены приближенно (считаем, что у разработчика графика имеются необходимые для этого нормативы).

Формирование ресурсного обеспечения и объема трудозатрат. Формирование ресурсного обеспечения целесообразно начать с планирования ресурсов. Ресурсы делятся на два основных класса:

- трудовые или возобновляемые, которые могут быть повторно использованы на различных работах проекта (люди, оборудование);

- материальные или не возобновляемые, которые на работах проекта расходуются и вновь использованы быть не могут (например, материи электроэнергия, финансовые средства и т. д.).

Оборудование и материалы: для выполнения данной лабораторной работы необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, MS Project.

Указания по технике безопасности: к выполнению лабораторных работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения лабораторной работы необходимо выполнить следующее:

1.Изучить рекомендуемую литературу.

2.Сформировать перечень задач проекта

3.Сформировать ресурсное обеспечение.

4.Ответить на контрольные вопросы.

5.Оформить отчет.

Содержание отчета: отчет по лабораторной работе должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1.Системы управления проектами.

2.Характерные формы представления сведений о проекте.

3.Цели использования систем управления проектами.

4.Типы задач используемые Project.

5.Задачи-вехи проекта.

Список литературы, рекомендуемый к использованию по данной теме:

1. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 206 с.

2. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. 113 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 139 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 186 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 145 с.

Практическое занятие № 3. Формирование взаимосвязи задач графика реализации проекта

Цель работы: изучить основные способы формирования взаимосвязи задач графика реализации проекта.

Теоретическая часть

Формирование взаимосвязи задач графика реализации проекта. Для представления последовательности выполнения задач в Project используются так называемые *связи задач.* При помощи связей для каждой задачи могут быть определены предшествующие задачи и последующие задачи. Для хранения этой информации в Project 2003 специально предназначены поля Предшественники и Последователи. В соответствии с возможностями Project для любой пары взаимосвязанных работ (одна из которых является предшествующей, а вторая – последующей) можно задать любой из типов приведенных ниже.

- Окончание-начало (ОН) (Finish-to-Start (FS))
- Окончание-окончание (ОО) (Finish- to-Finish (FF))
- Начало-начало (НН) (Start-to-Start (SS))
- Начало-окончание (НО) (Start to-Finish (SF))

Здесь первое определение (перед дефисом) относится к предшествующей работе, второе - к последующей. Для любой связи можно определить относительное запаздывание, т. е. вре-менной разрыв (Lag) или опережение - перекрытие работ по времени (Lead), в любых допустимых единицах времени.

Временные показатели взаимосвязанных работ автоматически пересчитываются при изменении показателей любой из работ.

При формировании последовательности работ наиболее часто приходится наполнять следующие операции:

- определение списка предшественников для текущей задачи;
- введение временного разрыва между задачами;
- разрыв связи между задачами.

Project позволяет выполнять перечисленные операции разными способами.

Оборудование и материалы: для выполнения данной лабораторной работы необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, MS Project.

Указания по технике безопасности: к выполнению лабораторных работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения лабораторной работы необходимо выполнить следующее:

1.Изучить рекомендуемую литературу.

2.Сформировать взаимосвязи задач проекта.

3.Ответить на контрольные вопросы.

4.Оформить отчет.

Содержание отчета: отчет по лабораторной работе должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1.Суммарные задачи проекта.

2.Критические задачи проекта.

3.Виды ресурсов используемые при выполнении проектов.

4.График ресурсов проекта.

5.Фильтры используемые Project.

Список литературы, рекомендуемый к использованию по данной теме:

1. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 206 с.

2. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. 113 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 139 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 186 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 145 с.

Практическое занятие № 4. Разработка предварительного расписания проекта

Цель работы: изучить основные принципы разработки предварительного расписания проекта.

Теоретическая часть

В Project любая задача, с точки зрения ограничения сроков ее начала из окончания, может быть отнесена к любому из перечисленных ниже типов.

- Как можно раньше (As Soon As Possible).
- Как можно позже (As Late As Possible).
- Начало не позднее (Start No Later Than).
- Начало не ранее (Start No Earlier Than).
- Окончание не позднее (Finish No Later Than).
- Окончание не ранее (Finish No Earlier Than).
- Фиксированное начало (Must Start On).
- Фиксированное окончание (Must Finish On).

Большинство перечисленных ограничений (кроме первых двух) должно быть связано с конкретными датами ограничений.

В общем случае управление временными ограничениями задач включает две основные операции:

- ввод временного ограничения;
- отмена временного ограничения, установленного ранее.

Оборудование и материалы: для выполнения данной лабораторной работы необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, MS Project.

Указания по технике безопасности: к выполнению лабораторных работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения лабораторной работы необходимо выполнить следующее:

1.Изучить рекомендуемую литературу.

2.Разработать предварительное расписание проекта.

3.Ответить на контрольные вопросы.

4.Оформить отчет.

Содержание отчета: отчет по лабораторной работе должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1.Основные элементы проекта.

2.Средства интерфейса Project.

3.Формы представления информации Project (8форм)

4.Основная цель процессов инициации.

5.Назначение предварительного плана проекта.

Список литературы, рекомендуемый к использованию по данной теме:

1. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 206 с.

2. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. 113 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 139 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 186 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 145 с.

6. Сорокин, А. А. Управление проектом : учеб. пособие / А.А. Сорокин, А.Ю. Орлова - Ставрополь : Издательство ФГБОУ ВПО СКФУ, 2015. - 253 с. : ил.

Практическое занятие № 5. Создание отчетов по проекту

Цель работы: изучить методы создания и анализа отчетов по проекту.

Теоретическая часть Для печати результатов работы из Project можно использовать два способа, возможности которых эффективно дополняют друг друга:

- печать экранных форм;
- печать заранее сформированных отчетов.

Кроме перечисленных возможностей, Project позволяет вставлять в документы MS Office изображения экранных форм как графические рисунки.

Для уверенного форматирования табличных отчетов и отчетов, основанных на экранных формах, необходимо иметь представление об особенностях форматирования листов распечатки средствами Project.

Для управления размещением отчета на листах следует представлять себе принципиальную схему формирования отчета. Распечатка отчета, теоретические размеры которой определяются по высоте количеством элементов графика, а по ширине - количеством печатаемых столбцов таблиц и выбранным шрифтом, покрывается листами выбранного размера.

Т.о. возможно, что отчет схематически разбивается на несколько листов бумаги, покрывающих распечатку. Если в распечатку входят табличная часть и календарная диаграмма, которая не размещается на одном листе, то на каждом последующем листе по ширине повторяется печать таблицы, расположенной в левой части отчета. Но справа от этой таблицы на каждом листе печатается уже другая часть календарной диаграммы.

В связи с тем, что расположение отрезков задач на календарной части линейной диаграммы может быть произвольным, на некоторых листах распечатки такие отрезки могут просто отсутствовать. Возможности Project позволяют (необходимости исключить печать таких листов.

Project позволяет предварительно просмотреть на экране распечатку. Благодаря этому можно сохранить много времени, бумаги и нервов.

Оборудование и материалы: для выполнения данной лабораторной работы необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, MS Project.

Указания по технике безопасности: к выполнению лабораторных работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения лабораторной работы необходимо выполнить следующее:

1.Изучить рекомендуемую литературу.

2.Сформатируйте листы отчетов проекта.

3.Задайте вывод колонтитулов и легенды на листе распечатки проекта.

4.Получите стандартные отчеты проекта.

5.Постройте новые пользовательские отчеты о затратах и задачах проекта.

6.Ответить на контрольные вопросы.

7.Оформить отчет.

Содержание отчета: отчет по лабораторной работе должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Лист ресурсов проекта.

2. Реализация проекта с использованием возможностей Консультанта.

3.Операции с фильтрами.

4. Группы отчетов Project.

5. Управление элементами пользовательского интерфейса.

6. Планирование предметной области и определение структуры работ на стадии предварительного планирования.

Список литературы, рекомендуемый к использованию по данной теме:

1. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 206 с.

2. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. 113 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 139 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 186 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 145 с.

6. Сорокин, А. А. Управление проектом : учеб. пособие / А.А. Сорокин, А.Ю. Орлова - Ставрополь: Издательство ФГБОУ ВПО СКФУ, 2015. - 253 с. : ил.

Практическое занятие № 6. Формирование базового плана проекта

Цель работы: изучить способы формирования базового плана проекта.

Теоретическая часть Оценка финансовой состоятельности проекта - это

специфическая область, в которой применяются методики бизнес-планирования. Следует учитывать, что даже при полном использовании рекомендаций Project, как и любая другая система управления проектами, позволит только сформировать исходные данные для анализа финансовой состоятельности проекта и документировать эту информацию. Выполнение самого анализа требует применения экономических методов и применяемых в выполняющей проект фирме процедур.

На основе информации о предварительном плане проекта в соответствии с принятыми в выполняющей проект фирме процедурами должны быть определены показатели проекта и уже на их основе должно быть принято решение о запуске проекта или об отказе от него. Конечно, это всегда требует проведения переговоров с инвестором, заказчиком, потребителями и другими важными участниками проекта. Этим должна завершиться инициация проекта.

Базовый план проекта возникает после утверждения предварительного плана проекта. Очень часто это происходит именно при принятии решения о запуске проекта. В таких случаях утвержденный план должен быть зафиксирован, защищен от несанкционированных изменений и распространен между участниками проекта. Очевидно, что утверждение бумажных документов (например, распечаток линейной диаграммы и бюджета предварительного расписания проекта) выполняется его визированием руководителем соответствующего уровня, который имеет на это право. Понятно, что эти документы могут быть скопированы и размножены при помощи любых технических средств.

Оборудование и материалы: для выполнения данной лабораторной работы необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, MS Project.

Указания по технике безопасности: к выполнению лабораторных работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения лабораторной работы необходимо выполнить следующее:

1.Изучить рекомендуемую литературу.

2.Проведите анализ состоятельности проекта.

3.Создайте базовый план проекта.

4.Ответить на контрольные вопросы.

5.Оформить отчет.

Содержание отчета: отчет по лабораторной работе должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1.Оценка стоимости проекта

2.Бюджет проекта

3.Группы отчетов Project

4.Оценка финансовой состоятельности проекта

5.Базовый план проекта

6.Детальное планирование проектов

Список литературы, рекомендуемый к использованию по данной теме:

1.Сорокин, А. А. Управление проектом : учеб. пособие / А.А. Сорокин, А.Ю.Орлова - Ставрополь : Издательство ФГБОУ ВПО СКФУ, 2015. - 253 с. : ил.

2.Борис, О. А. Управление проектами: фазы разработки и методология : учеб.пособие / О.А. Борис ; под ред. В.Н. Парахиной. – Ставрополь : Фабула, 2011. – 64 с.

2.Борис, О. А. Управление проектами: фазы разработки и методология : учеб. пособие /О.А. Борис ; под ред. В.Н. Парахиной. – Ставрополь : Фабула, 2011. – 64 с.

3.

Практическое занятие № 5. Оценка стоимости проекта

Цель работы: изучить основные способы оценки стоимости проекта.

Теоретическая часть Оценку стоимости проекта не следует путать с бухгалтерским учетом. Она включает следующие процессы:

- предварительная оценка финансовой состоятельности проекта;
- распределение лимитов затрат по элементам проекта.

Project обеспечивает поддержку этих процессов.

Оценка потребности в ресурсах для реализации проекта в Project основывается на принципе «снизу вверх», когда информация о задачах, включенных в график выполнения проекта, содержит оценки потребности в финансовых средствах для каждой из них. Project позволяет учитывать потребность финансовых ресурсах уже на самых ранних стадиях планирования проекта. На этой или на любой другой стадии выполнения проекта для каждой работы учитываются два компонента затрат:

- затраты, связанные с использованием ресурсов на назначениях проекта;
- прочие прямые затраты, связанные с выполнением задач проекта.

Полная сумма затрат на реализацию проекта в Project вычисляется по формуле следующего вида:

Затраты Проекта = ΣЗатратыi =ΣФиксированныеЗатратыi +

+ΣЗатратынаИспольз.j + СтандартнаяСтавкаj · Трудозатратыj |Fji =0 +

+ СтавкаСверхурочныхj · Трудозатратыij|Fji)

где: - Затраты Проекта - оценка стоимости проекта;

- Затратыi, - оценка стоимости j-й задачи проекта;

- ФиксированныеЗатратыi - прочие прямые затраты для выполнения i-й задачи проекта;

- ЗатратынаИспользi - затраты за разовое использование j-го ресурса;

- СтандартнаяСтавкаi - стандартная тарифная часовая ставка для ресурсов j-го вида;

- СтавкаСверхурочныхi - тарифная часовая ставка для ресурсов j -го вида при условии их перегрузки (если этот показатель не задан или перегрузка ресурсов отсутствует, то этот показатель автоматически принимается равным показателю СтандартнаяСтавкаj);

- Трудозатратыij- объем трудозатрат ресурса j-го вида, назначенных для i-ой задачи;

- Fjt - функция, численно равная нулю, если в интервале времени t данный ресурс у в масштабе проекта не перегружен, и равная единице, если этот ресурс в данном интервале времени перегружен.

В приведенной формуле суммирование по индексу i определяет затраты по всем задачам графика, суммирование по индексу j - затраты по всем ресурсам, а t - индекс интервала времени.

Оборудование и материалы: для выполнения данной лабораторной работы необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, MS Project.

Указания по технике безопасности: к выполнению лабораторных работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения лабораторной работы необходимо выполнить следующее:

1.Изучить рекомендуемую литературу.

2.Введите показатели фиксированных затрат для задач графика.

3.Сформируйте таблицы тарифных ставок.

4.Постройте диаграмму Гантта для предварительного графика реализациипроекта.

5.Ответить на контрольные вопросы.

6.Оформить отчет.

Содержание отчета: отчет по лабораторной работе должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1.Последовательность действий по формированию нового файла графика реализациипроекта

2.Опорные даты проекта

3.Взаимосвязь задач графика реализации проекта

4.Типы задач проекта

5.Типы задач проекта с точки зрения сроков ее начала или окончания

Список литературы, рекомендуемый к использованию по данной теме:

1.Сорокин, А. А. Управление проектом : учеб. пособие / А.А. Сорокин, А.Ю.Орлова - Ставрополь : Издательство ФГБОУ ВПО СКФУ, 2015. - 253 с. : ил.

2.Борис, О. А. Управление проектами: фазы разработки и методология : учеб.пособие / О.А. Борис ; под ред. В.Н. Парахиной. – Ставрополь : Фабула, 2011. – 64 с.

Практическое занятие №7. Бюджет проекта

Цель работы: изучить способы разработки бюджета проекта.

Теоретическая часть Анализ состава основных процессов планирования проекта показывает, что оценить связанные с проектом затраты еще недостаточно, и на этой основе следует разработать бюджет проекта. Под бюджетом проекта понимается как общая сумма затрат на проект, так и рас-пределение этих затрат по календарным интервалам. Следует отметить, что выполнение этой работы вручную с использованием снабженного планом проекта не очень сложно, но достаточно трудоемко. До этого информация преимущественно вводилась в базу данных Project, но с этого момента получение обработанных Project данных начинает приносить пользу. Оценки распределения затрат по времени Project выполняет на основании расчета временных показателей задач.

Поскольку поля Затраты и Фиксированные затраты определены для задач графика, а для каждой из них Project автоматически вычисляет даты начала и окончания, то и затраты тоже оказываются распределенными во времени в соответствии с введенными в Project для каждой задачи показателями. Для того чтобы получить доступ к информации о бюджете проекта, можно использовать формы представления информации о графике реализации проекта «Использование задач» или «График ресурсов».

Оборудование и материалы: для выполнения данной лабораторной работы необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, MS Project.

Указания по технике безопасности: к выполнению лабораторных работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения лабораторной работы необходимо выполнить следующее:

1.Изучить рекомендуемую литературу.

2.Введите показатели фиксированных затрат для задач графика.

3.Сформируйте таблицы тарифных ставок.

4.Ответить на контрольные вопросы.

5.Оформить отчет.

Содержание отчета: отчет по лабораторной работе должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1.Единицы времени применяемые Project

2.Назначение формы Календарь

3.Линейная диаграмма (Гантта)

4.Диаграмма Гантта с отслеживанием

5.Сетевой график проекта

Список литературы, рекомендуемый к использованию по данной теме:

1. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 206 с.

2. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. 113 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 139 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 186 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 145 с.

6. Сорокин, А. А. Управление проектом : учеб. пособие / А.А. Сорокин, А.Ю. Орлова - Ставрополь : Издательство ФГБОУ ВПО СКФУ, 2015. - 253 с. : ил.

Практическое занятие №1. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники

Учебные и воспитательные цели:

Изучить требования и рекомендации по защите информации.

Теоретическая часть

«Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждены приказом Гостехкомиссии России от 30.08.2002 №282.

СТР-К является нормативно-методическим документом и устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну на территории Российской Федерации.

Требования и рекомендации этого документа распространяются на защиту государственных информационных ресурсов некриптографическими методами (служебная тайна), направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и специальных воздействий на информацию в целях её уничтожения, искажения и блокирования.

При проведении работ по защите негосударственных информационных ресурсов, составляющих коммерческую тайну, банковскую тайну и т.д., требования настоящего документа носят рекомендательный характер.

Документ определяет следующие вопросы защиты конфиденциальной информации:

– организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;

– состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;

– требования и рекомендации по защите речевой информации при ведении переговоров, в том числе с использованием технических средств;

– требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;

– порядок обеспечения защиты информации при эксплуатации объектов информатизации;

– особенности защиты информации при разработке и эксплуатации АС, использующих различные типы СВТ и информационные технологии;

– о порядок обеспечения защиты информации при взаимодействии абонентов с Сетями.

Защита информации, обрабатываемой с использованием технических средств, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в виде системы (подсистемы) защиты информации во взаимосвязи с другими мерами по защите информации. Защите подлежит речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнито-оптической и иной основе.

Объектами защиты при этом являются:

– средства и системы информатизации (СВТ, АС различного уровня и назначения на базе СВТ, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования

документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), средства защиты информации, используемые для обработки конфиденциальной информации;

– технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);

– защищаемые помещения.

– Защита информации на объекте информатизации достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам, несанкционированного доступа, программно-технических

– воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе её обработки, передачи и хранения, а также работоспособности технических средств.

При защите информации в локальных вычислительных сетях (ЛВС) конфиденциальная информация может обрабатываться только в ЛВС, расположенных в пределах контролируемой зоны.

Средства зашиты информации от НСД должны использоваться во всех узлах ЛВС независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС и требуют постоянного квалифицированного контроля настроек СЗИ администратором безопасности информации. Класс защищённости ЛВС определяется в соответствии с требованиями действующих руководящих документов ФСТЭК России.

Для управления, контроля защищённости ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, должны использоваться соответствующие сертифицированные по требованиям безопасности информации средства защиты.

Вопросы и задания:

1. Что является объектом информатизации?
2. Определение СТС.
3. Обобщенная структурная схема ТКУИ, обрабатываемой СВТ.

Список литературы, рекомендуемый к использованию по данной теме

1. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 206 с.

2. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. 113 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 139 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 186 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью:

Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 145 с.

Практическое занятие №2. Классификация технических каналов утечки информации

Учебные и воспитательные цели:

Изучить классификацию технических каналов утечки информации.

Теоретическая часть

Под техническими средствами приема, обработки, хранения и передачи информации (ТСПИ) понимают технические средства, непосредственно обрабатывающие конфиденциальную информацию. К таким средствам относятся: электронно-вычислительная техника, режимные АТС, системы оперативно-командной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.д.

При выявлении технических каналов утечки информации ТСПИ необходимо рассматривать как систему, включающую основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами), распределительные и коммутационные устройства, системы электропитания, системы заземления.

Отдельные технические средства или группа технических средств, предназначенных для обработки конфиденциальной информации, вместе с помещениями, в которых они размещаются, составляют объект ТСПИ. Под объектами ТСПИ понимают также выделенные помещения, предназначенные для проведения закрытых мероприятий.

Наряду с ТСПИ в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с ТСПИ и находящиеся в зоне электромагнитного поля, создаваемого ими. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и т.д.

В качестве канала утечки информации наибольший интерес представляют ВТСС, имеющие выход за пределы контролируемой зоны (КЗ), т.е. зоны, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков

Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации можно разделить на электромагнитные, электрические и параметрические.

Электромагнитные каналы утечки информации

К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений (ЭМИ) ТСПИ:

- излучений элементов ТСПИ;
- излучений на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;

– излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Электромагнитные излучения элементов ТСПИ. В ТСПИ носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам ТСПИ вокруг них (в окружающем пространстве) возникает электрическое и магнитное поле. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Электромагнитные излучения на частотах работы ВЧ генераторов ТСПИ и ВТСС. В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т.д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных ВЧ колебаний генераторов. Эти промодулированные ВЧ колебания излучаются в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ. Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи т.п.) возможно за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения лежит в пределах рабочих частот нелинейных элементов УНЧ (например, полупроводниковых приборов, электровакуумных ламп и т.п.). Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе УНЧ в нелинейный режим работы, т.е. в режим перегрузки.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными вне контролируемой зоны.

Зона, в которой возможен перехват (с помощью разведывательного приемника) побочных электромагнитных излучений и последующая расшифровка содержащейся в них информации (т.е. зона, в пределах которой отношение "информационный сигнал/помеха" превышает допустимое нормированное значение), называется (опасной) зоной 2.

Электрические каналы утечки информации

Причинами возникновения электрических каналов утечки информации могут быть:

– наводки электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;

– просачивание информационных сигналов в цепи электропитания ТСПИ;

– просачивание информационных сигналов в цепи заземления ТСПИ.

Наводки электромагнитных излучений ТСПИ возникают при излучении элементами ТСПИ (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий ТСПИ и посторонних проводников или линий ВТСС. Уровень наводимых сигналов в значительной

степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ТСПИ и посторонних проводников.

Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется (опасной) зоной 1.

Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенная случайная антеннапредставляет собой компактное техническое средство, например телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д. К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Просачивание информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором выпрямительного устройства. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Просачивание информационных сигналов в цепи заземления. Кроме заземляющих проводников, служащих для непосредственного соединения ТСПИ с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны (металлические оболочки) соединительных кабелей, металлические трубы систем отопления и водоснабжения, металлическая арматура железобетонных конструкций и т.д. Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, на которую могут наводиться информационные сигналы. Кроме того, в грунте вокруг заземляющего устройства возникает электромагнитное поле, которое также является источником информации.

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам, проходящим через помещения, где установлены ТСПИ, а также к их системам электропитания и заземления. Для этих целей используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Съем информации с использованием аппаратных закладок. В последние годы участились случаи съема информации, обрабатываемой в ТСПИ, путем установки в них электронных устройств перехвата информации –закладных устройств.

Электронные устройства перехвата информации, устанавливаемые в ТСПИ, иногда называют аппаратными закладками. Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в ТСПИ иностранного производства, однако возможна их установка и в отечественных средствах.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем по команде передается на запросивший ее объект.

Параметрический канал утечки информации

Перехват обрабатываемой в технических средствах информации возможен также путем их “высокочастотного облучения”. При взаимодействии облучающего электромагнитного поля с элементами ТСПИ происходит переизлучение электромагнитного поля. В ряде случаев это вторичное излучение модулируется информационным сигналом. При съеме информации для исключения взаимного влияния облучающего и переизлученного сигналов может использоваться их временная или частотная развязка. Например, для облучения ТСПИ могут использовать импульсные сигналы.

При переизлучении параметры сигналов изменяются. Поэтому данный канал утечки информации часто называют параметрическим.

Для перехвата информации по данному каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности и специальные радиоприемные устройства.

Информация после обработки в ТСПИ может передаваться по каналам связи, где также возможен ее перехват.

В настоящее время для передачи информации используют в основном КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи. В зависимости от вида каналов связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные.

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования.

Данный канал перехвата информации наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры разведки к кабельным линиям связи.

Самый простой способ –это непосредственное параллельное подключение к линии связи. Но данный факт легко обнаруживается, так как приводит к изменению характеристик линии связи за счет падения напряжения.

Поэтому средства разведки к линии связи подключаются или через согласующее устройство, несколько снижающее падение напряжения, или через специальные устройства компенсации падения напряжения. В последнем случае аппаратура разведки и устройство компенсации падения напряжения включаются в линию связи последовательно, что существенно затрудняет обнаружение факта несанкционированного подключения к ней.

Контактный способ используется в основном для снятия информации с коаксиальных и низкочастотных кабелей связи. Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации.

Электрический канал наиболее часто используется для перехвата телефонных разговоров. При этом перехватываемая информация может непосредственно записываться на диктофон или передаваться по радиоканалу в пункт приема для ее записи и анализа. Устройства, подключаемые к телефонным линиям связи и комплексированные с устройствами передачи информации по радиоканалу, часто называют телефонными закладками.

В случае использования сигнальных устройств контроля целостности линии связи, ее активного и реактивного сопротивления факт контактного подключения к ней

аппаратуры разведки будет обнаружен. Поэтому спецслужбы наиболее часто используют индуктивный канал перехвата информации, не требующий контактного подключения к каналам связи. В данном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики используются в основном для съема информации с симметричных высокочастотных кабелей. Сигналы с датчиков усиливаются, осуществляется частотное разделение каналов, и информация, передаваемая по отдельным каналам, записывается на магнитофон или высокочастотный сигнал записывается на специальный магнитофон.

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные низкочастотные усилители, снабженные магнитными антеннами.

Некоторые средства бесконтактного съема информации, передаваемой по каналам связи, могут комплексироваться с радиопередатчиками для ретрансляции в центр ее обработки.

Вопросы и задания:

1. Источники сигнала.
2. Функции передатчика.
3. Классификация технических каналов утечки информации.

Список литературы, рекомендуемый к использованию по данной теме

1. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 206 с.

2. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. 113 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 139 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 186 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 145 с.

Практическое занятие №3. Четырехфазная модель процесса управления информационной безопасностью

Учебные и воспитательные цели:

Изучить четырехфазную модель процесса управления информационной безопасностью.

Теоретическая часть

Мы приступаем к детальному рассмотрению четырехфазной (планирование - реализация - оценка - корректировка, ПРОК) модели процесса управления информационной безопасностью, примененной в стандарте BS 7799-2:2002.

Процесс управления имеет циклический характер; на фазе первоначального планирования осуществляется вход в цикл. В качестве первого шага должна быть определена и документирована политика безопасности организации.

Затем определяется область действия системы управления информационной безопасностью. Она может охватывать всю организацию или ее части. Следует специфицировать зависимости, интерфейсы и предположения, связанные с границей между СУИБ и ее окружением; это особенно важно, если в область действия попадает лишь часть организации. Большую область целесообразно поделить на подобласти управления.

Ключевым элементом фазы планирования является анализ рисков. Этот вопрос детально рассмотрен в курсе "Основы информационной безопасности"; здесь мы не будем на нем останавливаться.

Результат анализа рисков - выбор регуляторов безопасности. План должен включать график и приоритеты, детальный рабочий план и распределение обязанностей по реализации этих регуляторов.

На второй фазе - фазе реализации - руководством организации выделяются необходимые ресурсы (финансовые, материальные, людские, временные), выполняется реализация и внедрение выбранных регуляторов, сотрудникам объясняют важность проблем информационной безопасности, проводятся курсы обучения и повышения квалификации. Основная цель этой фазы - ввести риски в рамки, определенные планом.

Назначение фазы оценки - проанализировать, насколько эффективно работают регуляторы и система управления информационной безопасностью в целом. Кроме того, следует принять во внимание изменения, произошедшие в организации и ее окружении, способные повлиять на результаты анализа рисков. При необходимости намечаются корректирующие действия, предпринимаемые в четвертой фазе. Коррекция должна производиться, только если выполнено по крайней мере одно из двух условий:

- выявлены внутренние противоречия в документации СУИБ;
- риски вышли за допустимые границы.

Оценка может выполняться в нескольких формах:

- регулярные (рутинные) проверки;
- проверки, вызванные появлением проблем;
- изучение опыта (положительного и отрицательного) других организаций;
- внутренний аудит СУИБ;
- инспекции, проводимые по инициативе руководства;
- анализ тенденций.

Аудит должен выполняться регулярно, не реже одного раза в год. В процессе аудита следует убедиться в следующем:

- политика безопасности соответствует производственным требованиям;
- результаты анализа рисков остаются в силе;
- документированные процедуры выполняются и достигают поставленных целей;
- технические регуляторы безопасности (например, межсетевые экраны или средства ограничения физического доступа) расположены должным образом, правильно сконфигурированы и работают в штатном режиме;
- действия, намеченные по результатам предыдущих проверок, выполнены.

Даже если недопустимых отклонений не выявлено и уровень безопасности признан удовлетворительным, целесообразно зафиксировать изменения в технологии и производственных требованиях, появление новых угроз и уязвимостей, чтобы предвидеть будущие изменения в системе управления.

Систему управления информационной безопасностью надо постоянно совершенствовать, чтобы она оставалась эффективной . Эту цель преследует четвертая фаза рассматриваемого в стандарте цикла - корректировка. Она может потребовать как относительно незначительных действий, так и возврата к фазам планирования (например, если появились новые угрозы) или реализации (если следует осуществить намеченное ранее).

При корректировке прежде всего следует устранить несоответствия следующих видов:

– отсутствие или невозможность реализации некоторых требований СУИБ;

– неспособность СУИБ обеспечить проведение в жизнь политики безопасности или обслуживать производственные цели организации.

Задача фазы оценки - выявить проблемы. На фазе корректировки необходимо докопаться до их корней и устранить первопричины несоответствий, чтобы избежать повторного появления. С этой целью могут предприниматься как реактивные, так и превентивные действия, рассчитанные на среднесрочную или долгосрочную перспективу.

Таково (в сжатом изложении) содержание двух частей стандарта BS 7799. Может показаться, что каждое из его положений самоочевидно; тем не менее, собранные вместе и систематизированные, они обладают несомненной ценностью.

Вопросы и задания:

1. Формы оценки.
2. Опишите процесс аудита.
3. Опишите процесс коррекции.

Список литературы, рекомендуемый к использованию по данной теме

1. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 206 с.

2. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. 113 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 139 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 186 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 145 с.

Практическое занятие №4. Эксплуатационное окружение, управление криптографическими ключами

Учебные и воспитательные цели:

1. Изучить эксплуатационное окружение.
2. Разобрать управление криптографическими ключами.

Теоретическая часть

Эксплуатационное окружение - это совокупность необходимых для функционирования модуля средств управления аппаратными и программными компонентами. В стандарте FIPS 140-2 рассматривается несколько видов окружения:

– универсальное, с коммерческой операционной системой, управляющей как компонентами модуля, так и другими процессами и приложениями;

– ограниченное, являющееся статическим, немодифицируемым (например, виртуальная Java-машина на непрограммируемой плате для персонального компьютера);

– модифицируемое, которое может быть реконфигурировано и включать средства универсальных ОС .

Ядро универсального и модифицируемого окружения - операционная система. На первом уровне безопасности к ней предъявляются следующие требования:

– используется только однопользовательский режим, параллельная работа нескольких операторов явным образом запрещается;

– доступ процессов, внешних по отношению к модулю, к данным, критичным для безопасности, запрещается, некриптографические процессы не должны прерывать работу криптографического модуля;

– программное обеспечение модуля следует защитить от несанкционированного раскрытия и модификации;

– целостность ПО модуля контролируется утвержденными средствами.

Для второго уровня безопасности требуется использование ОС, сертифицированных на соответствие определенным профилям защиты на основе "Общих критериев" с оценочным уровнем доверия не ниже второго. Для защиты критичных данных должно применяться произвольное управление доступом с определением соответствующих ролей. Необходимо протоколирование действийкрипто-офицера.

Характерная черта третьего уровня безопасности - использование доверенного маршрута.

На четвертом уровне безопасности криптографического модуля нужна ОС с оценочным уровнем доверия не ниже четвертого.

Требования безопасного управления криптографическими ключами охватывают весь жизненный цикл критичных данных модуля. Рассматриваются следующие управляющие функции: генерация случайныхчисел; генерация ключей ; распределение ключей ; ввод/вывод ключей ; хранение ключей ; обнуление ключей.

Секретные ключи необходимо защищать от несанкционированного раскрытия, модификации и подмены, открытые - от модификации и подмены.

Компрометация методов генерации или распределения ключей (например, угадывание затравочного значения, инициализирующего детерминированный генератор случайных чисел) должна быть не проще определения значений ключей.

Для распределения ключей может применяться как ручная транспортировка, так и автоматические процедуры согласования ключей.

Допускается ручной (с клавиатуры) и автоматический (например, при помощи смарт-карты) ввод ключей. На двух нижних уровнях безопасности при автоматическом вводе секретные ключи должны быть зашифрованы; ручной ввод может осуществляться в открытом виде. На третьем и четвертом уровнях при ручном вводе ключей в открытом виде применяются процедуры разделения знаний.

Модуль должен ассоциировать введенный ключ (секретный или открытый) с владельцем (лицом, процессом и т.п.).

Вопросы и задания:

1. Виды окружения.
2. Требования к ОС.
3. Управляющие функции.

Список литературы, рекомендуемый к использованию по данной теме

1. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 206 с.

2. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. 113 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 139 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 186 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия-Телеком, 2012. – 145 с.