МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению лабораторных работ
по дисциплине
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
для направления подготовки **09.03.02 Информационные системы и технологии**
направленность (профиль) **Информационные системы и технологии обработки цифрового контента**

Пятигорск
2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В методических указаниях содержатся материалы, необходимые для самостоятельной подготовки студентов к выполнению лабораторных работ. В описание работ включены цель работы, порядок ее выполнения, рассмотрены теоретические вопросы, связанные с реализацией поставленных задач, приведена необходимая литература.

Методические указания посвящены курсу «Информационная безопасность».

Практикум построен на принципе последовательного изучения объекта исследования с развитием и закреплением знаний и навыков работы.

Результаты работы представляются, как правило, в виде файлов, формат и наименование которых определяется требованиями по оформлению.

Каждая работа заканчивается контрольными вопросами, позволяющими провести самоконтроль и укрепить теоретические знания и практические навыки.

Состав и оформление проекта приводится в соответствие с действующими на сегодняшний день нормами и требованиями государственных стандартов РФ.

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование набора общепрофессиональных компетенций будущего бакалавра по направлению подготовки 09.03.02.

Задачами освоения дисциплины являются: формирование базовых понятий в области информационной безопасности и защиты информации, осознание места и роли информационной безопасности в системе национальной безопасности РФ и выработка первоначальных лабораторных навыков по защите документов на персональном компьютере.

2. ОБОРУДОВАНИЕ И МАТЕРИАЛЫ

Аппаратные средства: персональный компьютер.

Программные средства: ОС MS Windows, MS Office.

Учебный класс оснащен IBM-совместимыми компьютерами, объединенными в локальную сеть. Локальная сеть учебного класса имеет постоянный доступ к сети Internet по выделенной линии. Для проведения лабораторных работ необходимо 10 ПК.

3. УКАЗАНИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ

Перед началом работы следует убедиться в исправности электропроводки, выключателей, штепсельных розеток, при помощи которых оборудование включается в сеть, наличии заземления компьютера, его работоспособности.

Для снижения или предотвращения влияния опасных и вредных факторов необходимо соблюдать санитарные правила и нормы, гигиенические требования к персональным электронно-вычислительным машинам.

Во избежание повреждения изоляции проводов и возникновения коротких замыканий не разрешается: вешать что-либо на провода, закрашивать и белить шнуры и провода, закладывать провода и шнуры за газовые и водопроводные трубы, за батареи отопительной системы, выдергивать штепсельную вилку из розетки за шнур, усилие должно быть приложено к корпусу вилки.

Для исключения поражения электрическим током запрещается: часто включать и выключать компьютер без необходимости, прикасаться к экрану и к тыльной стороне блоков компьютера, работать на средствах вычислительной техники и периферийном оборудовании мокрыми руками, работать на средствах вычислительной техники и периферийном оборудовании, имеющих нарушения целостности корпуса, нарушения изоляции проводов, неисправную индикацию включения питания, с признаками электрического напряжения на

корпусе, класть на средства вычислительной техники и периферийном оборудовании посторонние предметы.

Запрещается под напряжением очищать от пыли и загрязнения электрооборудование.

Во избежание поражения электрическим током, при пользовании электроприборами нельзя касаться одновременно каких-либо трубопроводов, батарей отопления, металлических конструкций, соединенных с землей.

После окончания работы необходимо обесточить все средства вычислительной техники и периферийное оборудование. В случае непрерывного учебного процесса необходимо оставить включенными только необходимое оборудование.

4. СОДЕРЖАНИЕ ЛАБОРАТОРНЫХ РАБОТ

Лабораторное занятие №1. Оценка рисков информационной безопасности на основе методики OCTAVE

Цель работы: освоить на практике процесс оценки рисков информационной безопасности на основе методики OCTAVE.

Теоретическая часть

На сегодняшний день вопрос оценки рисков информационной безопасности является актуальным для многих предприятий. Информационный риск – это возможность наступления случайного события в информационной системе предприятия, приводящего к нарушению ее функционирования, снижению качества информации, в результате которых наносится ущерб предприятию. Связано это в первую очередь с модернизированной нормативно-правовой базой, позволяющей четко определять наказания и штрафы для операторов систем защиты конфиденциальной информации, не обеспечивающих принципы конфиденциальности, целостности и доступности последней.

Но разберемся, зачем нужно исследовать риски в сфере ИБ и что это может дать при разработке системы обеспечения ИБ для ИС. Для любого проекта, требующего финансовых затрат на его реализацию, весьма желательно уже на начальной стадии определить, что мы будем считать признаком завершения работы и как будем оценивать результаты проекта. Для задач, связанных с обеспечением ИБ это более чем актуально.

На практике наибольшее распространение получили два подхода к обоснованию проекта подсистемы обеспечения безопасности.

Первый из них основан на проверке соответствия уровня защищенности ИС требованиям одного из стандартов в области информационной безопасности. Это может быть *класс* защищенности в соответствии с требованиями руководящих документов ФСТЭК России, *профиль защиты*, разработанный в соответствии со стандартом ISO-15408, или какой-либо другой набор требований. Тогда критерий достижения цели в области безопасности - это выполнение заданного набора требований. *Критерий эффективности* - минимальные суммарные *затраты* на выполнение поставленных функциональных требований:

Вместе с этим сформулированные понятия уровня исходной защищенности и вероятности реализации угрозы не позволяют оператору получить полное представление о защищенности ценных ресурсов и спрогнозировать возможный ущерб при их разглашении, удалении или изменении. Существующие методики оценки рисков информационной безопасности (CRAMM, FRAP, RiskWatch, OCTAVE и др.) позволяют спрогнозировать возможный ущерб.

Наиболее интересной и многосторонней является методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation, в переводе с англ. – «оперативная оценка критических угроз, активов и уязвимостей»).

В основе ее работы лежит дерево, имеющее вершины «Ресурс», «Уязвимость», «Угроза», «Ущерб», «Риск». В данной статье предпринята попытка проецирования данной

методики на процесс оценки рисков предприятий разного профиля на территории Российской Федерации. Алгоритм оценки рисков информационной безопасности (ИБ) на предприятии в соответствии с методикой OCTAVE состоит из нескольких этапов (рисунок):

1) Определение активов организации
2) Определение ценности активов организации (S_i).
3) Определение угроз и соответствующих им уязвимости.
4) Оценка вероятности реализации угроз (V_{ry}).
5) Определение риска информационной безопасности (R).
6) Формирование плана по снижению риска ИБ [1].

На рис. 1 представлена блок-схема алгоритма оценки рисков ИБ в соответствии с методикой OCTAVE

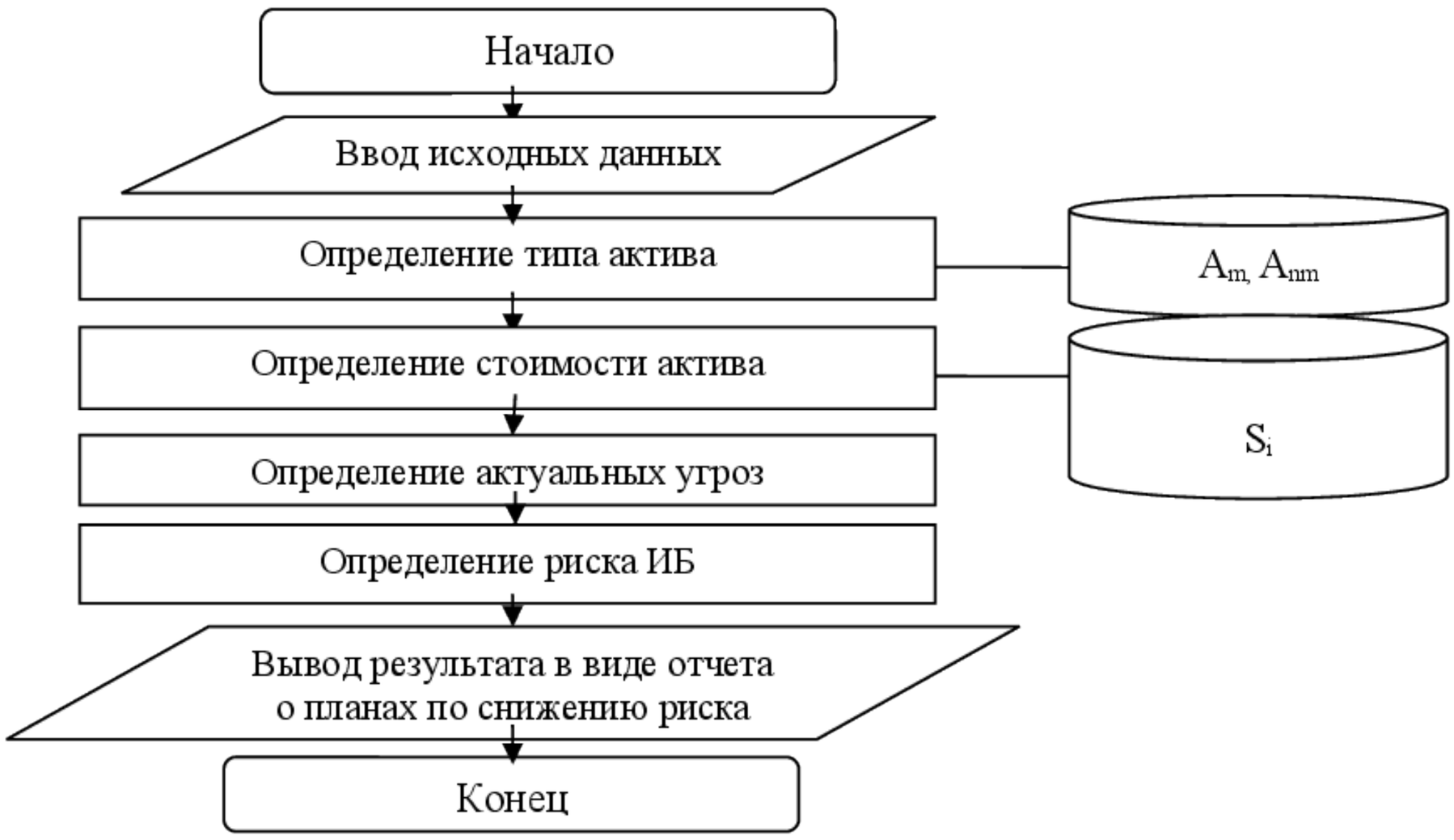

Рис. 1.

Блок-схема алгоритма оценки рисков ИБ в соответствии с методикой OCTAVE

Пример расчета риска для условной организации – ООО «Олимп»:

1) На данном этапе необходимо определить все активы организации. Целесообразно разделить их на материальные (A_m) и нематериальные (A_{nm}) (табл. 1).

Таблица 1.

Определение активов организации

№ п/п	**Материальные активы (A_m)**	**№ п/п**	**Нематериальные активы (A_{nm})**
1.1	Производственное оборудование	2.1	Персональные данные (личные дела сотрудников, медицинские карты)
1.2	Электронно-вычислительные машины	2.2	Коммерческая тайна (бизнес-план, секрет производства)
1.3	Комплектующие изделия	2.3	Иная конфиденциальная информация

2) Для определения ценности активов организации необходимо определить их возможную стоимость или тот денежный ущерб, который может быть нанесен вследствие разглашения, утраты, уничтожения данного актива.

Для удобства будем использовать информационной безопасности используем балльную систему. Для оценки стоимости активов введем соответствующие баллы (табл. 2).

Таблица 2. Определение ценности активов организации

№ актива	Основание для оценки актива	Стоимость актива (S_i)	№ актива	Основание для оценки актива	Стоимость актива (S_i)
1.1	Производственное оборудование	10 баллов (≥ 1 000 000 руб.)	2.1	Персональные данные	6 баллов (500 000 т.руб.)
1.2	Электронно-вычислительные машины	2 балла (> 10 000 т.руб.)	2.2	Коммерческая тайна	6 баллов (120 000 т.руб.)
1.3	Комплектующие изделия	6 баллов (> 100 000 т.руб.)	2.3	Иная конфиденциальная информация	2 балла (50 000 т.руб.)

3) На следующем этапе оценки рисков ИБ определяем угрозы безопасности информации и соответствующие им уязвимости (табл. 3) [2].

Таблица 3. Перечень угроз и соответствующих им уязвимостей

№ п/п	Угрозы	Уязвимости
1	Утечка видовой информации	Отсутствие жалюзи на окнах
		Расположение ПК мониторами к окнам
2	Утечка акустической информации	Отсутствие шумогенератора
3	Кража носителей информации	Хранение носителей информации за пределами сейфа
		Отсутствие системы контроля доступа
		Отсутствие системы видеонаблюдения
		Отсутствие системы охранной сигнализации
4	Утечка информации по каналам ПЭМИН	Отсутствие экранирования кабельных коммуникаций
5	Преднамеренное уничтожение информации	Отсутствие утвержденного «Положения о разграничении доступа»
		Отсутствие программной системы разграничения доступа типа Secret Net
		Отсутствие системы контроля доступа, КПП
		Отсутствие утвержденного «Положения о защите конфиденциальной информации, обрабатываемой в организации»
6	Непреднамеренное уничтожение информации	Отсутствие системы резервного копирования
		Отсутствие учета доступа сотрудников к конфиденциальной информации
7	Установка ПО, не связанного с исполнением служебных обязанностей	Отсутствие средств доверенной загрузки
8	Действия вредоносных программ	Не установлено сертифицированное антивирусное ПО
		Отсутствие средств резервного копирования

9	Угрозы несанкционированного доступа по каналам связи	Отсутствие средств межсетевого экранирования
10	Стихийное бедствие	Отсутствие противопожарной системы
11	Непреднамеренная модификация (уничтожение) информации сотрудниками	Отсутствие средств защиты от НСД

4) На следующем этапе определяем вероятность реализации угроз - $V_{гу}$. Предварительно необходимо указать наличие средств защиты в организации (табл. 4).

Таблица 4. Фрагмент опросной таблицы «Оценка вероятности реализации угроз»

№ п/п	**Угроза**	**Средство нейтрализации угрозы**	**Имеется ли на объекте данное средство защиты?**	
			Да	Нет
1	Утечка видовой информации	Жалюзи на окнах	+	
2	Утечка акустической информации	Шумогенератор		+
3	Кража носителей информации	Сейфы для хранения носителей информации	+	
		Система контроля доступа		+
		Система видеонаблюдения	+	
		Охранная сигнализация	+	
4	Утечка информации по каналам ПЭМИН	Экранирование кабельных коммуникаций		+
5	Преднамеренное уничтожение информации	Система видеонаблюдения	+	
		Сигнализация	+	
		Решетки на окнах		+
		КПП		+
6	Непреднамеренное уничтожение информации	Учет доступа сотрудников к конфиденциальной информации		+
		Средства резервного копирования		+
7	Установка ПО, не связанного с исполнением служебных обязанностей	Средства доверенной загрузки	+	
8	Действия вредоносных программ	Антивирусное сертифицированное ПО на ПК сотрудников		+
		Средства резервного копирования		+
9	Угрозы несанкционированного доступа по каналам связи	Средства межсетевого экранирования	+	
10	Стихийное бедствие	Противопожарная система	+	
11	Непреднамеренная модификация (уничтожение) информации сотрудниками	Средства защиты от НСД	+	

19 – 100%

10 – x%

100/19=5,3%

Вероятность реализации угроз ($V_{гу}$) определяется следующим образом:

- $V_{гу}$=1 - в случае наличия на объекте средств защиты не менее 50 % от общего числа средств защиты;

- $V_{гу}$=5 - в случае отсутствия на объекте средств защиты от 50 % до 80 % от общего числа средств защиты;

- $V_{гу}$=10 - в случае отсутствия более 80 % средств защиты.

В приведенном фрагменте опросной таблицы (табл. 4) на объекте необходимо наличие 19 различных средств защиты. Из них отсутствует 57% средств защиты, следовательно, $V_{гу}$=5.

5) Для определения риска информационной безопасности (R) воспользуемся формулой:

$$R= S*V_{гу}, \qquad (1)$$

где:

$V_{гу}$ – вероятность реализации угрозы;

S – ценность всех активов, определяемое выражением:

$$S=\sum_{i=0}^{n} S_i, \qquad (2)$$

где:

S_i – стоимость активов, по которым проводится расчет риска.

Если проводится расчет риска для активов «Электронно-вычислительные машины» и «Коммерческая тайна», то S=2+6=8 (балов), а R=5*8=40.

6) Определив значение риска, мы можем сформировать план по его снижению. Для этого необходимо определить величину риска ИБ, выраженную через качественный показатель (табл. 5) и временное значение риска ИБ по таблице 6 в зависимости от показателя вероятности реализации угроз ($V_{гу}$).

Таблица 5. Определение величины риска ИБ

	R						
$V_{гу}$	60-100	50-59	30-49	20-29	10-29	6-9	2-5
10	Высокая	Средняя	Средняя	Низкая	Низкая	Низкая	Низкая
5	Высокая	Высокая	Средняя	Средняя	Низкая	Низкая	Низкая
1	Высокая	Высокая	Высокая	Высокая	Высокая	Средняя	Низкая

Для R=40 и $V_{гу}$ = 5 качественный показатель величины риска ИБ будет: Средняя.

Если проводить расчет риска для активов «Производственное оборудование» и/или «Комплектующие изделия», то Перечень угроз и соответствующих им уязвимостей необходимо скорректировать под данные активы.

Определим временное значение риска ИБ по таблице 6 для нашего показателя вероятности реализации угроз ($V_{гу}$). План по снижению риска: на среднюю перспективу

Таблица 6. Определение временных значений риска ИБ

$V_{гу}$	План по снижению риска

1	Долговременный
5	На среднюю перспективу
10	Списки задач на ближайшее время

На основании данных табл. 5-6 можно сделать вывод о том, что план по снижению риска индивидуален для каждой вероятности реализации угроз.

Иллюстрация процесса оценки риска ИБ по методике OCTAVE на примере условной организации – ООО «Олимп» представлена в табл. 7.

Таблица 7. Процесс оценки риска ИБ

Активы организации	**Ценность актива**	**Вероятность реализации угрозы**	**Риск ИБ**	**Величина риска ИБ**	**План по снижению риска**
ЭВМ+ Коммерческая тайна	S= 8	$V_{гу}$= 5	R=40	Средняя	На среднюю перспективу

В отличие от прочих методик, OCTAVE не предполагает привлечения для исследования безопасности ИС сторонних экспертов, а вся документация по OCTAVE общедоступна и бесплатна, что делает методику особенно привлекательной для предприятий с жестко ограниченным бюджетом, выделяемым на цели обеспечения ИБ.

Таким образом, с помощью использования основ методики OCTAVE можно однозначно определить риск информационной безопасности.

Задания

Для выполнения лабораторной работы необходимо:

1) Описать активы организации согласно примера, представленного в табл. 1. Для этого учесть, что активами организации являются электронно-вычислительные машины и персональные данные.
2) Определить ценности активов организации согласно примера, представленного в табл. 2.
3) Определить угрозы и соответствующих им уязвимости. Для этого взять за основу таблицу 3, при необходимости дополнить её.
4) Определить вероятность реализации угроз - $V_{гу}$ (табл. 4). Для заполнения таблицы использовать варианты заданий, приведенные в таблице 8. Вариант задания определяется по порядковому номеру студента в списке преподавателя.

Таблица 8.

Варианты исходных данных для определения вероятности реализации угроз

№ п/п	**Средство нейтрализации угрозы**	**Варианты с имеющимися на объекте средствами защиты**																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	Жалюзи на окнах	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
2	Шумогенератор		+	+	+	+	+	+	+	+					+	+	+	+	+	+	+
3	Сейфы для хранения носителей информации	+			+	+	+	+	+	+	+	+	+	+				+	+	+	+
	Система контроля доступа				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
	Система видеонаблюдения					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

№ п/п	Средство нейтрализации угрозы	Варианты с имеющимися на объекте средствами защиты																			
	Сохранная сигнализация						+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
4	Экранирование кабельных коммуникаций							+	+	+	+	+	+	+	+	+	+	+	+	+	+
5	Система видеонаблюдения								+	+	+	+	+	+	+	+	+	+	+	+	+
	Сигнализация									+	+	+	+	+	+	+	+	+	+	+	+
	Решетки на окнах										+	+	+	+	+	+	+	+	+	+	+
	КПП																				
6	Учет доступа сотрудников к конфиденциальной информации												+	+	+	+	+	+	+	+	+
	Средства резервного копирования																			+	+
7	Средства доверенной загрузки																	+	+	+	+
8	Антивирусное сертифицированное ПО на ПК сотрудников										+	+	+					+	+	+	+
	Средства резервного копирования																			+	+
9	Средства межсетевого экранирования																				+
10	Противопожарная система	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
11	Средства защиты от НСД																				+

5) Определить ценность всех активов по формуле (2).
6) Определить риск информационной безопасности по формуле (1).
7) Сформировать план по снижению риска, воспользовавшись таблицами 5-6.
8) Проиллюстрировать процесс оценки риска ИБ, воспользовавшись таблицей 7.
9) Оформить отчёт.
10) Ответить на контрольные вопросы.
11) Сделать вывод.

Контрольные вопросы:

1. Раскройте понятие информационного риска.
2. Перечислите этапы оценки риска по методике OCTAVE.
3. Что подразумевается под критерием эффективности?
4. Назовите способы предотвращения риска.

Список литературы

Перечень основной литературы:

1. Голембиовская, О.М. Оценка рисков безопасности информационных систем персональных данных / О.М. Голембиовская, В.И. Аверченков, М.Ю. Рытов//Информация и безопасность. – Воронеж. 2 12. – №3. – С. 321 – 328.

2. Формализация подходов к обеспечению защиты персональных данных, обрабатываемых в информационных системах: монография/ О.М.Голембиовская, М.Ю.Рытов, К.Е.Шинаков. – Брянск: БГТУ, 2014. – 189 с.

Перечень дополнительной литературы:

1 Булгакова С.В. Управленческий учет : учебник для бакалавров / С.В. Булгакова ; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский государственный университет», Министерство образования и науки РФ. - Воронеж : Издательский дом ВГУ, 2015. - 370 с. - Библиогр.: с. 357-364. - ISBN 978-5-9273-2193-3 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=441585.

2. Гринберг, А.С. Документационное обеспечение управления: учебник / А.С. Гринберг, Н.Н. Горбачёв, О.А. Мухаметшина. - Москва : Юнити-Дана, 2015. - 391 с. : табл., граф., ил., схемы - Библиогр.: с. 382-383. - ISBN 978-5-238-01770-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=115031.

Интернет-ресурсы:

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.
4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

Лабораторное занятие №2. Разработка политики информационной безопасности предприятия: верхний уровень

Цель работы: изучить существующие стандарты международного и отечественного уровня в области построения политики безопасности.

Актуальность темы

Актуальность разработки политик информационной безопасности для компаний объясняется необходимостью создания механизма управления и планирования информационной безопасности. Также политики ИБ позволяют совершенствовать следующие направления деятельности компании: поддержка непрерывности бизнеса; повышение уровня доверия к компании; привлечение инвестиций и т.д. Естественно, что совершенствование направлений деятельности организации зависит от грамотности составления политики информационной безопасности.

Теоретическая часть

Для организаций общий подход и намерения в области обеспечения информационной безопасности (ОИБ), официально выраженные руководством, отражаются в разработанном, утвержденном им и строго выполняемом на практике всеми ее сотрудниками и бизнес-партнерами документе – Политика ИБ организации.

Политика ИБ непосредственно связана с законодательством в области ОИБ. Она представляет собой директиву и выражает позицию высшего руководства организации по отношению к деятельности в области ОИБ за счет создания программы ОИБ, установки ее целей и распределения обязанностей, а также стремление организации соответствовать государственным, международным требованиям и стандартам в этой области. Таким образом.

Политика ИБ организации является основой для разработки целого ряда документов в области ОИБ: стандартов, руководств, процедур, практик, регламентов, должностных инструкций и пр.

Политика ИБ организации определяется как:

– совокупность требований и правил по ОИБ для объекта ИБ, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия заданному множеству угроз ИБ, с учетом ценности защищаемой информационной сферы и стоимости системы ОИБ (СОИБ);

– документированные решения в области ОИБ;

– совокупность (одно или несколько) документированных правил, процедур, лабораторных приемов в области безопасности, которыми руководствуется организация в своей деятельности;

– документацию, определяющую высокоуровневые цели, содержание и основные направления и устанавливающую правила, процедуры, практические приемы и руководящие принципы ОИБ активов организации, которыми она руководствуется в своей деятельности.

Политика информационной безопасности представляет собой комплекс документов, отражающих все основные требования к обеспечению защиты информации и направления работы предприятия в этой сфере. При построении политики безопасности можно условно выделить три ее основных уровня: верхний, средний и нижний.

Верхний уровень политики информационной безопасности предприятия служит:

– для формулирования и демонстрации отношения руководства предприятия к вопросам информационной безопасности и отражения общих целей всего предприятия в этой области;

– основой для разработки индивидуальных политик безопасности (на более низких уровнях), правил и инструкций, регулирующих отдельные вопросы;

– средством информирования персонала предприятия об основных задачах и приоритетах предприятия в сфере информационной безопасности.

Примерная схема представлена на рисунке 1.

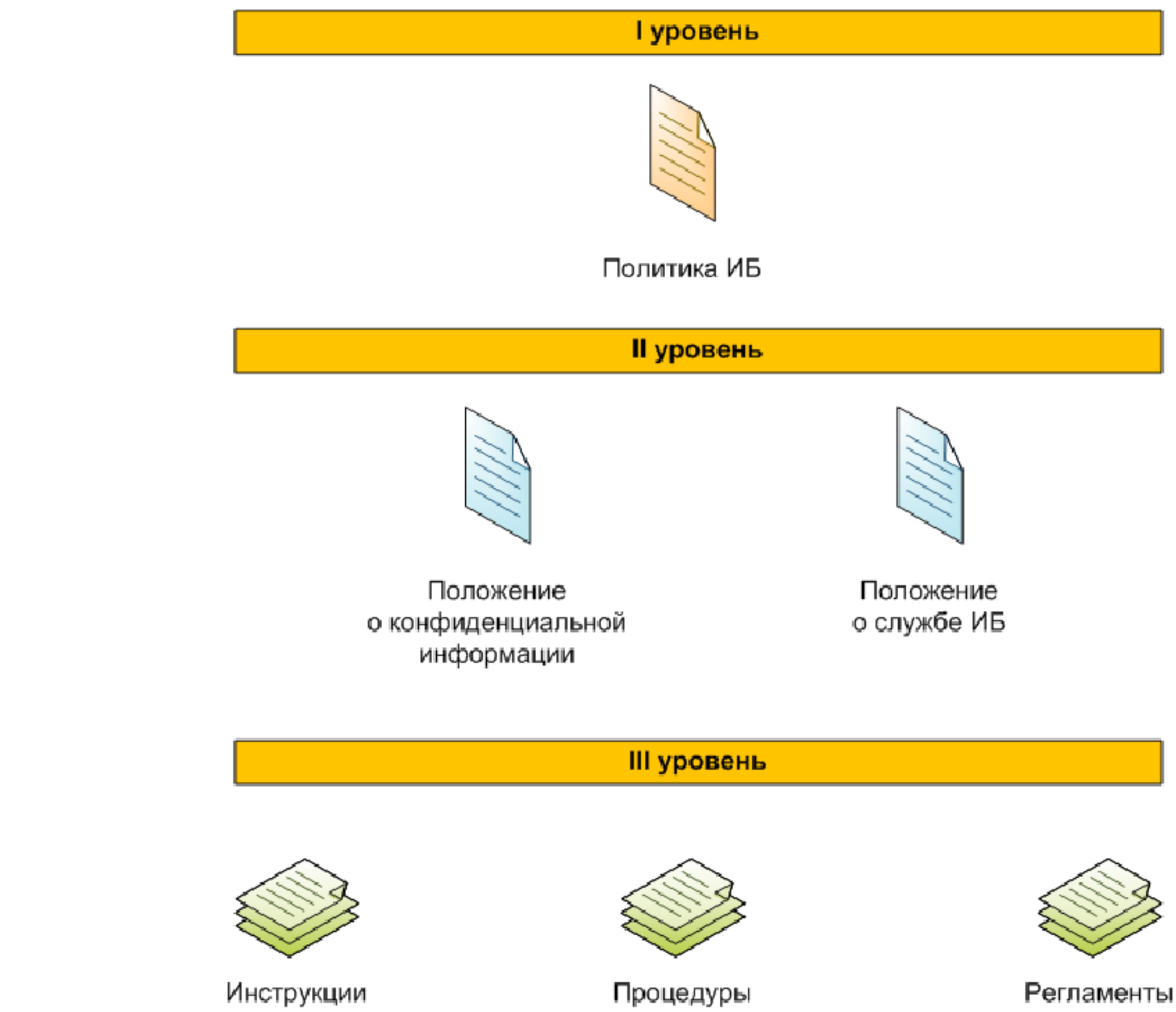

Рисунок 1. Структура нормативно-методических документов в области ИБ

При разработке политик безопасности всех уровней необходимо придерживаться следующих основных правил:

- Политики безопасности на более низких уровнях должны полностью подчиняться соответствующей политике верхнего уровня, а также действующему законодательству и требованиям государственных органов.
- Текст политики безопасности должен содержать только четкие и однозначные формулировки, не допускающие двойного толкования.
- Текст политики безопасности должен быть доступен для понимания тех сотрудников, которым он адресован.

В целом политика информационной безопасности должна давать ясное представление о требуемом поведении пользователей, администраторов и других специалистов при внедрении и использовании информационных систем и средств защиты информации, а также при осуществлении информационного обмена и выполнении операций по обработке информации. Кроме того, из политики безопасности, если она относится к определенной технологии или некоторой области защиты информации, должны быть понятны основные принципы работы этой технологии. Важной функцией политики безопасности является четкое разграничение ответственностей в процедурах информационного обмена: все заинтересованные лица должны ясно осознавать границы как своей ответственности, так и

ответственности других участников соответствующих процедур и процессов. Также одной из задач политики безопасности является защита не только информации и информационных систем, но и защита самих пользователей (сотрудников предприятия и его клиентов и контрагентов).

Политика информационной безопасности на этом уровне может определять и описывать:

– собственно, решение об осуществлении целенаправленной систематической деятельности по обеспечению информационной безопасности предприятия;

– перечень основных информационных ресурсов, таких как информационные системы, массивы данных, информация об отдельных фактах и явлениях (конструкторских разработках, коммерческих сделках, результатах НИОКР и т.п.), защита которых имеет наибольший приоритет для всего предприятия;

– общий подход к распределению ответственности за обеспечение информационной безопасности внутри организации;

– указание на необходимость для всего персонала соблюдать определенные меры предосторожности при работе с информацией и информационными системами, повышать свою квалификацию в данной области и осознавать меру ответственности за возможные нарушения;

– отношение руководства предприятия к фактам нарушения требований по обеспечению информационной безопасности и лицам, совершающим такие нарушения, а также общий подход к их преследованию в случае выявления таких фактов.

Задания

На лабораторном занятии необходимо:

1) дать описание организации политики информационной безопасности для конкретного предприятия, закреплённого за каждым студентом согласно порядковому номеру в списке преподавателя (см. приложение Б).

Отчет раздела политики ИБ «1. Общие положения» должен включать следующие главы:

1. Назначение политики информационной безопасности.
2. Основные принципы обеспечения ИБ.
3. Соответствие ПБ действующему законодательству.
4. Ответственность за реализацию политик информационной безопасности.
5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе.
6. Защищаемые информационные ресурсы Организации.

Для описания раздела политики ИБ «1. Общие положения» конкретного предприятия использовать характеристики организаций, приложение Б и шаблон политики ИБ, приложение В.

2) Оформить отчёт.

3) Ответить на контрольные вопросы.

4) Сделать вывод.

Контрольные вопросы:

1. Кто утверждает все оформленные решения, формирующие ПБ?
2. Кто несёт ответственность обеспечения защиты информации?
3. Перечислите категории информационных ресурсов, подлежащих защите в Организации?
4. Кто несет ответственность за сохранность персональных данных сотрудника организации?

Список литературы

Перечень основной литературы:

1 Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 c.— Режим доступа: http://www.iprbookshop.ru/52182.— ЭБС «IPRbooks», по паролю.

2. Бирюков А.Н. Процессы управления информационными технологиями [Электронный ресурс]/ Бирюков А.Н.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 263 c.— Режим доступа: http://www.iprbookshop.ru/52165.— ЭБС «IPRbooks», по паролю.

Перечень дополнительной литературы:

1 Булгакова, С.В. Управленческий учет : учебник для бакалавров / С.В. Булгакова ; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский государственный университет», Министерство образования и науки РФ. - Воронеж : Издательский дом ВГУ, 2015. - 370 с. - Библиогр.: с. 357-364. - ISBN 978-5-9273-2193-3 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=441585.

2. Гринберг, А.С. Документационное обеспечение управления: учебник / А.С. Гринберг, Н.Н. Горбачёв, О.А. Мухаметшина. - Москва : Юнити-Дана, 2015. - 391 с. : табл., граф., ил., схемы - Библиогр.: с. 382-383. - ISBN 978-5-238-01770-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=115031.

Интернет-ресурсы:

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
для студентов направления подготовки **09.03.02 Информационные системы и технологии**
направленность (профиль) **Информационные системы и технологии обработки цифрового контента**

Пятигорск, 2022

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– написание докладов;

– подготовка к семинарам, практическим и лабораторным работам, их оформление;

– составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

– выполнение учебно-исследовательских работ, проектная деятельность;

– подготовка лабораторных разработок и рекомендаций по решению проблемной ситуации;

– выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

– компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

– выполнение курсовых работ (проектов) в рамках дисциплин;

– выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

● подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);

● основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);

● заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Информационная безопасность» направлена на формирование следующих **компетенций**:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и лабораторных умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на лабораторных и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (астр.)		
			СРС	Контактная работа с преподавателем	Всего
ОПК-3 (ИД-1$_{ОПК-3}$ИД-2$_{ОПК-3}$ ИД-3$_{ОПК-3}$)	Самостоятельное изучение литературы и источников	Собеседование	75,78	8,42	84,2
ОПК-3 (ИД-1$_{ОПК-3}$ИД-2$_{ОПК-3}$ ИД-3$_{ОПК-3}$)	Подготовка к лабораторным занятиям	Защита ПР	1,62	0,18	1,8
ОПК-3 (ИД-1$_{ОПК-3}$ИД-2$_{ОПК-3}$ ИД-3$_{ОПК-3}$)	Написание реферата/доклада	Защита доклада	9	1	10
		Итого	86,4	9,6	96

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;

2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на лабораторных занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладовов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направление для дальнейшего совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т, п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки

а студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласовать с преподавателем.

Доклад должен быть написан грамотным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

● Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.

● Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

● Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

● Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

● Приложение (при необходимости).

Требования к оформлению:

● текст с одной стороны листа;
● шрифт Times New Roman;
● кегль шрифта 14;
● межстрочное расстояние 1,5;
● поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
● доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на лабораторных занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

• соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности в содержании доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Рейтинговая оценка знаний не предусмотрена

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая лабораторная работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение публично представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен, допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с проектом.	Технические средства и информационные технологии освоены и использованы для реализации проекта полностью	Студент проявил инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационные способности.	Проект представлен полностью и в срок.
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующими и информационными технологиями	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь отдельные не существенные	Проект не сдан.

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.		поручения в групповом проекте.	

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению лабораторных задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1. Галатенко В.А. Информационная безопасность [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 c. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограниченно

2. Нестеров С.А. Информационная безопасность [Электронный ресурс]: учебное пособие/ Нестеров С.А.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014.— 322 c.- Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-87623-969-3, экземпляров неограниченно

Дополнительная литература:

1. Фаронов А.Е. Информационная безопасность при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 c. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-9500999-7-7, экземпляров неограниченно

2. Защита информации в операционных системах: учеб.пособие.- Ставрополь: Изд-во СГУ, 2015.- 318 с - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-91359-219-4, экземпляров неограниченно

Методическая литература:

1. Методические рекомендации по выполнению лабораторных работ по дисциплине "Информационная безопасность"

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине "Информационная безопасность"

Интернет-ресурсы:

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Цифровая грамотность и обработка больших данных»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022