МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
2017 г.

Система анализа рисков и проверки политики информационной безопасности предприятия

Методические указания по выполнению лабораторной работы

Курск 2017

УДК 621.(076.1)

Составители: В.В. Карасовский, О.А. Демченко

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *А.Г. Спеваков*

Система анализа рисков и проверки политики информационной безопасности предприятия: методические указания по выполнению лабораторной работы» / Юго-Зап. гос. ун-т; сост.: В.В. Карасовский, О.А. Демченко. Курск, 2017.- 9 с.: ил.1, табл.: 1 ,Библиогр.: с. 8.

Содержат сведения об администрирование и управление программно-аппаратными средствами контроля и фильтрации сетевых пакетов способах, а так же защиты от несанкционированного доступа к ресурсам персонального компьютера. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Предназначены для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Изучение процесса создания политики информационной безопасности, ознакомление с методикой анализа рисков и международным стандартом ISO 17799.

.

2. ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ:

Организационные методы защиты информации, как правило, используются для парирования угроз. Кроме того, организационные методы используются в любой системе защиты без исключений.

В Российской Федерации вопросы информационной безопасности нашли отражение в «Концепции национальной безопасности Российской Федерации», утвержденной Указом Президента РФ № 1300 от 17 декабря 1997 года. В этом документе отмечается, что «в современных условиях всеобщей информатизации и развития информационных технологий резко возрастает значение обеспечения национальной безопасности РФ в информационной сфере».

В законе «Об информации, информатизации и защите информации» даны определения основных терминов: информация; информатизация; информационные системы; информационные ресурсы; конфиденциальная информация; собственник и владелец информационных ресурсов; пользователь информации. Государство гарантирует права владельца информации, независимо от форм собственности, распоряжаться ею в пределах, установленных законом.

Другим важным правовым документом, регламентирующим вопросы защиты информации в КС, является закон РФ «О государственной тайне». Закон определяет уровни секретности государственной информации (грифы секретности) и соответствующую степень важности информации. Руководствуясь данным законом и «Перечнем сведений, отнесенных к государственной тайне», соответствующие государственные служащие устанавливают гриф секретности информации.

Выработку политики информационной безопасности, подготовку законодательных актов и нормативных документов, контроль над выполнением установленных норм обеспечения безопасности информации осуществляют государственные органы (рис. 1)

Рис. 1 – Структура государственных органов

Возглавляет государственные органы обеспечения информационной безопасности Президент РФ. Он руководит Советом Безопасности и утверждает указы, касающиеся обеспечения безопасности информации в государстве.

Общее руководство системой информационной безопасности, наряду с другими вопросами государственной безопасности страны, осуществляют Президент и Правительство Российской Федерации.

Органом исполнительной власти, непосредственно занимающимся вопросами государственной безопасности, является Совет Безопасности при Президенте РФ. В состав Совета Безопасности входит Межведомственная комиссия по информационной безопасности. Комиссия готовит указы Президента, выступает с законодательной инициативой, координирует деятельность руководителей министерств и ведомств в области информационной безопасности государства.

Рабочим органом Межведомственной комиссии по информационной безопасности является Государственная техническая комиссия при Президенте РФ.

Информационная безопасность достигается проведением руководством соответствующего уровня политики информационной безопасности. Основным документом, на основе которого проводится политика информационной безопасности, является программа информационной безопасности. Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления государством, ведомством, организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в КС. В программах информационной безопасности содержатся также общие требования и принципы построения систем защиты информации в КС.

3. ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

Провести анализ рисков и проверку политики информационной безопасности с помощью программного комплекса Office 2005 Demo(ГРИФ, КОНДОР). В ходе выполнения лабораторной работы разработать политику информационной безопасности и анализировать риски предприятия.

Варианты: (указывается количество вводимых данных, сами данные пользователь выбирает сам), ресурсов 3, отдел 1

Таблица 1 – Варианты заданий

Вариант	**Вид информации**	**Группы пользователей**	**Каналы связи**	**Бизнес-процессы**	**Средства защиты**	**Средства защиты информации**
1	2	3	1	2	7-8	3-4
2	3	2	1	2	7-8	3-4
3	4	3	1	2	7-8	3-4
4	2	3	1	2	7-8	3-4
5	3	2	1	2	7-8	3-4
6	4	3	1	2	7-8	3-4
7	2	3	1	2	7-8	3-4
8	3	2	1	2	7-8	3-4
9	4	3	1	2	7-8	3-4
10	2	3	1	2	7-8	3-4
11	3	2	1	2	7-8	3-4
12	4	2	1	2	7-8	3-4
13	2	2	1	2	7-8	3-4
14	3	2	1	2	7-8	3-4
15	4	3	1	2	7-8	3-4
16	2	2	1	2	7-8	3-4
17	3	2	1	2	7-8	3-4
18	4	3	1	2	7-8	3-4
19	2	2	1	2	7-8	3-4
20	3	2	1	2	7-8	3-4
21	4	3	1	2	7-8	3-4
22	2	2	1	2	7-8	3-4
23	3	2	1	2	7-8	3-4

24	4	3	1	2	7-8	3-4
25	2	2	1	2	7-8	3-4

По результатам выполнения составить отчет ГРИФ, потом открыть данный проект в программе КОНДОР и составить отчет по организационным мерам и политике доступа.

4. ТРЕБОВАНИЯ К ОТЧЕТУ

1. Титульный лист
2. Цель работы
3. Краткая теория по лабораторной работе
4. Задание
5. Ход выполнения работы
6. Выводы по работе

5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое политика информационной безопасности?
2. Какие организационные меры защиты существуют?
3. Назначение организационных мер?
4. Какие из них наиболее эффективны? Почему?
5. Перечислите основные нормативные документы, регламентирующие ИБ в России
6. Какой состав и организационная структура системы обеспечения информационной безопасности?
7. В чем заключается стандарт ISO 17799?
8. Опишите методику анализа рисков.

6. БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. М.: Энергоиздат, 1994. Кн. 1-2.
2. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты

информации от НСД в автоматизированных системах и средствах вычислительной техники. - Москва, 1992.

3. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. - Москва, 1992.

4. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - Москва, 1992.

5. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. - Москва, 1992.

6. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. - Москва, 1992.

7. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.-М., Яхтсмен, 1996.

8. И.Н. Анисимова, Е.В. Стельмашонок. Защита информации.: Учебное пособие - СПб, СпбГИЭУ, 2002.