Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

Рассмотрено
цикловой комиссией
Протокол заседания № 1
от «31» августа 2020 г.
Председатель цикловой комиссии
_____/ Чобану Л.А./

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
учебной дисциплины
ОП. 04 Основы информационной безопасности
по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
квалификация
техник по защите информации

Разработчик:
преподаватель
ОГАПОУ «Белгородский индустриальный колледж»
Петрушин С.Д.

Белгород 2020 г.

Содержание

1. Пояснительная записка

1.1. Краткая характеристика дисциплины, ее цели и задачи. Место лабораторных работ в курсе дисциплины

Дисциплина ОП. 04 «Основы информационной безопасности» является частью рабочей основной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности

телекоммуникационных систем

Дисциплина изучается в IV семестре. В целом рабочей программой предусмотрено 18 часов на выполнение лабораторных работ, что составляет 23 % от обязательной аудиторной нагрузки, которая составляет 78 часа.

Цель настоящих методических рекомендаций: оказание помощи обучающимся в выполнении лабораторных работ по дисциплине ОП. 04 Основы информационной безопасности», качественное выполнение которых поможет обучающимся освоить обязательный минимум содержания дисциплины и подготовиться к промежуточной аттестации в форме дифференцированного зачета.

1.2. Организация и порядок проведения лабораторных работ

Лабораторные работы проводятся после изучения теоретического материала. Введение лабораторных работ в учебный процесс служит связующим звеном между теорией и практикой. Они необходимы для закрепления теоретических знаний, а также для получения практических навыков и умений. При проведении лабораторных работ задания, выполняются студентом самостоятельно, с применением знаний и умений, усвоенных на предыдущих занятиях, а также с использованием необходимых пояснений, полученных от преподавателя. Обучающиеся должны иметь методические рекомендации по выполнению лабораторных работ, конспекты лекций, измерительные и чертежные инструменты, средство для вычислений.

1.3. Общие указания по выполнению лабораторных работ

Курс лабораторных работ по дисциплине ОП. 04 «Основы информационной безопасности»предусматривает проведение 9 работ, посвященных изучению:

- определению объектов защиты на типовом объекте информатизации;
- классификации защищаемой информации по видам тайны и степеням конфиденциальности;
- определению угроз объекта информатизации и их классификация;
- работе в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.

Выбор мер защиты информации для автоматизированного рабочего места

При подготовке к проведению лабораторной работы необходимо:

• ознакомиться с лабораторным оборудованием;

• ознакомиться с порядком выполнения работы.

После выполнения лабораторной работы обучающийся к следующему занятию оформляет отчет, который должен содержать:

• название лабораторной работы, ее цель;

• краткие, общие сведения об изучаемом лабораторном оборудовании;

• необходимый графический материал, указанный преподавателем при выполнении лабораторной работы (принципиальная схема лабораторной установки, графики);

• данные, полученные непосредственно из проводимых опытов;

• результаты обработки данных опытов с необходимыми пояснениями;

• графический материал, отображающий полученные в ходе опытов значения измеряемых величин;

• оценку результатов испытаний.

При работе в лаборатории необходимо руководствоваться инструкциями по технике безопасности, учитывающими все специфические особенности лаборатории.

В лаборатории нельзя находиться в отсутствие преподавателя или лица, ответственного за технику безопасности.

При нахождении в лаборатории следует находиться в рабочей зоне, указанной преподавателем. С самого начала необходимо убедиться в том, что испытательный стенд находится в полностью обесточенном (отключенном) состоянии.

Перед выполнением лабораторной работы необходимо получить вводные инструкции преподавателя и внимательно ознакомиться с описанием лабораторного стенда и оборудованием.

Внимание! Включать лабораторные установки и выполнять какие-либо действия с приборами допускается ТОЛЬКО с разрешения преподавателя!

При обнаружении признаков неисправности, таких как: появление искрения, дыма, специфического запаха, следует немедленно отключить все источники электроэнергии и сообщить о случившемся преподавателю.

При возникновении реальной опасности травматизма для одного или нескольких присутствующих, участники испытания должны произвести срочное отключение лаборатории от всех источников электроэнергии выключением вводного автомата. Лаборатории должны иметь средства пожаротушения и оказания первой медицинской помощи. На первом занятии изучаются правила техники безопасности и проводится вводный инструктаж с последующей проверкой его усвоения, о чем свидетельствует запись в журнале по технике безопасности кабинета/лаборатории, подписываемый преподавателем, проводившем инструктаж, и всеми обучающимися.

1.4. Критерии оценки результатов выполнения лабораторных работ

Критериями оценки результатов работы обучающихся являются:

– уровень усвоения обучающимся учебного материала;

– умение обучающегося использовать теоретические знания при выполнении практических задач;

– сформированность общеучебных и профессиональных компетенций:

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей;

ОК 09. Использовать информационные технологии в профессиональной деятельности;

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках;

ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями;

– обоснованность и четкость изложения материала;

– уровень оформления работы.

– анализ результатов.

Критерии оценивания лабораторной работы

Оценка	**Критерии оценивания**
5	Работа выполнена в полном объеме с соблюдением необходимой последовательности проведения, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом, формулирует собственные, самостоятельные, обоснованные, представляет полные и развернутые ответы на дополнительные вопросы.
4	Работа выполнена в полном объеме с соблюдением необходимой последовательности проведения, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом, допуская незначительные ошибки на дополнительные вопросы.
3	Работа выполнена в полном объеме, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом на минимально допустимом уровне, допуская ошибки на дополнительные вопросы.
2	Работа выполнена не полностью. Студент практически не владеет теоретическим материалом, допускает ошибки при ответе на дополнительные вопросы.

2. Тематическое планирование лабораторных работ

	Наименование тем	Вид и название работы студента	Количество часов на выполнение работы
Раздел 1	**Теоретические основы информационной безопасности**		**10**
1.2	**Основы защиты информации**	**Лабораторная работа №1 «**Определение объектов защиты на типовом объекте информатизации.»	2
		Лабораторная работа №2-3 «Классификация защищаемой информации по видам тайны и степеням конфиденциальности.»	4
1.3	**Угрозы безопасности защищаемой информации.**	**Лабораторная работа №4-5** «Определение угроз объекта информатизации и их классификация.»	4
Раздел 2	**Методология защиты информации**		8
2.2	**Нормативно правовое регулирование защиты информации**	**Лабораторная работа №6-7** «Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.»	4
2.3	**Защита информации в автоматизированных (информационных) системах**	**Лабораторная работа №8-9** «Выбор мер защиты информации для автоматизированного рабочего места.»	4
		Итого:	**18**

3. Содержание лабораторных работ

Лабораторная работа №1

Тема: «Определение объектов защиты на типовом объекте информатизации.»

Цель: определить объекты защиты на типовом объекте информатизации.

Теоретические вопросы

1. Теория защиты информации.
2. Обеспечение информационной безопасности и направления защиты.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная).
4. Требования к системе защиты информации.
5. Общая модель воздействия на информацию.
6. Общая модель процесса нарушения физической целостности информации.
7. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.

Задание 1. Описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды угроз.
2. Характер происхождения угроз.
3. Классы каналов несанкционированного получения информации.
4. Источники появления угроз.
5. Причины нарушения целостности информации.
6. Потенциально возможные злоумышленные действия.
7. Определить класс защиты информации.

Наименование объекта защиты информации

1. Одиночно стоящий компьютер в бухгалтерии.
2. Сервер в бухгалтерии.
3. Почтовый сервер.
4. Веб-сервер.
5. Компьютерная сеть материальной группы.
6. Одноранговая локальная сеть без выхода в Интернет.
7. Одноранговая локальная сеть с выходом в Интернет.
8. Сеть с выделенным сервером без выхода в Интернет.
9. Сеть с выделенным сервером с выходом в Интернет.
10. Телефонная база данных (содержащая информацию ограниченного пользования) в твердой копии и на электронных носителях.
11. Телефонная сеть.
12. Средства телекоммуникации (радиотелефоны, мобильные телефоны, пейджеры).
13. Банковские операции (внесение денег на счет и снятие).
14. Операции с банковскими пластиковыми карточками.
15. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
16. Компьютер, хранящий конфиденциальную информацию о разработках предприятия.

17. Материалы для служебного пользования на твердых носителях в производстве.

18. Материалы для служебного пользования на твердых носителях на закрытом предприятии.

19. Материалы для служебного пользования на твердых носителях в архиве.

20. Материалы для служебного пользования на твердых носителях в налоговой инспекции.

21. Комната для переговоров по сделкам на охраняемой территории.

22. Комната для переговоров по сделкам на неохраняемой территории.

23. Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).

24. Судебные материалы (твердая копия).

25. Паспортный стол РОВД.

26. Материалы по владельцам автомобилей (твердая копия, фотографии, электронные носители и др.).

27. Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.).

28. Сведения по тоталитарным сектам и другим общественно-вредным организациям.

29. Сведения по общественно-полезным организациям (красный крест и др.).

30. Партийные списки и руководящие документы.

Задание 2. Необходимо предложить анализ увеличения защищенности объекта защиты информации на типовом объекте информатизации по следующим разделам:

1. Определить требования к защите информации.
2. Классифицировать автоматизированную систему.
3. Определить факторы, влияющие на требуемый уровень защиты информации.
4. Выбрать или разработать способы и средства защиты информации.
5. Построить архитектуру систем защиты информации.
6. Сформулировать рекомендации по увеличению уровня защищенности.

Лабораторная работа №2-3

Тема: «Классификация защищаемой информации по видам тайны и степеням конфиденциальности»

Цель: проведение классификации защищаемой информации по видам тайны и степеням конфиденциальности.

Теоретические вопросы

1. Виды защищаемой информации.
2. Виды конфиденциальной информации.
3. Какая информация относится к государственной тайне?
4. Порядок занесения сведений к государственной тайне.
5. Какая информация относится к профессиональной тайне?
6. Какие сведения относятся к персональным данным?
7. Какие сведения не относятся к коммерческой тайне?
8. Принципы засекречивания данных.

Задание 1. Найти и изучить текст документа «Доктрина информационной безопасности». Заполнить таблицы.

Таблица 1. Классификация национальных интересов в информационной сфере по принадлежности интересов

Национальные интересы в информационной сфере		
Интересы личности	Интересы общества	Интересы государства
(содержание)	(содержание)	(содержание)

Таблица 2. Классификация национальных интересов в информационной сфере по важности интересов

Национальные интересы в информационной сфере			
Соблюдение конституционных прав и свобод, ...	Информационное обеспечение государственной политики РФ.	Найти самостоятельно	Найти самостоятельно
(содержание)	(содержание)	(содержание)	(содержание)

- коммерческую тайну предприятия;
- служебную информацию ограниченного распространения, обладателем которой является предприятие.

Лабораторная работа №4-5

Тема: «Определение угроз объекта информатизации и их классификация»

Цель: определение угроз объекта информатизации и их классификация. ***Теоретические вопросы***

1. Понятие угрозы безопасности информации.
2. Системная классификация угроз безопасности информации.
3. Угрозы информационной безопасности РФ.
4. Источники угроз информационной безопасности РФ.
5. Содержание угроз информационной безопасности РФ.
6. Каналы и методы несанкционированного доступа к информации
7. Уязвимости. Методы оценки уязвимости информации

Задание 1. Найти и изучить текст документа «Доктрина информационной безопасности». Заполнить таблицы.

Таблица 1. Классификация угроз информационной безопасности РФ по общей направленности

Угрозы информационной безопасности РФ			
Угрозы конституционным правам и свободам, общественному сознанию личности	Угрозы информационному обеспечению государственной политики	Угрозы развитию Отечества	Угрозы безопасности информационных и телекоммуникационных средств и систем
(содержание)	(содержание)	(содержание)	(содержание)

Таблица 2. Источники угроз информационной безопасности

Источники угроз информационной безопасности	
Внешние источники	Внутренние источники
(содержание)	(содержание)

Задание 2. Составить перечень угроз для заданного объекта информатизации. Заполнить таблицу.

Таблица 1 . Перечень угроз

Номер угрозы	Источник угрозы	Среда распространения	Носитель информации

Задание 3. Провести анализ потенциальных каналов утечки на указанном объекте. Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения по образцу таблицы 1.

Таблица 1. Перечень потенциальных каналов утечки информации

Каналы утечки информации с объекта защиты			Место расположения
	Оптический канал	Окно со стороны проспекта	каб. № 1
		Окно со стороны проспекта	каб. № 2
		Окно со стороны проспекта	каб. № 3
	Радиоэлектронный канал	Стоянка автотранспорта на просп.	указать
		Система часофикации	указать
		Телефон	указать
		Розетки	указать
		ПК	указать
		Воздушная линия электропередачи	указать
		Система оповещения	указать
		Система пожарной сигнализации	указать
	Акустический канал	Теплопровод подземный	указать
		Водопровод подземный	указать
		Стены помещения	указать
		Батареи	указать
		Окна контролируемого помещения	указать
	Материально-вещественный канал	Документы на бумажных носителях	указать
		Персонал предприятия	указать
		Производственные отходы	указать

Задание 3. Построить модель угроз и комплексную модель каналов утечки информации для заданного объекта. Заполнить таблицы.

Таблица 1. Модель угроз защищаемого объекта

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы

Таблица 2. Комплексная модель каналов утечки

№ п/п	Цена информации	Источник сигнала	Путь утечки	Вид канала	Оценка реальности	Величина угрозы/ранг

Лабораторная работа №6-7

Тема: «**РАБОТА В СПРАВОЧНО-ПРАВОВОЙ СИСТЕМЕ С НОРМАТИВНЫМИ И ПРАВОВЫМИ ДОКУМЕНТАМИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Цель: научиться работать в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.

Теоретические вопросы

1. Законодательные акты в области защиты информации.
2. Российские и международные стандарты, определяющие требования к защите информации.
3. Система сертификации РФ в области защиты информации.
4. Основные правила и документы системы сертификации РФ в области защиты информации. ***Задание 1.*** Изучить основные положения ФЗ «Об информации, информационных технологиях

и защите информации».

Найти ответы на следующие вопросы:

1. Какие отношения в информационной сфере регулируются ФЗ «Об информации, информационных технологиях и защите информации».
2. На каких принципах основывается регулирование отношений в информационной сфере.
3. На какие виды подразделяется информация по категориям доступа:

1) _____ ;
2) _____ .

4. На какие виды подразделяется информация в зависимости от порядка предоставления?

1) _____ ;
2) _____ ;
3) _____ ;
4) _____ .

5. Какие права имеет обладатель информации?

1) _____ ;
2) _____ ;
3) _____ ;
4) _____ ;
5) _____ .

6. Каковы обязанности обладателя информации?

1) _____ ;
2) _____ ;
3) _____ .

7. К какой информации не может быть ограничен доступ?

1) _____ ;
2) _____ ;
3) _____ ;
4) _____ .

8. Какие требования по защите информации в информационной системе должны быть

обеспечены?

1)_____ ;
2)_____ ;
3) _____ ;
4) _____ ;
5) _____ ;
6) _____ .

9. Может ли государственный орган отказать гражданину в предоставлении информации, непосредственно затрагивающей его права и свободы?

Задание 2. Изучить часть 4 Гражданского кодекса РФ. Дать развернутый ответ на поставленные вопросы. Необходимо обосновать свой ответ, указав наименование соответствующего нормативного документа, его статью и пункт статьи, на которые следует опираться.

Задача 1

Гражданин Иванов предложил гражданам Шаталову и Моисееву идею создания информационно-справочной системы «Альбомы рок-музыкантов» в среде программирования Delphi 6.0, лицензионная версия которой была приобретена Моисеевым. Граждане Шаталов и Моисеев создали такую систему и зарегистрировали свое авторство на нее без участия гражданина Иванова. Имеет ли место в данной ситуации нарушение авторского права гражданина Иванова?

Задача 2

Гражданин Алексеев создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием - «Alex 3D» и зарегистрировал на него свои права. 20.09.2006 этот гражданин заключил договор с компанией «Moscow Technology и передал свои имущественные права на распространение своего программного продукта сроком на один год (т.е. до 19.09.2007). После заключения договора компания «Moscow Technology» распространила версию

программы "Alex 3D" с предварительной модификацией данного программного продукта без ведома автора. Имеет ли место в данной ситуации нарушение авторского права гражданина Алексеева?

Задача 3

Гражданин Серебренников разработал в соавторстве с гражданином Семеновым информационно-справочную систему «Энциклопедия. Животные Крайнего севера». Финансовую поддержку программных разработок вышеупомянутым гражданам оказал гражданин Андреев. Граждане Серебренников и Семенов 13.05.06 оформили свое авторство на данную информационную систему. В марте 2006 г. данный программный продукт был выпущен под авторством гражданина Андреева. Имеет ли место в данной ситуации нарушение авторского права граждан Серебренникова и Семенова?

Задача 4

Будет ли удовлетворен судебный иск студента Максимкина к студенту Федорову в том, что последний нарушил авторское право, выдавая идею Максимкина получить более

эффективный алгоритм сортировки массива на основе линейной и пузырьковой сортировки за свою?

Задача 5

Гражданин В. А. Мельников, автор и правообладатель электронной энциклопедии «Вокруг света», планировал сотрудничать с компанией «Видеотех», занимающейся тиражированием программных продуктов. Экземпляр электронной энциклопедии был передан в компанию для ознакомления. При этом договор о передаче компании «Видеотех» имущественных прав на программу составлен не был. В. А. Мельников предъявил судебный иск к компании «Видеотех», которая осуществила выпуск данного программного продукта. Какое решение вынесет суд и почему?

Задача 6

Гражданин М. А. Петров, автор и правообладатель информационно-справочной системы «Энциклопедия. Легковые автомобили от А до Я», 19.04.2007 подписал договор с компанией «Мир программ» о передаче имущественного права на выпуск своей системы. Первые экземпляры программы должны были поступить в продажу не раньше 17.06.2007. Однако 25.05.2007 года гражданин Петров обнаружил экземпляры своего программного продукта в одном из ларьков. Имеется ли несоответствие, связанное с нарушением информационной безопасности?

Задача 7

Гражданин П. А. Сергеев зарегистрировал созданную им информационную систему «Растения Омской области» под своим именем 17.05.2007. Его авторское право на созданную им информационную систему будет действовать до 17.05.2057. Имеется ли несоответствие, связанное с нарушением информационной безопасности?

Задача 8

Гражданка И. П. Лукашина решила зарегистрировать свое авторское право на созданную ею базу данных и осуществила это следующим образом: © 2006 Лукашина Ирина. Имеется ли несоответствие, связанное с нарушением информационной безопасности?

Задача 9

Гражданин В. П. Чумаков зарегистрировал свое авторское право на созданную им операционную систему «New System». Однако гражданину Чумакову не принадлежит право модификации созданного им программного продукта. Имеется ли несоответствие, связанное с нарушением информационной безопасности?

Задание 3. Изучить содержания ст. 272, 273, 274 УК РФ. Дать развернутый ответ на поставленные вопросы. Необходимо обосновать свой ответ, указав наименование соответствующего нормативного документа, его статью и пункт статьи, на которые следует опираться.

Задача 1

Бывший сотрудник химико-биологического предприятия вместе со своим приятелем-программистом скопировали конфиденциальную информацию: состав ингредиентов, их

пропорции и формулу нового лекарственного препарата - с целью продажи этой информации конкурирующей организации. Можно ли квалифицировать действия лица (группы

лиц) в описанной ситуации как противоправные?

Задача 2

П.П. Андреев, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (файлы с расширением *.exe. В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб размере 750 000 рублей. Можно ли квалифицировать действия лица (группы лиц) в описанной ситуации как противоправные?

Задача 3

Сотрудник Научно-исследовательского института приборостроения скопировал схемы, чертежи и графики прибора с целью продажи этой информации зарубежной фирме-производителю. Можно ли квалифицировать действия лица (группы лиц) в описанной ситуации как противоправные?

Задача 4

Решение в пользу какой стороны и почему вынесет суд при предъявлении владельцем фирмы «Электронная галерея» И. С. Дубцовым судебного иска к продавцу этой же фирмы, если по вине последнего произошло электрическое замыкание и было повреждено значительное количество компьютерной техники?

Задача 5

Будет ли привлечена к уголовной ответственности главный бухгалтер, торговой сети «Оптпром» С.Н. Вульф, если ее действия повлекли уничтожение компьютерной информации в базах данных вышеуказанной торговой сети и после ревизии предприятие было оштрафовано на 350 000 рублей?

Задача 6

Будет ли удовлетворен иск компании «Интермедиа» о привлечении к уголовной в ответственности гражданина Р.И. Сизова и выплате им фирме денежной компенсации, если он внедрил в компьютерную сеть компании программу, действие которой заключается в уничтожении исполняемых файлов в какой-либо компьютерной сети. Функционирование данной программы принесло убытки различным организациям на общую сумму 670 000 рублей.

Задача 7

За несанкционированный доступ и копирование компьютерной информации суд приговорил гражданина РФ В. А. Лютикова к 5 годам лишения свободы. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 8

Студентам технического университета за доступ к компьютерной системе службы внутренних дел и копирование части файлов данной системы было предъявлено обвинение по ст. 272, п. 1 УК РФ. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 9

Н. А. Симонова, сотрудница отдела продаж косметической компании «Макияж», за распитие кофейного напитка в непосредственной близости от ЭВМ была наказана исправительными работами сроком на 15 суток. Найдите и исправьте несоответствие в

предложенной ситуации, если оно имеет место.

Задача 10

Оператор ПК торговой сети «Вернисаж» Д. С. Ермилов был обвинен по ст. 272, п. 1 УК РФ за изменение данных в поле «Адрес» в базе данных клиентских платежей. Эту модификацию он произвел по просьбе самой клиентки в связи с изменением ее места жительства. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 11

За распространение программы, действие которой заключается в уничтожении текстовых файлов в какой-либо компьютерной сети, студент III курса авиационного техникума был наказан судом штрафом в размере 100 минимальных размеров оплаты труда. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 12

За несанкционированный доступ к компьютерной информации в файлах химико-биологического исследовательского центра «New Life» и ее модификацию гражданку РФ А. С. Иванову суд приговорил к 8 месяцам исправительных работ. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 13

За нарушение работы с компьютерной системой бухгалтерских платежей авиакомпании «Небеса» сотруднице вышеупомянутой организации Т. В. Бариновой, действия которой привели к модификации компьютерных данных и принесли авиакомпании «Сибирь» денежные убытки в размере 150 000 рублей, было предъявлено обвинение по ст. 274 УК РФ. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Лабораторная работа №8-9

Тема: «Выбор мер защиты информации для автоматизированного рабочего места»

Цель: выбор мер защиты информации для автоматизированного рабочего места.

Теоретические вопросы

1. Основные механизмы защиты информации.
2. Система защиты информации.
3. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.
4. Программные и программно-аппаратные средства защиты информации.
5. Инженерная защита и техническая охрана объектов информатизации.
6. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.

Задание 1. Построить функциональную структуру СФЗ заданного объекта. Разработать модель мероприятий физической защиты объекта в соответствии с моделями угроз и каналов утечки информации на заданном объекте.

В процессе организационных мероприятий необходимо определить:

а) контролируемую зону (зоны);

б) выделить из эксплуатируемых технических средств технические средства, используемые для передачи, обработки и хранения конфиденциальной информации (ОТСС);

в) выявить в контролируемой зоне (зонах) вспомогательные технические средства и системы (ВТСС).

Задание 2. Составить план организационно-технических мероприятий по образцу таблицы 1.

Таблица 1. План организационно-технических мероприятий

№ п\п	Демаскирующий признак	Мероприятия по уменьшению (ослаблению) демаскирующих признаков
I. Организационные мероприятия		
1	Прибытие сотрудников на службу в форменной одежде	1. Прибытие сотрудников на службу в форменной одежде другого ведомства. 2. Проведение совещаний и переподготовки сотрудников других ведомств
2	Перемещение сотрудников	1. Разграничение доступа сотрудников в различные помещения. 2. Организация пропускного режима
3	Готовая продукция	1. Разграничение доступа сотрудников в склад при вывозе продукции за пределы предприятия
4	Отходы производства	1. Сбор и утилизация отходов производства. 2. Уничтожение отходов делопроизводства
II. Технические мероприятия		

1	Излучение ПЭВМ	1. Организация работы системы зашумления. 2. Установка в ПЭВМ генераторов зашумления. 3. Персонификация доступа в систему. 4. Программная защита системы ПЭВМ. 5. Плановые (внеплановые) проверки ПЭВМ
2	Телефонная связь	1. Организация работы внутренней АТС. 2. Запись переговоров сотрудников по телефонам. 3. Закрытие каналов связи
3	Строительные конструкции здания	1. Нанесение на стекла пленки поглощающей ИК-излучение. 2. Установка системы виброакустического зашумления стекол и строительных конструкций. 3. Специальная проверка персонала обслуживающего смежные помещения

Задание 3. Подготовить план внедрения на предприятии конфиденциального делопроизводства, используя следующую методику:

- первый этап - определение перечня сведений конфиденциального характера и документов, содержащих конфиденциальные сведения. Разделение сведений на несколько групп по степени конфиденциальности (например: строго конфиденциальные, конфиденциальные, для служебного пользования);
- второй этап - утверждение перечня сведений конфиденциального характера у руководства, а также определение порядка и сроков переутверждения данного перечня, а также снижение и снятие грифа конфиденциальности;
- третий этап - определение правил конфиденциального бумажного делопроизводства на основе общего бумажного делопроизводства;
- четвертый этап - определение порядка допуска сотрудников к сведениям конфиденциального характера;
- пятый этап - заключение договоров о нераспространении конфиденциальных сведений между сотрудниками, которые будут допущены к работе с конфиденциальной информацией и руководством организации;
- шестой этап - создание необходимых нормативных документов (инструкций, должностных обязанностей и т.д.);
- седьмой этап - доведение нормативных документов до сотрудников в рамках функциональных обязанностей;
- восьмой этап - создание механизмов контроля за соблюдением конфиденциального делопроизводства;
- девятый этап - создание механизма ответственности за нарушение правил конфиденциального делопроизводства.

Задание 4. Составить план реализации мероприятий по защите информации, учитывая критические ресурсы и информационную инфраструктуру.

К критическим ресурсам следует отнести:

-персонал;

-информационную структуру;
-физическую инфраструктуру.
К информационной инфраструктуре следует отнести:
-компьютеры;
-программы и данные;
-информационные сервисы;
-документацию.

4. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Бубнов А.А. Основы информационной безопасности [Текст]: учеб. пособие для студентов учреждений среднего проф. образования. - 3-е изд., стер. - М.: Академия, 2017. - 256 с.

2. Мельников В.П. Информационная безопасность [Текст] : Учебник / В. П. Мельников, А. И. Куприянов; Под ред.В,П. Мельникова. - 2-е изд., перераб. и доп. - М. : Академия, 2019. - 268 с.

Дополнительные источники:

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.

2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2016.

3. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М. : КНОРУС, 2016.

4. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2016.

5. Ищейнов, В.Я. Информационная безопасность и защита информации: словарь терминов и понятий: словарь / Ищейнов В.Я. — Москва: Русайнс, 2019. — 226 с. — URL: https://book.ru/book/932909 (дата обращения: 01.11.2019). — Текст : электронный.

6. Крылов, Г.О. Базовые понятия информационной безопасности: учебное пособие / Крылов Г.О., Ларионова С.Л., Никитина В.Л. — Москв : Русайнс, 2019. — 257 с. — URL: https://book.ru/book/932492 (дата обращения: 01.11.2019). — Текст: электронный.

7. Кузнецова, А.В. Искусственный интеллект и информационная безопасность общества: монография / Кузнецова А.В., Самыгин С.И., Радионов М.В. — Москва: Русайнс, 2019. — 118 с. — URL: https://book.ru/book/934089 (дата обращения: 01.11.2019). — Текст: электронный.

8. Нестеров С.А. Основы информационной безопасности. Учебное пособие. – С-Пб.: Лань. 2016.

9. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017.

10. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2019. — 227 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/80290.html (дата обращения: 05.11.2019). — Режим доступа: для авторизир. пользователей

Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

Группа 21 БТС

ЖУРНАЛ ОТЧЕТОВ
по выполнению лабораторных работ
учебной дисциплины
ОП. 04 Основы информационной безопасности
по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

ВЫПОЛНИЛ _____ /_____/

ПРИНЯЛ _____ /Рачинский С.А./

Белгород 2019 г.