МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(ДГТУ)

Методические указания

ДЛЯ ВЫПОЛНЕНИЯ КОНТРОЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

«Информационные системы в сфере экономической безопасности»
для обучающихся по направлению подготовки (специальности)
38.05.01 «Экономическая безопасность»
специализация «Экономико-правовое обеспечение экономической безопасности»

Ростов-на-Дону
ДГТУ
2018

УДК 657.9

Составитель: И.В. Золотарева

Методические указания для выполнения контрольной работы по дисциплине «Информационные системы в сфере экономической безопасности». – Ростов-на-Дону: Донской гос. техн. ун-т, 2018. – 34 с.

Содержат контрольные вопросы и задания к контрольной работе.

Предназначены для обучающихся специальности 38.05.01 «Экономическая безопасность», специализация «Экономико-правовое обеспечение экономической безопасности.

УДК 657.9

Печатается по решению редакционно-издательского совета
Донского государственного технического университета

Научный редактор д-р эк. наук, профессор Г.Е. Крохичева

Ответственный за выпуск зав. кафедрой «Экономическая безопасность, учет и право» д-р эк. наук, профессор Г.Е. Крохичева

В печать ___.___.20___ г.
Формат 60×84/16. Объем ___ усл. п. л.
Тираж ___ экз. Заказ № ___.

Издательский центр ДГТУ
Адрес университета и полиграфического предприятия:
344000, г. Ростов-на-Дону, пл. Гагарина, 1

Для студентов заочной формы обучения учебным планом предусмотрено выполнение контрольной работы.

Контрольная работа по дисциплине «Информационные системы в сфере экономической безопасности» выполняется в форме эссе.

Информационные системы в сфере экономической безопасности — неотъемлемая часть системы управления современным хозяйствующим субъектом.

Контрольная работа – это один из основных видов самостоятельной работы обучающихся и важный этап их профессиональной подготовки. Основными целями написания контрольной работы являются: расширение и углубление знаний обучающихся, выработка приемов и навыков в анализе теоретического и практического материала, а также обучение логично, правильно, ясно, последовательно и кратко излагать свои мысли в письменном виде. Обучающийся, со своей стороны, при выполнении контрольной работы должен показать умение работать с литературой, давать анализ соответствующих источников, аргументировать сделанные в работе выводы и, главное, – раскрыть выбранную тему.

Методологической основой контрольной работы должны являться законы, рекомендации и указы Президента РФ по экономическим и хозяйственным вопросам, инструктивные материалы, специальная литература, а также учетные и базисные данные, характеризующие финансово-хозяйственную деятельность предприятия.

При подготовки контрольной работы студенту необходимо обратить внимание на:

1) степень раскрытия сущности проблемы (соответствие содержания теме эссе; полнота и глубина раскрытия основных понятий проблемы; умение работать с литературой, систематизировать и структурировать материал; умение обобщать, сопоставлять различные точки

зрения по рассматриваемому вопросу, аргументировать основные положения и выводы, обобщающие авторскую позицию по поставленной проблеме);

2) соблюдение требований по оформлению (правильное оформление текста эссе, ссылок на используемые литературные источники; соблюдение требований к объему эссе; грамотность и культура изложения);

Обучающимся в процессе написания контрольной работы в форме эссе необходимо выполнить ряд требований по оформлению:

1. Титульный лист с указанием темы.

2. Текст должен быть написан грамотно в редакторе Word. Шрифт: Times New Roman, кегль – 14, интервал – полуторный. Выравнивание по ширине. Все поля по 20 см.

3. Таблицы с исходной информацией должны иметь подстрочную (внизу таблицы) ссылку на источник информации и номер страницы источника, откуда эта информация получена. Все таблицы должны быть пронумерованы и иметь названия;

4. Все части работы необходимо озаглавить, станицы – пронумеровать;

5. Работа должна заканчиваться списком использованных источников в соответствии с принятой последовательностью: законы, указы, нормативные и директивные документы, первоисточники. Специальную литературу необходимо излагать в алфавитном порядке с указанием: автора; названия литературного источника; города; издательства; года издания; страницы, содержащей использованную информацию. В конце работы (после списка использованной литературы) должен быть указан перечень привлеченных интернет-источников.

По контрольной работе проводится устный опрос (зачет контрольной работы), после которого студент приступает к сдаче промежуточной аттестации в форме зачета.

По результатам устного опроса по контрольной работе обучающемуся выставляется оценка «зачтено», или «не зачтено».

Оценка «зачтено» выставляется обучающемуся, если:

4

- обучающийся демонстрирует базовые знания, умения и навыки, примененные при выполнении контрольной работы;

- у обучающегося не имеется затруднений в использовании научно-понятийного аппарата в терминологии курса, а если затруднения имеются, то они незначительные;

- на дополнительные вопросы преподавателя обучающийся дал правильные или частично правильные ответы;

- методические рекомендации при подготовки контрольной работы выполнены в полном объеме.

Компетенция(-и) или ее (их) часть(-и) сформированы на базовом уровне.

Оценка «не зачтено» ставится обучающемуся, если:

- обучающийся имеет представление о содержании темы, но не знает основные положения (темы, раздела, закона и т.д.), к которому относится задание, не способен выполнить задание с очевидным решением, не владеет навыками в области изучаемой дисциплины;

- обучающийся не демонстрирует базовые знания, умения и навыки, необходимые для выполнения заданий контрольной работы;

- в процессе ответа по теоретическому и практическому материалу, содержащиеся в контрольной работе, допущены принципиальные ошибки при изложении материала;

- методические рекомендации при подготовки контрольной работы не выполнены в полном объеме.

Компетенция(-и) или ее (их) часть(-и) не сформированы

Номер варианта контрольной работы зависит от начальной буквы фамилии обучающегося и определяется на основе данных приведенной ниже таблицы.

Таблица – Выбор темы контрольной работы

Начальная буква фамилии студента	*Номер задания контрольной работы*	*Начальная буква фамилии студента*	*Номер задания контрольной работы*
А	1	П	15
Б	2	Р	16
В	3	С	17
Г	4	Т	18
Д	5	У	19
Е	6	Ф	20
Ж	7	Х	21
З	8	Ц	22
И	9	Ч	1
К	10	Ш	2
Л	11	Щ	3
М	12	Э	4
Н	13	Ю	5

По контрольной работе проводится устный опрос, после которого магистрант приступает к сдаче промежуточной аттестации в форме экзамена.

Экзамен проводится в устной форме. Во время экзамена, обучающемуся задается три вопроса из общего перечня контрольных вопросов для подготовки к экхзамену.

Вопросы к экзамену

1. Информационная система. Этапы развития.
2. Виды информационных систем. Элементы систем. Цели систем.
3. Свойства ИС. Процессы обеспечения работы ИС
4. Для каких целей внедряются ИС
5. Какие задачи решаются с использованием ИС
6. Анализ информационной структуры фирмы
7. Уровни управления фирмой
8. Классификация персонала по уровням управления
9. Стандарты унифицированных систем документации
10. Системы классификации и классификаторы
11. Общероссийский классификатор органов власти и управления (ОКОГУ)

12. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
13. Общероссийский классификатор форм собственности (ОКФС)
14. Общероссийский классификатор организационно-правовых форм (ОКОПФ)
15. Общероссийский классификатор информации о населении (ОКИН)
16. Общероссийский классификатор основных фондов (ОКОФ)
17. Общероссийская классификация видов экономической деятельности, продукции и услуг (ОКДП)
18. Общероссийская классификация услуг населению (ОКУН)
19. Общероссийская классификация профессий рабочих, должностей служащих и тарифных разрядов ОКПДТР
20. Общероссийский классификатор валют ОКВ
21. Общероссийский классификатор отраслей народного хозяйства (ОКОНХ)
22. Общероссийский классификатор продукции (ОКП)
23. Общероссийский классификатор единиц измерения (ОКЕИ)
24. Классификатор международных единиц измерения
25. Целевая установка при разработке локальных классификаторов . Условия информационного обеспечения
26. Построение баз данных 2 этапа
27. Комплекс технических средств, предназначенный для работы ИС
28. Формы организации технического обслуживания
29. Организационное обеспечение ИС
30. Функции организационного обеспечения ИС
31. Математическое и программное обеспечение определения
32. Средства математического обеспечения ИС
33. Программное обеспечение ИС
34. Правовое обеспечение ИС
35. Эргономическое обеспечение ИС
36. Кадровое, экономическое обеспечение ИС

37. Обеспечивающая подсистема. Состав
38. Функциональные подсистемы
39. Какими факторами определяются состав задач ИС
40. Разделение ИС по виду классификации
41. Классификация ИС по признакам
42. Классификация ИС по характеру используемой информации
43. Классификация ИС по сфере применения
44. Классификация ИС по степени автоматизации
45. Классификация по признаку структурированности решаемых задач
46. ИС создающие управленческие отчеты
47. ИС разрабатывающие возможные альтернативные решения
48. Типовые виды деятельности, определяющие функциональный признак классификации ИС
49. Функции ИС
50. Функциональные системы
51. Типы информационных систем
52. Назначения информационных систем по уровням
53. Стратегические ИС
54. Оперативные ИС
55. Архивная информация
56. Информационные системы офисной автоматизации
57. Функции информационных систем в системе офисной автоматизации
58. ИС обработки знаний
59. ИС менеджеров среднего звена
60. Управленческие ИС менеджеров среднего звена
61. Основные характеристики управленческих ИС
62. ИС поддержки принятия решений
63. Характеристики поддержки принятия решений
64. Стратегический метод и стратегическая система сходства и различия
65. Внешние факторы влияющие на выбор ИС в фирме

66. Долгосрочное планирование в ИС
67. Аналитические возможности ИС
68. Локальные ИС
69. Корпоративная ИС
70. Фактографические ИС
71. Классификация ФИС
72. Какие ИС относятся к ФИС
73. Автоматизированная ИС (АИС)
74. Автоматизированные системы обработки данных (АСОД)
75. Автоматизированные информационно-логические системы
76. Автоматизированные системы управления (АСУ)
77. Классификация ФИС по признакам
78. ФИС сбор информации, этапы
79. ФИС директивная информация
80. Учетно-отчетная информация
81. Условно-переменная и переменная информация
82. Методы сбора нерегламентированной информации ФИС
83. Обработка информации ФИС
84. Этапы развития ФИС
85. Принципы построения ФИС
86. Системный подход ФИС
87. Критерии выбора источника информации
88. Классификация предприятий по признакам
89. Функциональная структура промышленного предприятия ЭИС
90. Пространственная иерархия
91. Функциональная иерархия
92. Ситуационная иерархия
93. Информационная иерархия
94. Уровни управления предприятием
95. Объекты управления на предприятии

96. Уровни автоматизации на предприятии

97. Экономическая задача на предприятии

98. Классификация экономических задач на предприятии

99. Свойства экономических задач на предприятии

100. Факторы влияющие на эффективность решения экономической задачи

101. Разработка программного обеспечения технологических процедур

102. Виды иерархий

103. Семантические и алгоритмические связи в экономических задачах

104. Детерминированные и стохастические связи в экономических задачах

По результатам устного опроса по контрольной работе обучающемуся выставляется положительная оценка.

Оценка выставляется обучающемуся, если:

- обучающийся демонстрирует базовые знания, умения и навыки, примененные при выполнении контрольной работы;

- у обучающегося не имеется затруднений в использовании научно-понятийного аппарата в терминологии курса, а если затруднения имеются, то они незначительные;

- на дополнительные вопросы преподавателя, обучающийся дал правильные или частично правильные ответы;

- методические рекомендации при подготовки контрольной работы выполнены в полном объеме.

Компетенция(-и) или ее (их) часть(-и) сформированы на базовом уровне (уровень 1) (см. табл. 1).

Оценка «удовлетворительно» ставится обучающемуся, если:

- обучающийся имеет представление о содержании темы, но не знает основные положения (темы, раздела, закона и т.д.), к которому относится задание, не способен выполнить задание с очевидным решением, не владеет навыками в области изучаемой дисциплины;

- обучающийся не демонстрирует базовые знания, умения и навыки, необходимые для выполнения заданий контрольной работы;

- в процессе ответа по теоретическому и практическому материалу, содержащиеся в контрольной работе, допущены принципиальные ошибки при изложении материала;

- методические рекомендации при подготовки контрольной работы не выполнены в полном объеме.

Компетенция(-и) или ее (их) часть(-и) не сформированы.

Краткий конспект лекций

ТЕМА 1. Понятие информационной безопасности

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин «информационная безопасность» используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства. В Законе РФ «Об участии в международном информационном обмене» информационная безопасность (ИБ) определяется аналогичным образом - как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. В данном курсе наше внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, на каком языке (русском или каком-либо ином) она закодирована, кто или что является ее источником и какое психологическое воздействие она оказывает на людей. Поэтому термин «информационная безопасность» будет использоваться в узком смысле, так, как это принято, например, в англоязычной литературе. Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе, владельцам и пользователям информации и поддерживающей инфраструктуры. (Далее будет пояснено, что следует понимать под поддерживающей инфраструктурой.) Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности. Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов,

связанных с использованием информационных систем (ИС). Угрозы информационной безопасности - это оборотная сторона использования информационных технологий.

ТЕМА 2. Основные составляющие информационной безопасности

Информационная безопасность - многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры. Иногда в число основных составляющих ИБ включают защиту от несанкционированного копирования информации, но, по видимому, это слишком специфический аспект с сомнительными шансами на успех, поэтому далее его выделять не будем. Поясним понятия доступности, целостности и конфиденциальности. 1. Доступность - это возможность за приемлемое время получить требуемую информационную услугу. 2. Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. 3. Конфиденциальность - это защита от несанкционированного доступа к информации. Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, выделим ее как важнейший элемент информационной безопасности.

ТЕМА 3. Основные принципы обеспечения информационной безопасности

Основными принципами информационной безопасности являются: ■ обеспечение целостности и сохранности данных, т.е. надежное их хранение в неискаженном виде; ■ соблюдение конфиденциальности информации (ее недоступность для тех пользователей, которые не имеют соответствующих прав); ■ доступность информации для всех авторизованных пользователей при условии контроля за всеми процессами использования ими получаемой информации; ■ беспрепятственный доступ к информации в любой момент, когда она может понадобиться. Эти принципы невозможно реализовать без особой интегрированной системы информационной безопасности, выполняющей следующие функции: ■ выработку политики информационной безопасности; ■ анализ рисков (т.е. ситуаций, в которых может быть нарушена нормальная работа информационной системы, а также утрачены или рассекречены данные); ■ планирование мер по обеспечению информационной безопасности; ■ планирование действий в чрезвычайных ситуациях; ■ выбор технических средств обеспечения информационной безопасности. Политика информационной безопасности определяет: ■ какую информацию и от кого (чего) следует защищать; ■ кому и какая информация требуется для выполнения служебных обязанностей; ■ какая степень защиты необходима для каждого вида информации; ■ чем грозит потеря того или иного вида информации; ■ как организовать работу по защите информации. Обычно руководители организации решают, какой риск должен быть исключен, а на какой можно пойти, они же затем определяют объем и порядок финансирования работ по обеспечению выбранного уровня информационной безопасности. Идентификация угроз означает уяснение наступления из-за этого возможных негативных воздействий и последствий. Реализация угрозы может привести к раскрытию, модификации, разрушению информации или отказу в информационном обслуживании. Среди долговременных последствий реализации угрозы могут быть такие, как

потеря бизнеса, нарушение какойлибо важной тайны, гражданских прав, адекватности данных, гибель человека и т.п. Вообще надо сказать, что реализация многих угроз приводит обычно к более, чем одному воздействию. К последним следует отнести: неавторизованный доступ к локальным вычислительным сетям (ЛВС), несоответствующий доступ к ресурсам ЛВС, неавторизованную модификацию данных и программ, раскрытие данных, раскрытие трафика ЛВС, подмену трафика ЛВС и, наконец, неработоспособность ЛВС.

ТЕМА 4. Основные определения и классификация угроз

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность. Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, - злоумышленником. Потенциальные злоумышленники называются источниками угрозы. Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении). Недооценка этого фактора приводит к весьма печальным последствиям. В качестве примеров следует упомянуть кражу 16 тысяч номеров кредитных карт у компании Western Union и кражу конфиденциальной информации об участниках мирового экономического форума в Давосе. Есть и менее известные, но не менее интересные примеры, иллюстрирующие, например, незащищенность баз данных, причем, не только в финансовой сфере. В июне 2000 г. некий Келли сумел проникнуть в базу данных федерального казначейства Австралии. Злоумышленник получил доступ к конфиденциальной информации о 17 000 бизнесменов и сообщил об этом в прямом эфире радиостанции ABC. Что характерно, казначейство отказалось давать какие-либо комментарии по поводу расследования этого дела. Другой пример также показателен, потому что демонстрирует, как используется труд хакеров в политической борьбе. В

2000 г. одна из оппозиционных мексиканских партий наняла хакеров для доступа к засекреченной базе данных правящей революционной партии Мексики (PRI). В результате был получен доступ к данным аудита, со списком ведущих бизнесменов, принимавших участие в сомнительных сделках. В частности, один из кредитов, фигурировавший в этой информации, получило местное отделение правящей партии, а другой - компания, которой владел сын бывшего высокопоставленного члена этой партии. Оказалось также, что три банкира выдали кредиты самим себе. Все это, а также ряд других факторов, привело к проигрышу правящей партии.

ТЕМА 5. Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), когда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок. Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе. Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками – максимальная автоматизация и строгий контроль. Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы: отказ пользователей; внутренний отказ информационной системы; отказ поддерживающей инфраструктуры. Обычно применительно к пользователям рассматриваются следующие угрозы: нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими

характеристиками ИС); невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.); невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.). Основными источниками внутренних отказов являются: отступление (случайное или умышленное) от установленных правил эксплуатации; выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.); ошибки при (пере)конфигурировании системы; отказы программного и аппаратного обеспечения; разрушение данных; разрушение или повреждение аппаратуры. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы: нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования; разрушение или повреждение помещений; невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.). Весьма опасны так называемые «обиженные» сотрудники – нынешние и бывшие. Как правило, они стремятся нанести вред организации – «обидчику», например: испортить оборудование; встроить логическую «бомбу», которая со временем разрушит программы и/или данные; удалить данные. Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия, - пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных «злоумышленников» (среди которых самый опасный – перебой электропитания) приходится 13% потерь, нанесенных информационным системам. Некоторые примеры угроз доступности Угрозы доступности могут выглядеть грубо – как повреждение или даже разрушение оборудования (в том числе, носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего – грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования – не редкость.

ТЕМА 6. Основные угрозы целостности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. Можно предположить, что реальный ущерб был намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты. Не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно. В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних. Ранее было отмечено различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

 ввести неверные данные; изменить данные. Иногда изменяются содержательные данные, иногда – служебная информация. Показательный

случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее начальником президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что в указанное время он разговаривал по мобильному телефону, находясь вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние «файл против файла». Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарша знала пароль вицепрезидента, поскольку ей было поручено его менять), и иск был отвергнут. (Теоретически возможно, что оба фигурировавших на суде файла были подлинными, корректными с точки зрения целостности, а письмо отправили пакетными средствами, однако, это было бы очень странное для вицепрезидента действие.) Из приведенного случая можно сделать вывод не только об угрозах нарушения целостности, но и об опасности слепого доверия компьютерной информации. Заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль отправителя (мы приводили соответствующие примеры). Отметим, что последнее возможно даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов информационной безопасности: если нарушена конфиденциальность, может пострадать целостность.

ТЕМА 7. Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не

относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе, предметной. Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер. Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы.

Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности – частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или стараться свести дело к двумтрем легко запоминаемым (и столь же легко угадываемым) паролям. Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую – и не может быть обеспечена) необходимая защита. Угроза же состоит в том, что ктото не откажется узнать секреты, которые сами просятся в руки. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети и т.п.), но идея одна – осуществить доступ к данным в тот момент, когда они наименее защищены. Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Весьма опасной угрозой являются выставки, на которые многие организации, недолго думая, отправляют оборудование из производственной сети, со всеми хранящимися на них

данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде. Это плохо даже в пределах защищенной сети организации; в объединенной сети выставки – это слишком суровое испытание честности всех участников. Еще один пример изменения, о котором часто забывают, - хранение данных на резервных носителях. Для защиты данных на основных носителях применяют развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.