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

«Информационная безопасность в профессиональной деятельности»
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 «Информационная безопасность в профессиональной деятельности». – Ростов-на-Дону: Донской гос. техн. ун-т, 2018. –14с.

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 «Информационная безопасность в профессиональной деятельности» выполняется в форме эссе.

Информационная безопасность в профессиональной деятельности— 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:

- 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 работ

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 (зачет контрольной работы), после которого магистрант приступает к сдаче промежуточной аттестации в форме зачета.

Зачет проводится в устной форме. Во время зачета, обучающемуся задается три вопроса из общего перечня контрольных вопросов для подготовки к зачету.

Вопросы к зачёту

1. Прогресс информационных технологий и необходимость обеспечения информационной

безопасности.

2. Основные понятия информационной безопасности.

3. Структура понятия информационная безопасность.

4. Система защиты информации и ее структура.

5. Экономическая информация как товар и объект безопасности.

6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.

7. Персональные данные и их защита.

8. Информационные угрозы, их виды и причины возникновения.

9. Информационные угрозы для государства.

10. Информационные угрозы для компании.

11. Информационные угрозы для личности (физического лица).

12. Действия и события, нарушающие информационную безопасность.

13. Личностно-профессиональные характеристики и действия сотрудников, способствующих

реализации информационных угроз.

14. Способы воздействия информационных угроз на объекты.

15. Внешние и внутренние субъекты информационных угроз.

16. Компьютерные преступления и их классификация.

17. Исторические аспекты компьютерных преступлений и современность.

18. Субъекты и причины совершения компьютерных преступлений.

19. Вредоносные программы, их виды.

20. История компьютерных вирусов и современность.

21. Государственное регулирование информационной безопасности.

22. Деятельность международных организаций в сфере информационной безопасности.

23. Нормативно-правовые аспекты в области информационной безопасности в Российской

Федерации.

24. Доктрина информационной безопасности России.

25. Уголовно-правовой контроль над компьютерной преступностью в России.

26. Федеральные законы по ИБ в РФ.

27. Политика безопасности и ее принципы.

28. Фрагментарный и системный подход к защите информации.

29. Методы и средства защиты информации.

30. Организационное обеспечение ИБ.

31. Организация конфиденциального делопроизводства.

32. Комплекс организационно-технических мероприятий по обеспечению защиты

информации.

33. Инженерно-техническое обеспечение компьютерной безопасности.

34. Организационно-правовой статус службы безопасности.

35. Защита информации в Интернете.

36. Электронная почта и ее защита.

37. Защита от компьютерных вирусов.

38. «Больные» мобильники и их «лечение».

39. Популярные антивирусные программы и их классификация.

40. Организация системы защиты информации экономических объектов.

41. Криптографические методы защиты информации.

42. Этапы построения системы защиты информации.

43. Оценка эффективности инвестиций в информационную безопасность.

44. План обеспечения непрерывной работы и восстановления функционирования

автоматизированной информационной системы.

45. Управление информационной безопасности на государственном уровне.

46. Аудит ИБ автоматизированных банковских систем.

47. Электронная коммерция и ее защита.

48. Менеджмент и аудит информационной безопасности на уровне предприятия.

49. Информационная безопасность предпринимательской деятельности.

50. Обеспечение информационной безопасности должностных лиц и представителей деловых

кругов.

51. Основные определения информационной безопасности

52. Информация как предмет защиты, жизненный цикл информации и вопросы безопасности

53. Составляющие безопасности. Комплексная защита информации. Понятие и задачи.

54. Принципы организации систем обеспечения информационной безопасности

55. Классификация угроз информационной безопасности (с примерами).

56. Способы и средства защиты информации.

57. Управление доступом. Матричная и многоуровневая модели управления доступом.

58. Основы шифрования. Симметричная и асимметричная криптосистемы. Хеш-функции.

59. Электронная цифровая подпись.

60. Аутентификация. Способы аутентификации. Проблемы парольной защиты.

61. Аутентификация при помощи цифровых сертификатов. Сертифицирующие центры

62. Вредоносное программное обеспечение. Жизненный цикл вируса.

Краткий конспект лекций по дисциплине «Информационная безопасность в профессиональной деятельности»

Информация (от латинского informatio — разъяснение, изложение) — с середины XX века общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом, обмен сигналами в животном и растительном мире, передачу признаков от клетки к клетке, от организма к организму; одно из основных понятий кибернетики.

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Согласно стандартам по обеспечению информационной безопасности главное в любой компании является:

·Определить цель для обеспечения защиты информации компьютерных систем;

·Получить максимально эффективную систему управления информационной безопасностью;

·Произвести вычисления совокупности как количественных, так и качественных показателей, насколько они подходят под поставленные цели;

·Применение всех мер для обеспечения информационной безопасности, постоянное наблюдение за текущим состоянием системы;

·Применять инструкции по управлению безопасностью, которые позволяют правдиво оценить имеющуюся защиту информации.

Для субъектов, использующих информационные системы, важны следующие признаки информационных ресурсов: конфиденциальность, доступность и целостность.

Конфиденциальность — это защита информации от несанкционированного доступа. Иначе говоря, есть полномочия на доступ — есть информация. Примером может служить неразглашение организацией информации о зарплате рабочих.

Доступность — критерий, характеризующийся быстрым нахождением нужной информации.

Целостность — это правдивость и актуальность информации, её защита от недозволенного доступа и разрушения (изменения). Целостность является самым важным аспектом информационной безопасности, когда речь идет о, например, рецептуре лекарств, предписанных медицинских процедур, ходе технологического процесса — если нарушить целостность информации всех перечисленных примеров, это может привести к непоправимым последствиям.

Проанализировав основные признаки информационных ресурсов, самым важным для пользователей ИС является доступность.

На полшага позади по важности стоит целостность — потому как нет смысла в информации, если она не правдива или искажена.

Помимо трех основных признаков моделей безопасности выделяют также другие, не всегда обязательные:

· апеллируемость — невозможность отказа от авторства;

· подотчётность — распознование субъекта доступа и регистрации его действий;

· аутентичность или подлинность — свойство, гарантирующее, что субъект или ресурс идентичны заявленным. Признак, гарантирующий, что информация идентична заявленной.

Информационной безопасности в разной степени могут наносить ущерб действия, называемые угрозами. Делят их на следующие категории:

1.Действия авторизованного пользователя. В категорию входят: целенаправленный ущерб (уничтожение данных на сервере, повреждение данных других пользователей по неосторожности)

2.Действия, осуществляемые хакерами. Имеются в виду, люди, профессионально занимающиеся компьютерными преступлениями. Хакеры используют метод DOS_атаки. Эта угроза несанкционированного проникновения может быть инструментом для уничтожения данных, использования конфиденциальной информации в незаконных целях, а также для кражи со счетов денежных средств и др. Атака типа DOS (сокр. от Denial of Service — «отказ в обслуживании») — атака извне на сетевые узлы организации, которые отвечают за её эффективную работу (почтовые сервера). Хакеры массово посылают пакеты данных на эти узлы, что влечет за собой их перегрузку, тем самым выводит на некоторое время из рабочего состояния. Что, в последствие, ведет за собой нарушения в бизнес-процессах, потере клиентов, репутации и др.

3.Компьютерные вирусы, вредоносные программы. Широко используются для проникновения на электронную почту, узлы корпоративной сети, на сам носитель и хранитель информации, что может

повлечь за собой утрату данных, кражу информации. Из-за вирусов приостанавливается рабочий процесс, теряется рабочее время. Важно указать, что вирус может дать возможность злоумышленникам частичный или полный контроль над деятельностью организации.

4.Спам. Еще недавно спам можно было отнести к незначительным раздражающим факторам, но сейчас он превратился в одну из главных угроз для информации: спам вызывает у работников чувство психологического дискомфорта, отнимает массу времени на удаление его с электронных почтовых ящиков, что может повлечь за собой и удаление важной корреспонденции. А это, в свою очередь, потеря информации, потеря клиентов.

5.«Естественные угрозы». Помимо внутренних факторов, на безопасность информации могут влиять и внешние: неправильное хранение информации, кража носителей, форс-мажорные обстоятельства и др.

Можно подвести своеобразный итог: в современном мире наличие хорошо развитой системы по защите информации является одним из главных условий конкурентоспособности и даже жизнеспособности любой компании.

Чтобы обеспечить максимально полную информационную безопасность, различные средства защиты должны работать в системе, т. е. применяться одновременно и под централизованным управлением.

На настоящее время существуют множество методов для обеспечения информационной безопасности:

- комплекс ЗА (аутентификация, авторизация, администратирование);
- средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;
- средства зашифровки важной информации, хранящейся на ПК;
- межсетевые экраны;
- средства контентной фильтрации;
- средства антивирусной защиты;

· системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Любое из перечисленных средств может применяться как индивидуально, так и в соединении с другими. Это делает спектр защиты информации более обширным, что, несомненно, является положительным фактором.

«Комплекс 3А». Идентификация и авторизация — это ведущие элементы информационной безопасности. При попытке доступа к любой защищенной информации идентификация устанавливает: являетесь ли вы авторизованным пользователем сети. Цель авторизации, выявить к каким информационным ресурсам данный пользователь имеет доступ. Функция администрирования заключается в наделении пользователя отдельными расширенными возможностями, определения объема возможных для него действий в рамках данной сети.

Системы зашифровки информации позволяют снизить к минимуму потери в случае попытки несанкционированного доступа к данным, а также перехвата информации при пересылке или передачи по сетевым протоколам. Главная цель данного метода защиты — это обеспечение сохранение конфиденциальности. К системам шифрования применяются требования, такие как высокий уровень секретности замка (т. е. криптостойкость) и легальность использования.

Межсетевой экран действует как защитный барьер между сетями, контролирует и защищает от несанкционированного попадания в сеть или, наоборот, выведения из неё пакетов данных. Межсетевые экраны подвергают проверке каждый пакет данных на соответствие входящего и исходящего IP_адреса базе адресов, которые разрешены.

Важно контролировать и фильтровать поступающую и исходящую электронную почту, для сохранения и защиты конфиденциальной информации. Проверка вложений и самих почтовых сообщений на основе

установленных в организации правил, позволяет защитить работников от спама, а организацию от ответственности по судебным искам.

Администратор, как и другой авторизованный пользователь, может иметь право на слежение за всеми изменениями информации на сервере благодаря технологии проверки целостности содержимого жесткого диска (integrity checking). Это даёт возможность обнаружить несанкционированный доступ, проконтролировать любые действия над информацией (изменение, удаление и др.), а также идентифицировать активность вирусов. Контроль осуществляется на основе анализа контрольных сумм файлов (CRC_сумм).

В настоящее время антивирусные технологии позволяют выявить почти все вирусные и вредоносные программы с помощью метода сравнения кода образца в антивирусной базе с кодом подозрительного файла. Подозрительные файлы могут помещаться в карантин, подвергаться лечению либо удаляться. Антивирусные программы могут быть установлены на файловые и почтовые сервера, межсетевые экраны, на рабочие станции, функционирующие под распространенными операционными системами (Windows, Unix- и Linux_системы, Novell) на процессорах различных типов.

Фильтры спама основательно снижают непроизводительные трудозатраты, связанные с отчисткой файлов от спама, снижают нагрузку серверов, способствуют улучшению психологического фона в коллективе. К тому же фильтры спама снижают риск заражения новыми вирусами, потому как они часто схожи по признакам со спамом и удаляются.

Для защиты от естественных угроз в организации должен быть создан и реализован план по предупреждению и устранению чрезвычайных ситуаций (пожар, потоп). Основным методом защиты данных является резервное копирование.

Существует множество средств технической защиты информации от несанкционированного доступа (НСД): замки разового пользования, пластиковые идентификационные карты, пломбы, оптические и

инфракрасные системы, лазерные системы, замки (механические, электромеханические, электронные), видео системы охраны и контроля.

Политика информационной безопасности представляет собой набор правил, законов, рекомендаций и практического опыта, определяющих управленческие и проектные решения в области защиты информации. ПИБ является инструментом, с помощью которого происходит управление, защита, распределение информации в системе. Политика должна определять поведение системы в различных ситуациях.

Программа политики безопасности содержит в себе следующие этапы создания средств защиты информации:

1. Нахождение информационных и технических ресурсов, которые необходимо защитить;
2. Раскрытие полного множества потенциально возможных угроз и каналов утечки информации;
3. Оценивание уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
4. Диагностирование требований к системе защиты;
5. Подборка средств защиты информации и их характеристик;
6. Внедрение и организация использования выбранных мер, способов и средств защиты;
7. Осуществление контроля целостности и управление системой защиты.

Оценка текущей ситуации подразделяется на две системы: это «исследование снизу вверх» и «исследование сверху вниз». Первая построена на том, что служба информационной безопасности, основываясь на всех известных видах атак, применяет их на практике, чтобы проверить, возможна ли данная атака со стороны реального правонарушителя.

Метод «сверху вниз» представляет собой подробное изучение всех существующих схем хранения и обработки информации. Первой ступенью метода является определение, какие информационные потоки следует

защитить. Затем анализируется настоящее состояние системы информационной безопасности, для определения реализованных методик защиты, в каком объеме, и на каком уровне они реализованы. На третьей ступени осуществляется классификация всех информационных объектов на группы в соответствии с ее конфиденциальностью.

После этого необходимо выяснить насколько серьезный ущерб может быть нанесен, если информационный объект атакуют. Эта ступень именуется как «вычисление рисков». Рассчитывают возможный ущерб от атаки, вероятность такой атаки и их произведение. Полученный ответ и есть возможный риск.

На самом главном и ответственном этапе происходит сама разработка политики безопасности предприятия, которая обеспечит максимально полную защиту от возможных рисков. Но необходимо учитывать проблемы, которые могут возникнуть на пути инициации политики безопасности. К подобным проблемам можно отнести законы страны и международного сообщества, этические нормы, внутренние требования организации.

После создания как таковой политики информационной безопасности производится расчет её экономической стоимости.

В финале разработки программа утверждается у руководства фирмы и детально документируется. После этого должна следовать активная реализация всех компонентов, указанных в плане. Перерасчет рисков, и впоследствии модификация политики безопасности компании чаще всего проводится раз в два года.

Сама ПИБ оформляется в виде документированных требований на информационную систему. Существует три уровня таких документов (еще это называют детализация):

Документы верхнего уровня политики информационной безопасности показывают позицию организации к деятельности в области защиты информации, её готовность соответствовать государственным и международным требованиям в этой области. Например, они могут быть

названы: «Концепция ИБ», «Политика ИБ», «Технический стандарт ИБ» и т. п. Документы верхнего уровня могут выпускаться в двух формах — для внешнего и внутреннего пользования.

Документы среднего уровня касаются отдельных сторон информационной безопасности. Здесь описаны требования на создание и эксплуатацию средств защиты информации по конкретной стороне защиты информации.

Документы нижнего уровня содержат правила и нормы работ, руководства по администрированию, инструкции по эксплуатации частных сервисов информационной безопасности.

Этапы жизненного цикла информационной системы делятся на: стратегическое планирование, анализ, проектирование, реализацию, внедрение (инициацию) и эксплуатацию. Рассмотрим каждый этап детально:

1. Начальная стадия (стратегическое планирование).

На первой стадии определяется область применения системы, и ставят граничные условия. Для этого необходимо опознать все внешние объекты, с которыми будет взаимодействовать разрабатываемая система, определить характер этого взаимодействия. На стадии стратегического планирования определяются все функциональные возможности, а также приводятся описания наиболее важных из них.

2. Стадия уточнения.

На стадии уточнения анализируется прикладная область, происходит разработка архитектурной основы информационной системы. Необходимо описать большую часть функциональных возможностей системы и учесть связь между отдельными составляющими. В конце стадии уточнения анализируются архитектурные решения и способы устранения ведущих рисков в программе.

3. Стадия конструирования.

На данной стадии создаётся законченное изделие, готовое к передаче пользователю. По окончании конструирования определяется работоспособность полученного программного обеспечения.

4. Стадия передачи в эксплуатацию (инициация).

Стадия представляет собой непосредственную передачу программного обеспечения пользователю. При использовании разработанной системы часто выявляются различного плана проблемы, которые требуют дополнительных работ и внесения корректировок в продукт. В конце данной стадии выясняют: достигнуты ли цели, поставленные перед разработчиками или нет.

5. Выведение из эксплуатации и утилизация. В результате этого этапа данные переносятся в новую ИС.

Любая информационная система может оставаться максимально полезной в течение 3—7 лет. Далее требуется её модернизация. Следовательно, можно прийти к выводу, что с проблемой модернизации устаревших информационных систем сталкивается практически каждый создатель.

Для решения проблемы обеспечения информационной безопасности важно применение законодательных, организационных и программно-технических мер. Невнимательность хотя бы к одному из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.