Министерство науки и высшего образования Российской Федерации

Томский государственный университет
систем управления и радиоэлектроники

О. В. Гальцева

Информационные технологии в управлении качеством и защита информации
Методические указания по выполнению самостоятельной работы студентов

Томск
2021

УДК 004.056.53
ББК У051
Г 177

Рецензент:

Лобода Ю.О., доцент каф. управления инновациями ТУСУР,
канд. пед. наук

Гальцева, Ольга Валерьевна
Г 177 Информационные технологии в управлении качеством и защита информации: Методические указания по выполнению самостоятельной работы бакалавров направления 27.03.02 «Управление качеством» / О.В. Гальцева. – Томск: Томск. гос. ун-т систем упр. и радиоэлектронники, 2022. – 14 с.

Методические указания содержат рекомендации и материалы, необходимые для самостоятельной работы студентов по дисциплине «Информационные технологии в управлении качеством и защита информации».
Для студентов высших учебных заведений, обучающихся в бакалавриате по направлению 27.03.02 «Управление качеством».

Одобрено на заседании кафедры УИ, протокол № 6 от 24.12.2021.

УДК 004.056.53
ББК У051

Оглавление

1 Общие положения

Данные методические указания разработаны для студентов, обучающихся в Томском государственном университете систем управления и радиоэлектроники (далее - Университет) по программам магистратуры.

Структура дисциплины «Информационные технологии в управлении качеством и защита информации» предполагает выполнение студентами самостоятельной работы как по освоению теоретического материала, так и в рамках выполнения практических заданий. Рекомендации по выполнению практических заданий приведены в соответствующих методических указаниях.

В ходе выполнения самостоятельной работы студентам прививаются навыки работы с учебно-методической документацией, умения увязывать теоретические знания с практикой, четко излагать свои мысли, отвечать на вопросы, оформлять и представлять результаты работы.

Рекомендации подготовлены с целью помочь студентам в успешном освоении дисциплины и прохождении аттестации, давая информацию об ее структуре и оценочных средствах.

2 Разделы и содержание дисциплины

Дисциплина «Информационные технологии в управлении качеством и защита информации» содержит следующие разделы:

1. Основные положения управления качеством информационных систем:

Структура, состав и характеристика информационных систем. Роль и место управления качеством информационных систем в решении задач информатизации и социально-экономического развития. Базовые понятия управления качеством информационных систем. Формы управления качеством информационных систем. Методика работы с источниками по дисциплине.

2. Информационные технологии в управлении качеством и защита информации:

Информационные технологии в управлении качеством. Комплексная защита информационных технологий и информации. Организационные мероприятия по обеспечению защиты информационных технологий и информации. Инженерно-технические мероприятия и специализированное техническое оборудование для защиты информационных технологий и информации

3. Технология обработки данных в управлении качеством информационных систем: защита качества технологии обработки данных:

Основные понятия технологии обработки данных КС УКИС. Взаимодействие технологических процессов обработки данных КС УКИС и управляемой ИС. Идентификация дефектов обработки данных. Регистрация дефектов обработки данных. Контроль качества технологического процесса обработки данных. Защита качества технологии обработки данных. Алгоритмы криптографической защиты качества данных.

4. Методология управления качеством информационных систем и защита информации:

Основные категории методологии управления качеством информационных систем. Принципы управления качеством ИС. Решение задач в управлении качеством ИС. Моделирование в управлении качеством ИС. Методы определения системы показателей качества ИС. Выявление рисков изучаемых объектов в управлении качеством ИС. Защита информации в ИС. Основные средства защиты информации в управлении качеством ИС.

5. Формы управления качеством информационных систем и обеспечение защиты информации:

Структурная схема ЕС ГУКП. Общегосударственные и межотраслевые системы управления народным хозяйством (комитеты РФ, министерства РФ). Отраслевые системы (ОС УКП). Территориальные системы (ТС УКП). Комплексные системы управления качеством продукции предприятий. Уровни управления качеством информационной продукции: общее организационно-административное управление качеством и оперативное (непосредственное) управление качеством. Единая техническая и экономическая политика в отношении качества продукции и обеспечения защиты информации

6. Проблемы управления качеством информационных систем и защита информации:

Общие проблемы управления качеством ИС и защиты информации. Решение вопросов их идентификации и классификации, технологии подготовки, применения средств защиты информации. Систематизированное представление информационных ресурсов в сфере научного и информационного производства, организация защиты информации. Развитие нормативноправового регулирования.

.

3 Организация самостоятельной работы студентов

Самостоятельная проработка лекционного материала направлена на получение навыков работы с конспектом, структурирования материала, а также умения выделить основные пункты и положения, изложенные на лекции. Целесообразно ознакомиться с информацией, представленной в файлах, содержащих презентации лекций, предоставляемых преподавателем. Кроме того, проработка лекционного материала способствует более глубокому пониманию и прочному запоминанию теоретической части дисциплины. Проработка лекционного материала включает деятельность, связанную с изучением рекомендуемых преподавателем источников, в которых отражены основные моменты, затрагиваемые в ходе лекций.

Важное место отведено работе с собственноручно составленным конспектом лекций. При конспектировании во время лекции помните, что не следует записывать все, что говорит и/или демонстрирует лектор: старайтесь выявить главное и записать только это. Цель конспекта – формирование целостного логически выстроенного взгляда на круг вопросов, затрагиваемых в ходе изучения соответствующей темы.

При проработке лекционного материала необходимо: - отработать прослушанную лекцию (прочитать конспект, прочитать дополнительную литературу по аналогичной теме и сопоставить записи с конспектом) и восполнить пробелы в знаниях, если таковые обнаружились; - перед каждой последующей лекцией прочитать предыдущую, чтобы обновить знания для восприятия последующей новой информации.

В ходе изучения дисциплины некоторые из тем курса выносятся исключительно на самостоятельное изучение. Следует обратить внимание на то, что работа по этим темам включает как подбор источников, так и изучение их содержания. В зависимости от особенностей усвоения учебного материала студентами и объема аудиторной работы некоторые из вопросов, рассматриваемые в ходе проведения лекций и лабораторных работ, могут быть также вынесены в формат самостоятельного изучения.

4 Терминология дисциплины

Чтобы свободно ориентироваться в материалах дисциплины студенту следует ознакомиться с применяемой терминологией:

- ***Автоматизированная система (АС)*** – совокупность программных и аппаратных средств, предназначенных для хранения и (или) управления данными и информацией и производства вычислений.
- ***Авторизация*** – предоставление лицу прав на какие-либо действия в системе. Асимметричный метод – метод шифрования, заключающийся в использовании двух ключей: несекретного для шифрования и секретного для расшифровывания, известного только получателю.
- ***Атака*** – попытка реализации угрозы.
- ***Аудит*** – анализ накопленной информации, проводимый оперативно, в реальном времени или периодически.
- ***Аутентификация*** – процедура проверки соответствия некоего лица и его учетной записи в компьютерной системе.
- ***Вирус*** – код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- ***Защита информации*** – комплекс мероприятий, направленных на обеспечение информационной безопасности.
- ***Информационная безопасность (ИБ)*** – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.
- ***Идентификация*** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
- ***Индексирование*** – выражение центральной темы или предмета какого- либо текста или описание какого-либо объекта на информационно- поисковом языке.
- ***Информационная система (ИС)*** – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, реализующих информационные процессы; предназначена для хранения, обработки, поиска, распространения, передачи и представления информации.
- ***Информационно-поисковая система (ИПС)*** – программная система для хранения, поиска и выдачи интересующей пользователя (абонента) информации.
- ***Информационно-поисковый язык (ИПЯ)*** – формализованный искусственный язык, предназначенный для индексирования документов, информационных запросов и описания фактов с целью последующего хранения и поиска.
- ***Информационные ресурсы*** – вся накопленная информация об окружающей нас действительности, зафиксированная на материальных носителях, обеспечивающих ее передачу во времени и пространстве между различными потребителями.
- ***Информационный менеджмент (ИМ)*** – совокупность методов и средств управления информационной деятельностью предприятия в целях обеспечения эффективности создания, внедрения и эксплуатации информационной системы, реализующей информационные технологии.
- ***Источник активных угроз*** – непосредственные действия злоумышленников, программные вирусы и т.п.
- ***ИТ-менеджер*** – человек, осуществляющий информационный менеджмент.

- ***Ключ*** – секретная информация, используемая криптографическим алгоритмом при шифровании / расшифровке сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности.
- ***Конфиденциальность*** – обеспечение доступа к информации только авторизованным пользователям.
- ***Криптографическая стойкость (криптостойкость)*** – способность криптографического алгоритма противостоять возможным атакам на него.
- ***Несанкционированный доступ (НСД)*** – доступ к программным данным, который получают абоненты, не прошедшие регистрацию и не имеющие права на ознакомление или работу с этими ресурсами.
- ***Политика информационной безопасности*** – совокупность документированных правил, процедур, практических приемов, решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.
- ***Симметричное шифрование*** – метод, заключающийся в использовании одного и того же ключа, хранящегося в секрете, для шифрования и для расшифровывания данных.
- ***Туннелирование*** – метод построения сетей, при котором один сетевой протокол «упаковывает» передаваемую порцию данных вместе со служебными полями в новый «конверт».
- ***Угроза*** – потенциальная возможность определенным образом нарушить информационную безопасность.
- ***Хэш-функция*** – труднообратимое преобразование данных, реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока и служит результатом хэш- функции.
- ***Червь*** – код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение.
- ***Шифрование*** – криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.
- ***Шифр, код*** – совокупность алгоритмов криптографических преобразований, отображающих множество возможных открытых данных на множество возможных зашифрованных данных и обратных им преобразований.
- ***Электронная цифровая подпись (ЭЦП)*** – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа и позволяющий идентифицировать владельца сертификата ключа подписи, а также обеспечивающий неотказуемость подписавшегося.
- ***DFD (Data Flow Diagram*** – Диаграмма потоков данных) – информационная модель, используемая для документирования механизмов передачи и обработки информации в моделируемой системе.
- ***IDEF0 (Function Modeling)*** – стандарт, определяющий методологию функционального моделирования. С помощью наглядного графического языка IDEF0 изучаемая система предстает в виде набора взаимосвязанных функций (функциональных блоков).

5 Вопросы для самоконтроля

При изучении материала дисциплины очень важно самостоятельно контролировать освоение материала. Сделать это удобно, отвечая на вопросы для самоконтроля:

1. Сущность качества и управления им.
2. Системы менеджмента качества в информационных системах.
3. Элементы системы управления качеством.
4. Развитие статистических методов контроля качества.
5. Систематический контроль качества от проектирования до изготовления продукции.
6. комплексный подход к управлению качеством.
7. Всеобщее управление качеством (Total Quality Management, TQM).
8. Сущность философии Деминга (учение Деминга) в информационных системах.
9. Нормативные и законодательные акты в области менеджмента качества.
10. Нормативные и законодательные акты в области обеспечения информационной защиты менеджмента качества.
11. Инструменты управления: алгоритмирование, мозговой штурм, древовидные и стрелочные диаграммы, модель «Кано».
12. Методы управления качеством: наделение работников полномочиями, метод сравнения (benchmarking), реинжиниринг в информационных системах.
13. Развития стандартов качества и защиты информации.
14. Основные причины, обусловившие разработку стандартов ISO и защиты информации.
15. Предназначение стандартов ISO серии 9000.
16. Автоматизация деятельности по управлению качеством.
17. Проблемы информационного обеспечения управления качеством.
18. Инновационные процессы в управлении качеством.
19. Электронный документооборот.

6 Тестовые вопросы по дисциплине

Тестирование является обязательной частью аттестации по дисциплине, а также важным средством проверки остаточных знаний студентов. Подготовка к тестированию предполагает повторение материала по всем разделам дисциплины. Для тестирования может использоваться следующий перечень вопросов:

1. Для безопасной передачи данных по каналам интернет используется технология:
а) WWW;
б) DICOM;
Проверено в генераторе 17
в) VPN;
г) FTP;
д) XML.

2. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа:
а) антивирус;
б) замок;
в) брандмауэр;
г) криптография;
д) экспертная система.

3. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:
а) идентификация;
б) аутентификация;
в) авторизация;
г) экспертиза;
д) шифрование.

4. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:
а) авторизация;
б) аутентификация;
в) обезличивание;
г) деперсонализация;
д) идентификация.

5. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:
а) авторизация;
б) обезличивание;
в) деперсонализация;
г) аутентификация;
д) идентификация.

6. Информационная безопасность в ИТ - это
а) модификация информации;
б) защита данных от преднамеренного доступа;
в) совокупность данных;
г) все что перечислено.

7. Способы цивилизованной защиты информации в ИТ - это
а) технические, законодательные и программные средства;
б) вирусные средства; в) системные программы;
г) прикладные программы.

8. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:
а) токен;
б) password;
в) пароль;
г) login;
д) смарт-карта.

9. Обязательное для выполнения лицом, получившим доступ к определенной информации,
требование не передавать такую информацию третьим лицам без согласия ее обладателя - это:
а) электронное сообщение;
б) распространение информации;
в) предоставление информации;
г) конфиденциальность информации;
д) доступ к информации.

10. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц - это
а) уничтожение информации;
б) распространение информации;
в) предоставление информации;
г) конфиденциальность информации;
д) доступ к информации.

11. Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные - это
а) информационная система персональных данных;
б) база данных;
в) централизованное хранилище данных;
г) система Статэкспресс;
д) сервер.

12. Отношения, связанные с обработкой персональных данных, регулируются законом…
а) «Об информации, информационных технологиях»;
б) «О защите информации»;
в) Федеральным законом «О персональных данных»;
г) Федеральным законом «О конфиденциальной информации»;
д) «Об утверждении перечня сведений конфиденциального характера.

13. Классификация сетей в информационных технологиях:
а) локальная, глобальная и региональная;
б) глобальная и региональная;
в) региональная и локальная;
г) специальная.

14. Хищение информации – это…
а) несанкционированное копирование информации;
б) утрата информации;
в) блокирование информации;
г) искажение информации;
д) продажа информации.

15. Владельцем информации первой категории является…
а) государство;
б) коммерческая организация;
в) муниципальное учреждение;
г) любой гражданин;
д) группа лиц, имеющих общее дело.

16. Информацией, составляющей государственную тайну, владеют:
а) государство;
б) только образовательные учреждения;
в) только президиум Верховного Совета РФ;
г) граждане Российской Федерации;
Проверено в генераторе 19
д) только министерство здравоохранения.

17. Для предотвращения потери информации в ИТ, необходимо…
а) проверять носители антивирусными программами;
б) проводить дефрагментацию диска;
в) использовать лицензионное программное обеспечение;
г) все действия правильные.

18. Нотация IDEF0 -
а) унифицированный язык моделирования;
б) система условных обозначений для моделирования бизнес-процессов;
в) диаграмма потоков данных;
г) методология функционального моделирования.

19. Нотация BPMN -
а) унифицированный язык моделирования;
б) система условных обозначений для моделирования бизнес-процессов;
в) диаграмма потоков данных;
г) методология функционального моделирования.

20. Нотация UML -
а) унифицированный язык моделирования;
б) система условных обозначений для моделирования бизнес-процессов;
в) диаграмма потоков данных;
г) методология функционального моделирования.

7 Контрольные вопросы

Приведенный ниже перечень вопросов рекомендуется использовать студенту для подготовки к аттестации по дисциплине:

1. Сущность информационных обеспечения в управлении качеством.
2. Классификация информации.
3. Понятие информационного ресурса.
4. Экономическая информация.
5. Количество информации.
6. Статистический, семантический, прагматический и структурный подходы.
7. Понятие и классификация информационных систем. Основные составляющие системы. Компоненты и свойства системы.
8. Задачи и функции, компоненты и архитектура ИС.
9. АРМ - средства автоматизации конечного рабочего места: понятие и содержание, классификация, принципы моделирования, применение интерактивных инструментальных средств.
10. Состав и структура АРМ, основные требования, этапы разработки.
11. Эргономическое обеспечение.
12. Визуальное моделирование.
13. Информационных систем управления качеством.
14. Объекты проектирования информационных систем.
15. Организация создания информационных систем. Стадии, методы.
16. Методы и модели формирования управленческих решений.
17. Роль пользователя в создании информационных систем.
18. Информационное обеспечение информационных систем: информационное, техническое, математическое и программное, методическое, лингвистическое, правовое и организационное. Проверено в генераторе 20
19. Анализ информации. Понятие информационного обеспечения, его структура.
20. Хранилища данных и базы знаний.

Список рекомендуемой литературы

1. Сухостат, В. В. Информационные технологии в управлении качеством и защита информации / В. В. Сухостат. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2020. – 82 с. [Электронный ресурс]: — Режим доступа: https://www.elibrary.ru/download/elibrary_46367777_80967233.pdf (дата обращения: 30.12.2021).

2. Вострецова, Л. Н. Информационные технологии в управлении качеством и защита информации : Учебное пособие / Л. Н. Вострецова. – Ульяновск : Ульяновский государственный университет, 2021. – 184 с. [Электронный ресурс]: — Режим доступа: https://www.elibrary.ru/download/elibrary_48399246_39860513.pdf (дата обращения: 30.12.2021).