Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Новгородский государственный университет имени Ярослава Мудрого»
МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ
ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ

Учебно-методическая документация

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОЦЕНКЕ КАЧЕСТВА ПОДГОТОВКИ ОБУЧАЮЩИХСЯ

ОП.15 ИНФОМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность:
09.02.01 Компьютерные системы и комплексы

Квалификация выпускника: техник по компьютерным системам
(базовая подготовка)

Разработчик: Преподаватель Цымбалюк А.Е.

Методические рекомендации по организации и выполнению самостоятельной работы дисциплины «Информационная безопасность» приняты на заседании предметной (цикловой) комиссии дисциплин профессионального цикла специальности 09.02.03 «Программирование в компьютерных системах», протокол № 1 от 05.09. 2014 г.

Председатель предметной (цикловой) комиссии _____/ Цымбалюк Л. Н.

2

Содержание

Пояснительная записка

Методические рекомендации по оценке качества подготовки обучающихся, являющиеся частью учебно-методического комплекса по дисциплине «Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно -коммуникационных сетях связи» составлены в соответствии с:

1 Федеральным государственным образовательным стандартом по специальности 09.02.01 Компьютерные системы и комплексы;

2 Рабочей программой дисциплины ОП.17 Информационная безопасность;

3 Положением об оценке качества освоения обучающимися основных профессиональных образовательных программ среднего профессионального образования в колледжах НовГУ.

Методические рекомендации по оценке качества подготовки обучающихся охватывают весь объем содержания учебной дисциплины «Вычислительная техника», включают в себя все виды планируемых аттестационных мероприятий с указанием формы проведения, перечня вопросов и практических заданий, критериев оценки.

Оценка качества подготовки обучающегося проводится **с целью** выявления уровня знаний, умений обучающегося.

После изучения дисциплины обучающийся **должен**

уметь:

- классифицировать угрозы информационной безопасности;
- проводить выборку средств защиты в соответствии с выявленными угрозами;
- определять возможные виды атак;
- осуществлять мероприятия по проведению аттестационных работ;
- разрабатывать политику безопасности объекта;
- выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
- использовать программные продукты, выявляющие недостатки систем защиты;
- производить установку и настройку средств защиты;
- конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
- выполнять тестирование систем с целью определения уровня защищенности;
- использовать программные продукты для защиты баз данных;
- применять криптографические методы защиты информации;

В результате освоения дисциплины обучающийся должен знать:

- каналы утечки информации;
- назначение, классификацию и принципы работы специализированного оборудования;
- принципы построения информационно-коммуникационных сетей;
- возможные способы несанкционированного доступа;
- нормативно-правовые и законодательные акты в области информационной безопасности;
- правила проведения возможных проверок;
- этапы определения конфиденциальности документов объекта защиты;
- технологии применения программных продуктов;
- возможные способы, места установки и настройки программных продуктов;

- конфигурации защищаемых сетей;
- алгоритмы работы тестовых программ;
- собственные средства защиты различных операционных систем и сред;
- способы и методы шифрования информации

Оценка качества подготовки обучающихся по данной дисциплине предусматривает следующие аттестационные мероприятия: итоговую аттестацию.

Итоговая аттестация по дисциплине в соответствии с учебным планом проводится в 7 семестре в форме экзамена.

Текущий контроль успеваемости

Раздел, тема	Формы и методы контроля
Раздел 1. Основы информационной безопасности	
Тема 1.1. Понятие информационной безопасности, угрозы ИБ	устный опрос на теоретическом занятии; выполнение внеаудиторной самостоятельной работы; выполнение аудиторной практической работы;
Тема 1.2. Конфиденциальная информация	устный опрос на теоретическом занятии; заслушивание подготовленных сообщений;
Раздел 2. Правовое обеспечение информационной безопасности	
Тема 2.1 Нормативно-правовые основы информационной безопасности в РФ.	устный опрос на теоретическом занятии; выполнение индивидуального задания для самостоятельной работы; выполнение аудиторной практической работы;
Тема 2.2 Лицензирование и сертификация	устный опрос на теоретическом занятии; заслушивание подготовленных сообщений;
Раздел 3. Организационное обеспечение информационной безопасности	
Тема 3.1 Понятие организационного обеспечения ИБ	устный опрос на теоретическом занятии; выполнение внеаудиторной самостоятельной работы; выполнение аудиторной практической работы;
Тема 3.2 Модели защиты информационных систем	устный опрос на теоретическом занятии; заслушивание подготовленных сообщений;
Раздел 4. Программно-аппаратные средства защиты информации	
Тема 4.1. Информационная безопасность в телекоммуникационных и информационно-коммуникационных сетях.	устный опрос на теоретическом занятии; выполнение внеаудиторной самостоятельной работы; выполнение аудиторной практической работы;
Тема 4.2. Антивирусная защита информации	устный опрос на теоретическом занятии; заслушивание подготовленных сообщений;
Раздел 5. Администрирование телекоммуникационных	

Раздел, тема	Формы и методы контроля
систем	
Тема 5.1 **Технологии защиты данных**	устный опрос на теоретическом занятии; выполнение внеаудиторной самостоятельной работы; выполнение аудиторной практической работы;
Тема 5.2 **Технология обеспечения безопасности сетевых операционных систем.**	устный опрос на теоретическом занятии; заслушивание подготовленных сообщений, выполнение итогового теста на сайте do.novsu.ru;

Итоговая аттестация

Семестр VII.
Форма промежуточной аттестации – экзамен

Вопросы к экзамену

1. Актуальность проблемы обеспечения безопасности информации. Классификация угроз информации. Основные методы реализации угроз информационной безопасности.
2. Информационная безопасность. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
3. Направления обеспечения информационной безопасности. Инженерно-техническая защита информации. Классификация основных видов технических каналов утечки информации. Каналы утечки информации, обрабатываемой ТСПИ.
4. Направления обеспечения информационной безопасности.
5. Инженерно-техническая защита информации. Методы и способы защиты информации.
6. Инженерно-техническая защита информации. Криптографическая защита информации. Электронная цифровая подпись.
7. Инженерно-техническая защита информации (основные определения, классификация).
8. Инженерно-техническая защита информации. Архитектура средств защиты информации.
9. Инженерно-техническая защита информации. Классификация основных видов технических каналов утечки информации. Каналы утечки информации при ее передаче по каналам связи.
10. Инженерно-техническая защита информации. Криптографическая защита информации. Симметричные криптосистемы шифрования.
11. Инженерно-техническая защита информации. Криптографическая защита информации. Асимметричные криптосистемы шифрования.
12. Инженерно-техническая защита информации. Классификация основных видов технических каналов утечки информации. Общая характеристика и классификация технических каналов утечки информации.
13. Инженерно-техническая защита информации. Классификация основных видов технических каналов утечки информации. Технические каналы утечки видовой информации.
14. Инженерно-техническая защита информации. Основные понятия криптографической защиты информации.
15. Инженерно-техническая защита информации. Классификация основных видов технических каналов утечки информации. Каналы утечки речевой информации.
16. Инженерно-техническая защита информации. Криптографическая защита информации. Хэш-функция.
17. Инженерно-техническая защита информации. Антивирусная защита информации.
18. Инженерно-техническая защита информации. Основные понятия криптографической защиты информации.

19. Инженерно-техническая защита информации. Методы и способы защиты информации.
20. Инженерно-техническая защита информации. Криптографическая защита информации. Симметричные криптосистемы шифрования.
21. Инженерно-техническая защита информации. Классификация основных видов технических каналов утечки информации. Каналы утечки речевой информации.
22. Инженерно-техническая защита информации (основные определения, классификация).
23. Инженерно-техническая защита информации. Криптографическая защита информации. Симметричные криптосистемы шифрования.
24. Инженерно-техническая защита информации. Методы и способы защиты информации.
25. Инженерно-техническая защита информации. Основные понятия криптографической защиты информации.
26. Организационная защита информации.
27. Правовая защита информации. Законодательство Российской Федерации по защите государственной тайны.
28. Правовая защита информации. Законодательство Российской Федерации по защите персональных данных.
29. Правовая защита информации. Положение о государственной системе защиты информации в Российской Федерации.
30. Правовая защита информации. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информатизации и о защите информации».
31. Правовая защита информации. Законодательство Российской Федерации по защите персональных данных.
32. Правовая защита информации. Лицензирование деятельности организаций, сертификация средств защиты информации.
33. Правовая защита информации. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информатизации и о защите информации».
34. Основные концептуальные положения системы защиты информации. Требования к системе защиты информации. Виды обеспечения системы защиты информации. Концептуальная модель информационной безопасности.
35. Ответственность за нарушение требований защиты информации Российской Федерации.

Практические задания

Средствами информационно-правовой базы осуществить поиск информации. Работу оформить в электронном виде.

1. Найдите определение понятия «лицензия» и «лицензиат»
2. Перечислите виды работ, подлежащие лицензированию при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации.
3. Указать необходимость аккредитации организации по требованиям безопасности информации.
4. Указать пять организаций-лицензиатов, имеющих действующие лицензии ФСТЭК/ФСБ России.
5. Указать пять организаций-лицензиатов, имеющих действующие аттестаты аккредитации ФСТЭК России.
6. Указать номер, дату выдачи и срок окончания сертификата/ов соответствия на средство защиты информации Dallas Lock 8.0-K
7. Указать номер, дату выдачи и срок окончания сертификата/ов соответствия на средство защиты информации VipNET Coordinator HW1000
8. Указать номер, дату выдачи и срок окончания сертификата/ов соответствия на средство защиты информации «Соболь» 3.0
9. Указать номер, дату выдачи и срок окончания сертификата/ов соответствия на средство защиты информации «Secret Net»
10. Указать номер, дату выдачи и срок окончания сертификата/ов соответствия на средство защиты информации «Аккорд»
11. Перечислите требования соблюдения национальных интересов Российской Федерации в информационной сфере
12. Укажите ответственность за разглашение сведений, составляющих персональные данные
13. Укажите порядок сертификации средств защиты информации
14. Перечислите общие методы обеспечения информационной безопасности Российской Федерации
15. Перечислите основные задачи и функции Совета Безопасности Российской Федерации
16. Укажите ответственность за использование вредоносных программ
17. Перечислите ограничения гражданин, допущенных к государственной тайне
18. Укажите как осуществляется допуск предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну
19. Перечислите органы защиты государственной тайны
20. Укажите виды деятельности по защите информации, подлежащих обязательному лицензированию
21. Укажите ответственность за разглашение сведений, составляющих государственную тайну
22. Перечислите угрозы информационной безопасности Российской Федерации
23. Перечислите источники угроз информационной безопасности Российской Федерации
24. Перечислите информацию, к которой не может быть ограничен доступ

25. Укажите ответственность за нарушение авторских прав (нелицензионное ПО)
26. Перечислить основные права на обработку информации в соответствии с Конституцией России.
27. Каким образом происходит формирования государственной политики в области обеспечения информационной безопасности?
28. Каким образом определяется система безопасности и ее функции?
29. Кем осуществляется контроль состояния защиты информации на предприятии?
30. Описать принцип засекречивания сведений и перечить сведения, не подлежащие засекречиванию.
31. Каким образом (какой организацией) осуществляется финансирование мероприятий по защите информации, содержащей сведения, отнесенных к государственной или служебной тайне.
32. Перечислите сведения, которые не могут быть отнесены к служебной информации ограниченного распространения.
33. Перечислите сведения, которые не могут составлять коммерческую тайну.
34. Опишите сведения, не подлежащие отнесению к государственной тайне и засекречиванию.
35. Перечислите сведения, которые относятся к персональным данным.
36. Дайте определение информации.
37. Дайте определение информационной системы
38. Дайте определение информационных технологий.
39. Дайте определение конфиденциальная информация.
40. Дайте определение документированной информации.
41. Дайте определение общедоступной информации
42. Дайте определение коммерческой тайны
43. Опишите варианты подписи документов: простая, усиленная неквалифицированная и усиленная квалифицированная

Критерии оценки

Методы оценки результатов обучения:

- традиционная система отметок в баллах за каждую выполненную работу, на основе которых выставляется итоговая отметка

- итоговая отметка определяется на основании годовой и оценки за дифференцированный зачёт.

В критерии оценки входят:

- Уровень освоения студентом материала, предусмотренный учебной программой по дисциплине;
- Уровень практических умений, продемонстрированных при выполнении практического задания;
- Логичность, обоснованность, чёткость, краткость изложения ответов;
- Степень владения профессиональной терминологией;

Оценка знаний производится по пятибалльной шкале. В основу критериев оценки учебной деятельности обучающихся положены объективность и единый подход. Данные критерии применяются при оценке устных, письменных, самостоятельных и других видов работ.

Оценка «5» - выставляется за полный, безошибочный ответ, при устных ответах устранения отдельных неточностей с помощью дополнительных вопросов учителя; студент должен правильно определять понятия и категории, выявлять основные тенденции и противоречия, свободно ориентироваться в теоретическом и практическом материале.

Оценка «4» - выставляется за правильные и достаточно полные ответы, не содержащие ошибок и упущений; незначительных (негрубых) ошибок при воспроизведении изученного материала; оценка может быть снижена в случае затруднений студента при ответе на дополнительные вопросы. При выполнении практической (лабораторной) работы допущены отдельные ошибки.

Оценка «3» - выставляется при недостаточно полном ответе; затруднениях при самостоятельном воспроизведении, необходимости незначительной помощи учителя; при наличии ошибок и некоторых пробелов в знаниях студента; затруднения при ответах на видоизменённые вопросы; в практической (лабораторной) работе содержатся серьёзные ошибки, индивидуальные задания решены не до конца;

Оценка «2» - выставляется в случае отсутствия необходимых теоретических знаний по дисциплинам, не выполнения практической (лабораторной) работы по дисциплине; затруднения при ответах на стандартные вопросы; наличия нескольких грубых ошибок; полного незнания изученного материала, отсутствия элементарных умений и навыков.

Общая классификация ошибок

При оценке знаний, умений и навыков учащихся следует учитывать все ошибки (грубые и негрубые) и недочеты.

Грубыми считаются следующие ошибки:

- незнание определения основных понятий, общепринятых символов обозначений величин, единиц измерения;
- неумение выделить в ответе главное;
- неумение выполнить практическое задание;
- неумение пользоваться первоисточниками, учебником и справочниками;

- нарушение техники безопасности;
- небрежное отношение к оборудованию.

К негрубым ошибкам следует отнести:
- неточность формулировок, определений, понятий;
- нерациональный метод решения задачи или недостаточно продуманный план устного ответа (нарушение логики, подмена отдельных основных вопросов второстепенными);
- нерациональные методы работы со справочной и другой литературой;
- неумение решать задачи, выполнять задания в общем виде.

Недочетами являются:
- нерациональные приемы решения практических задач;
- небрежное выполнение блок-схем;
- орфографические ошибки в употреблении основных понятий.

Информационное обеспечение обучения

Основная литература:

1. Т. Л. Партыка, И. И. Попов Информационная безопасность Москва, ИД «Форум», ИНФРА-М, 2008.
2. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность: Учебное пособие для сред. проф. образования -М. «Академия», 2009.

Дополнительная литература:

1. Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А.Шелупанов Основы информационной безопасности. Москва, Горячая линия - Телеком, 2006
2. В. Ф. Шаньгин Информационная безопасность комплексных систем и сетей. Москва, ИД «Форум», ИНФРА-М, 2008
3. П. Н. Башлы Информационная безопасность. Ростов-на- Дону Феникс.2006
4. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации. Составители А. П. Зайцев, А. А. Шелупанов. Издательство Томского государственного университета систем управления и радиоэлектроники. 2004
5. Защита информации в системах мобильной связи. Учебное пособие. Москва, Горячая линия - Телеком, 2009
6. Технические средства обеспечения информационной безопасности
7. Часть 1. Технические каналы утечки информации
8. Часть 2. Средства защиты информации от утечки по техническим каналам. Учебное пособие, Томск, 2004
9. П.Б.Хорев Методы и средства защиты информации в компьютерных системах Москва, Издательский центр «Академия», 2008
10. А.В.Соколов, О.М.Степанюк Методы информационной защиты объектов и компьютерных сетей - М.: ООО «Фирма «Издательство АСТ» 2000.
11. Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин Защита информации в компьютерных системах и сетях Москва, «Радио и связь», 1999
12. Д.В.Скляров Искусство защиты и взлома информации СПб.: БХВ-Петербург,2004
13. Б.А.Феденко, И.В.Макаров Безопасность сетевых ОС
14. О.М.Раводин, В.О.Раводин Безопасность операционных систем. Томск, Томский государственный университет систем управления и радиоэлектроники. 2005

3.2.8.Электронные источники информации:

Сайты дистанционного обучения:

http://intuit.ru

http://java.sun.com/

http://www.perl.org/

http://www.php.net/

Отечественные журналы

1. Мир ПК
2. Первая миля
3. Электросвязь
4. Сети
5. Мир связи

6. Технологии и средства связи
7. Радио
8. Мир ПК+СД
9. Мобильные компьютеры +СД
10. Системный администратор
11. Системы безопасности.
12. Сети и системы связи
13. Мобильные телекоммуникации
14. Технологии и средства связи
15. Радиомастер. Практическая радиоэлектроника
16. Ремонт электронной техники
17. Мир связи Connect
18. Мобильные системы

Интернет-ресурсы:

1. http://www.guardofinform.narod.ru/bibl_3.htm
2. www.minsvyaz.ru Официальный сайт Министерства информационных технологий и связи.
3. www.sotovik.ru Информационный сайт, посвященный телекоммуникациям: обзоры рынка, новости операторов.
4. www.telecomru.ru Экспертный портал "Телекоммуникации России" - независимое сетевое СМИ.
5. www.comnews.ru Новости рынка телекоммуникаций России и СНГ.
6. www.mobail-review.com Сайт, посвященный мобильным устройствам и технологиям, новостям операторов связи, рекламным акциям.
7. www.gptelecom.ru Законы РФ, постановления Правительства, документы Министерства связи и массовых коммуникаций РФ, технические документы и т. д.
8. www.osp.ru , www.pcmag.ru ,
9. www.crn.ru , www.elrussia.ru , www.kit-e.ru , www.globus-telecom.com , www.d-link.ru ,
10. www.intuit.ru , www.connect.ru , www.qwerty.ru ,
11. www.elsv.ru , www.ccc.ru Информационно-справочные системы.

Лист регистрации изменений

Номер изме-нения	Номер листа				Всего листов в документе	ФИО и подпись ответственного за внесение изменения	Дата внесения изменения	Дата введения изменения
	измененного	замененного	нового	изъятого				