ПЕРВОЕ ВЫСШЕЕ ТЕХНИЧЕСКОЕ УЧЕБНОЕ ЗАВЕДЕНИЕ РОССИИ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОРНЫЙ УНИВЕРСИТЕТ»

Утверждаю
Проректор по образовательной деятельности
_____ проф. А.П. Господариков
«5» марта 2018 г.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Информационная безопасность в АСУ ТП»

Форма обучения: очная

Объем программы: 40 часов

Руководитель программы: _____ Декан ФФиГД, к.т.н., доц. А.Б. Маховиков

Составители программы: _____ Доцент кафедры ИиКТ к.т.н Е.В. Катунцов

_____ Доцент кафедры АТПП к.т.н Н.И. Котелева

САНКТ-ПЕТЕРБУРГ
2018

1 Общие положения

1.1 Цель подготовки:

Приобретение теоретических знаний и практических навыков в области обеспечения информационной безопасности АСУ ТП.

1.2 Категория слушателей:

Специалисты и руководители подразделений, обеспечивающих функционирование АСУ ТП.

1.3 Планируемые результаты обучения - перечень профессиональных компетенций, качественное изменение которых осуществляется в результате обучения:

- понимание основных принципов обеспечения информационной безопасности в АСУ ТП;
- овладение методами защиты оконечного оборудования и сетей передачи информации АСУ ТП.

1.4 Требования к результатам освоения программы:

С целью достижения указанных в пункте 1.3 профессиональных компетенций, слушатели в процессе освоения программы повышения квалификации должны:

Получить знания по:

- основам управления информационной безопасностью в АСУ ТП;
- методам защиты оконечного оборудования и сетей передачи информации АСУ ТП;
- принципам аудита информационной безопасности в АСУ ТП.

Развить умения:

- выявлять угрозы информационной безопасности в АСУ ТП;
- обеспечивать защиту оконечных устройств и сетей АСУ ТП;
- проводить аудит информационной безопасности АСУ ТП.

1.5 Объем программы и виды учебной работы:

Вид учебной работы	Часы
Лекционные занятия	24
Практические занятия	14
Выполнение итоговой аттестации	2
Общий объем программы	**40**

1.6 Учебный план:

№	Наименование модуля	Всего часов	В том числе		
			Лекции	Практические занятия	Итоговая аттестация
1	Управление информационной безопасностью в АСУ ТП	8	8	-	-
2	Безопасность оконечных устройств АСУ ТП	8	4	4	-
3	Безопасность сетей передачи информации АСУ ТП	16	10	6	
4	Аудит информационной безопасности в АСУ ТП	6	2	4	
	Итоговая аттестация	2	-	-	2
	Всего	**40**	**24**	**14**	**2**

1.7 Календарный учебный график:

Продолжительность обучения	Количество часов в неделю (по расписанию обучения)	Виды занятий
Одна неделя	Пять раз в неделю по 8 часов аудиторной работы	Лекции, практические занятия, итоговая аттестация

1.8 Форма итоговой аттестации по программе:

Форма итоговой аттестации по программе – контрольное тестирование.

1.9 Вид документа, подтверждающий повышение квалификации:

После успешного окончания обучения выдается документ установленного образца о повышении квалификации – удостоверение о повышении квалификации (в объеме 40 часов).

2 Содержание обучения:

2.1 Содержание обучения по программе:

Наименование разделов профессионального модуля	Содержание учебного материала	Объем часов
Модуль 1. Управление информационной безопасностью в АСУ ТП	Тема 1.1. Базовые понятия и определения в области информационной безопасности	2
	Тема 1.2. Законодательство, государственные и отраслевые стандарты в области информационной безопасности	2
	Тема 1.3. Управление процессами информационной безопасности	2
	Тема 1.4. Политика информационной безопасности. Методика разбора инцидентов	2
Модуль 2. Безопасность оконечных устройств АСУ ТП	Тема 2.1. Основные угрозы безопасности оконечных устройств. Вирусы, черви, трояны. Шпионское программное обеспечение. Бэкдоры в программном обеспечении	2
	Тема 2.2. Атаки на оконечные устройства. Переполнение буфера. Повышение привилегий. Подбор пароля. Отказ в обслуживании	2
	Тема 2.3. Организация защиты оконечных устройств. Идентификация и авторизация пользователей. Антивирусное программное обеспечение. Персональные межсетевые экраны. Защита удаленного доступа	2
	Тема 2.4. Особенности безопасного использования SCADA систем и программного обеспечения PLC	2
Модуль 3. Безопасность сетей передачи информации АСУ ТП	Тема 3.1. Основные угрозы безопасности сетей передачи информации. Хищение и изменение информации	2
	Тема 3.2. Виды сетевых атак. Человек посередине. Переадресация порта. Атаки на маршрутизаторы и коммутаторы	2
	Тема 3.3. Обеспечение безопасности периметра сети. Межсетевые экраны. Системы обнаружения и предотвращения вторжений	2

Наименование разделов профессионального модуля	Содержание учебного материала	Объем часов
	Тема 3.4. Обеспечение безопасности локальной сети. Защита коммутаторов. Защита беспроводных сетей	2
	Тема 3.5. Обеспечение безопасности каналов передачи данных. Шифрование данных. Имитовставки. Цифровые подписи. Виртуальные частные сети	2
	Тема 3.6. Атаки методами социальной инженерии и защита от них	2
	Тема 3.7. Безопасность облачных технологий	
	Тема 3.8. Обеспечение безопасности в стандарте OPC	2
Модуль 4. Аудит информационной безопасности в АСУ ТП	Тема 4.1. Организация аудита информационной безопасности в АСУ ТП	2
	Тема 4.2. Аудит безопасности оконечных устройств. Программное обеспечение для поиска уязвимостей	2
	Тема 4.3. Аудит безопасности сетей передачи данных. Методы обнаружения уязвимостей в сетях	2

2.2 Вопросы для итогового теста:

1. Какова длинна хеш-значения получаемого в результате работы Secure Hash Algorithm 1 (SHA-1)
   a. 160 бит
   b. 160 байт
   c. 512 бит
   d. 512 байт
2. Для каких приложений наилучшим образом подходит режим шифрования Electronic Code Book (ECB)?
   a. Шифрование соединений по радио каналу
   b. Приложений с высокими требованиями к защищенности
   c. Шифрование маленьких запускаемых файлов
   d. Шифрование больших графических файлов
3. Невидимый цифровой водяной знак (Digital Watermark) это пример современного использования:
   a. Криптографии
   b. Криптоанализа
   c. Стеганографии
   d. Стеганоанализа
4. Наука о взломе шифров называется
   a. Криптография
   b. Криптоанализ
   c. Стеганография
   d. Стеганоанализ
5. Случайная величина прибавляемая к исходному сообщению по средствам XOR, перед шифрованием это:
   a. Контрольная сумма
   b. Вектор инициализации
   c. Величина контроля целостности

d. Величина избыточности

6. Какая характеристика не обязательна для обеспечения надежности одноразовых шифро-блокнотов (One-Time Pab)?

a. Блокноты генерируются истинно случайным образом
b. Ключи не могут использоваться дважды
c. Блокнот после использования уничтожается
d. Количество ключей в блокноте не должно превышать 128.

7. Какова эффективная криптостойкая длинна ключа в алгоритме Triple DES (3DES)

a. 56 бит
b. 112 бит
c. 168 бит
d. 192 бит

8. Классификация активов по уровням сможет помочь во всех нижеперечисленных ситуациях, исключая какую?

a. Группировка классифицированной информации по иерархии и уровню защиты
b. Исключение нечувствительных данных из мер излишней защиты
c. Извлечение данных из базы данных
d. Снижение стоимости защиты данных

9. Что из нижеперечисленного не является нарушением целостности (integrity) данных?

a. Не авторизованные изменения или манипуляция данных
b. Модификация данных без аутентификации
c. Преднамеренное или случайное изменение данных
d. Извлечение данных и последующее предоставление неавторизованного доступа к ним

10. Что из нижепричисленного относится по характеристикам к IDS (система обнаружения вторжений) работающей на базе правил?

a. Использования экспертной системой с запрограммированными условиями IF/THEN
b. Определение использования протокола в не типичной ситуации
c. Сравнение шаблонов поведения системы
d. Возможность определения новых атак

11. Какой тип резервного копирования архивирует только те файлы которые были изменены со времени последнего резервного копирования.

a. Инкрементальный
b. Полный
c. Частичный
d. Дифференциальный

12. Какой из нижеперечисленных шагов должен быть сделан первым перед внедрением комплексных мер физической безопасности?

a. Сознание методики оценки эффективности контрмер
b. Оценка рисков
c. Разработка программных документов
d. Внедрение контрмер

13. Мария должна посчитать какое количество ключей должно быть сгенерировано для 260 сотрудников использующих в компании ассиметричные алгоритмы шифрования. Какое количество ключей потребуется?

a. 33 670
b. 520
c. 67 340
d. 260

14. Шифрование может осуществляться на разных уровнях внутри операционной системы или на разных уровнях в стеке сетевых протоколов. Где находится PPTP шифрование?

a. Канальный уровень
b. Внутри приложения
c. Транспортный уровень
d. Канальный или физический уровень

15. Что является наиболее важным действием, которое необходимо выполнить при увольнении сотрудника?

a. Передать все файлы уволившегося сотрудника другому сотруднику.
b. Выполнить процедуру резервного копирования всех материалов и работы уволившегося сотрудника.
c. Оповестить других сотрудников об увольнении.
d. Деактивировать доступ к информационным ресурсам уволившегося сотрудника.

16. Какой из нижеперечисленных процессов является первым шагом в разработке BCP и DRP планов в компании?

a. Выбор альтернативной площадки
b. Анализ влияния на бизнес (Business Impact Analysis)
c. Тестовые процедуры и периодичность их выполнения
d. Классификация информации

17. Основная причина использования электронной подписи – убедиться в:

a. Конфиденциальности данных.
b. Целостности данных.
c. Наличии данных.
d. Своевременности данных.

18. Виртуальная частная сеть (VPN) обеспечивает конфиденциальность данных, используя:

a. Secure Sockets Layer (SSL)
b. Туннелирование
c. Электронную подпись
d. «Фишинг» (phishing)

19. Что из нижеперечисленного является особенностью IDS (Intrusion Detection System)?

a. Сбор информации о попытках атак
b. Определение слабых мест в определении политик
c. Блокировка доступа к определенным сайтам Интернет
d. Защита определенных серверов от доступа пользователей

20. Организация планирует расположение нового офиса, какой из ниже перечисленных факторов НАИМЕНЕЕ важен для выбора местоположения?

a. Расстояние до опорных пунктов экстренных служб.
b. Освещенность
c. Частота природных катастроф
d. Уровень преступности

21. Advanced Encryption Standard (AES) это алгоритм который используется для:

a. Обеспечения целостности данных
b. Шифрования массивов данных
c. Восстановления ключей
d. Распространения симметричных ключей

22. Какая из перечисленных контр мер не эффективна против спама?

a. Открытый mail relay сервер.
b. Надлежащим образом настроенный mail relay сервер
c. Фильтрация на магистральном почтовом сервере

d. Фильтрация на клиенте

23. Алиса хочет объединить все компьютеры проекта из разных отделов для того что бы упростить обмен информации о проекте по сети. Какая из следующих технологий позволит ей решить эту задачу?

a. VLAN
b. Открытая сетевая архитектура
c. Intranet
d. WAN

24. Что из нижеперечисленного не является достоинством VoIP?

a. Стоимость
b. Конвергенция (Convergence)
c. Гибкость (Flexibility)
d. Надежность

25. С какой целью компаниям стоит отправлять сотрудников в обязательные отпуска (Mandatory vacation):

a. Это позволяет сотрудникам лучше отдыхать, и следовательно лучше работать
b. Это облегчает поиск временной замены
c. Это позволяет выявить случаи мошенничества
d. Это необходимо для обеспечения предоставления наименьшего уровня доступа

26. Ознакомление о правилах безопасности (Security awareness) это:

a. тоже самое что и профессиональное обучение
b. проверка трудовой истории сотрудника и подтверждение его данных об образовании.
c. позволяет определить, кто в компании является потенциальной угрозой безопасности.
d. процедура с которой начинается первый день работы сотрудника

27. Что будет первичным шагом при оценке рисков, используя качественные (qualitative) методы.

a. Разработка сценария.
b. Оценить угрозы.
c. Определить потенциальные ежегодные потери.
d. Оценить потенциальные потери.

28. Какое из нижеперечисленных действий нельзя применять при управлении рисками:

a. Принять
b. Игнорировать
c. Переложить
d. Отказаться

29. Качественная оценка рисков использует следующие оценки:

a. Проценты
b. Расчёт полных ежегодных потерь
c. Высокий/средний/низкий
d. Величина в долларах

30. Какое из следующих определений соответствует принятию риска (acceptance):

a. Не использовать мероприятия направленные на смягчение риска и покрыть убытки из собственных источников в случае наступления риска.
b. Передать расходы по риску другой компании
c. Использовать дополнительные меры, которые позволят снизить финансовые затраты в случае наступления риска
d. Не принимать никаких действий, подумать о том, что делать с риском тогда, когда он наступит.

31. Какое из определений не является одним из триады информационной безопасности:

a. Целостность
b. Конфиденциальность
c. Масштабируемость
d. Доступность

32. Что такое хеш коллизия (Hash collision)

a. Ошибка при генерации хеш функции
b. Повторы в результирующей цифровой последовательности, которые свидетельствуют о ненадежности хеш алгоритма
c. Совпадение результирующей цифровой последовательности и цифровой подписи
d. Идентичная результирующая цифровая последовательность в результате разных исходных последовательностей.

33. Что является первым шагом при установлении защищенного соединение в гибридных системах таких как SSL или IPSEC

a. Обмен симметричными ключами
b. Обмен публичными ключами
c. Выбор хеш функции
d. Выбор алгоритма шифрования

34. Что является наилучшим методом проверки достоверности цифровой подписи:

a. Проверить подпись путем сравнения хеш функций вручную
b. Использовать публичный ключ для проверки цифровой подписи
c. Получить публичный ключ из доверенного удостоверяющего центра (trusted certificate authority) и проверить подпись с использованием полученного ключа
d. Использовать наиболее надежный хеш алгоритм для проверки.

35. Наука о скрытой передаче информации путём сохранения в тайне самого факта передачи называется:

a. Криптография
b. Стеганография
c. Криптоанализ
d. Стегаанализ

36. Что из нижеперечисленного не является правильной характеристикой хранилищ данных (data warehouse)?

a. Использование повышает риски неприкосновенности частной жизни.
b. Разработаны для хранения данных с целью последующего анализа.
c. Хранят данные из нескольких разных источников.
d. Созданы и используются для проектно-ориентированных тактических целей.

37. Когда организация не уверенна в окончательных свойствах разрабатываемого продукта, какая модель разработки подойдет наилучшим образом.

a. Cleanroom
b. Исследовательская модель
c. Прототипа модель
d. Итерационная разработка

38. Что из нижеперечисленного обычно не является частью системы контроля изменений

a. Тестирование
b. SLA для процесса утверждения
c. Отчеты для руководства
d. Одобрение изменений

39. Тимур и его команда получили от клиента заказ на проведение тестового взлома сети. Сетевые администраторы предупреждены о проведение теста но не знают время тестирования. Тимур собрал информацию о потенциальной цели из интернета, и также

обрывочная информация предоставлена клиентом. Какой уровень знания у команды тестирования, и какой тип теста будет проводится?

a. Полный уровень знаний; слепой тест.
b. Частичный уровень знаний; слепой тест.
c. Частичный уровень знаний; двойной слепой тест.
d. Нулевой уровень знаний; слепой тест.

40. Специалист по безопасности пытается предотвратить в компании ситуации когда пользователи получают излишние привилегии, какой из нижеперечисленных методов подойдет лучше всего?

a. Одобрение прав пользователей руководством
b. Двух-факторная идентификация и аутентификация.
c. Перехват предоставления привилегий в журналы аудита
d. Внедрение политики усиленного шифрования

41. Вася обнаружил что Ася получила неавторизованный доступ к его компьютеру, однако Ася не обладает очень большим опытом работы с компьютерами. Какую технику перехвата пароля вероятнее всего использовала Ася?

a. Словарная атака
b. Взгляд из-за плеча
c. Перехват электромагнитных полей
d. Радужные таблицы

42. Что такое публичный ключ:

a. Ключ при помощи которого зашифровывается и расшифровывается сообщение
b. Секретная цифровая последовательность используемая для зашифровывания сообщения с целью обеспечения конфиденциальности
c. Общедоступная цифровая последовательность с целью установления отправителя
d. Ключевая пара применяемая в ассиметричном шифровании

43. Что из нижеперечисленного не является атакой на результирующую цифровую последовательность хеш функции:

a. Грубая сила (Brute force)
b. Радужные таблицы (Rainbow tables)
c. Клавиатурный шпион (Keystroke logger)
d. Атака по словарю (Dictionary)

44. Какой из RAID массивов имеет наименьший коэффициент избыточности

a. RAID 1
b. RAID 5
c. RAID 10
d. RAID 0+1

45. Какой из RAID массивов имеет наименьший коэффициент отказоустойчивости

a. RAID 0
b. RAID 1
c. RAID 5
d. RAID 10

46. Какая информация не должна обязательно обрабатываться при инвентаризации оборудования с целью обеспечения информационной безопасности:

a. Информация о владельце
b. Информация о расположении
c. Данные о поставщике
d. Учетная информация (серийные номера и модели)

47. Какая стратегия использования программного обеспечения является наиболее рискованной для компании:

a. Использование программного обеспечения разных вендоров

b. Использование пиратского программного обеспечения
c. Использование программного обеспечения только одного вендора
d. Использование программного обеспечения с открытым кодом

48. Кто из нижеперечисленных администраторов имеет неограниченные привилегии в системах управления базами данных:
a. Администратор безопасности
b. Администратор базы данных
c. Сетевой администратор
d. Системный администратор

49. Какие требования выдвигаются к защите резервных копий:
a. Резервные копии могут быть защищены слабее, чем исходная информация
b. Резервные копии могут быть защищены сильнее, чем исходная информация
c. Резервные копии должны быть защищены не менее надежно, чем исходная информация
d. Резервные копии могут быть защищены также как и исходная информация

50. В соответствии с требованиями политики необходимо дополнительное разрешение на использование сниффера. Кто из ниже перечисленных сотрудников должен быть включен в список утверждающих:
a. Системный администратор
b. Сетевой администратор
c. Администратор безопасности
d. Администратор баз данных

51. Две части целостности - это система и
a. Данные
b. Процесс
c. Информация
d. Транзакции

52. Использование криптография повышает риски нарушения:
a. Целостности
b. Конфиденциальности
c. Доступности
d. Достоверности

53. Примером какого типа контроля доступа является детекторы движения и камеры наблюдения:
a. Административный
b. Технический
c. Логический
d. Физический

54. Какой из типов аутентификации не относится к методу «Что я знаю»:
a. Пароль
b. Парольная фраза
c. Асинхронный токен
d. Персональная история

55. Какой из типов аутентификации не относится к статическому биометрическому методу:
a. Сетчатка глаза
b. Геометрия ладони
c. Голосовой шаблон
d. Отпечаток пальца

56. В каком ответе содержится правильная последовательность шагов для оценки рисков
a. Идентификация угроз, идентификация уязвимостей, описание характеристик актива, определение последствий

b. Идентификация угроз, идентификация уязвимостей, определение вероятности, определение последствий
c. Оценка рисков, идентификация уязвимостей, определение вероятности, определение последствий
d. Идентификация угроз, подготовка рекомендации, определение вероятности, подготовка отчета

57. Какой из способов является наилучшим для хранения паролей внутри системы:
a. Файл с ограниченным доступом
b. Файл защищенный паролем
c. Обратимая шифрограмма
d. Необратимая шифрограмма

58. Какой из нижеперечисленных способов аутентификации позволяет усилить контроль доступа к системе:
a. Дискретный
b. Двух-факторный
c. Обязательный
d. Разграниченный по времени

59. Что из нижеперечисленного наименее важно для хранения в журналах безопасности:
a. Имя пользователя
b. Идентификатор пользователя
c. Тип события
d. Дата события

60. Что из нижеперечисленного является наиболее слабым звеном в обеспечении информационной безопасности:
a. Контроль доступа
b. Сотрудники
c. Руководство
d. Программы обучения

61. Какие основные знания содержатся в стандарте ISO 27002:
a. Управление информационной безопасностью
b. Рекомендации по разработке программного обеспечения
c. Информация по управлению персональными данными
d. Требования для кредитных организаций по работе с кредитными картами

62. Какой из нижеперечисленных алгоритмов не рекомендуется использовать для шифрования, так как он не является устойчивым к криптоанализу.
a. RSA
b. Diffie-Hellman
c. Merkle-Hellman Knapsack
d. Elgamal

63. В какой из нижеперечисленных режимов шифрования нет вектора инициализации
a. Cipher Block Chaining (CBC)
b. Output Feed Back (OFB)
c. Electronic Code Book (ECB)
d. Cipher Feed Back (CFB)

64. В каком случае удостоверяющий центр должен поместить сертификат в список отозванных сертификатов?
a. Тогда когда у сертификата закончился срок действия
b. В случае если сессионный ключ был скомпрометирован
c. Если сертификат не использовался в течении длительного периода времени
d. Если закрытый ключ владельца сертификата был скомпрометирован

65. Гайдлайны (Guidelines) это:
a. Рекомендации

b. Тоже самое что и стандарты
c. Обязательные к исполнению
d. Части высокоуровневых политик

66. Возможно …
a. Полностью устранить риск
b. Провести полную количественную оценку рисков
c. Провести полную качественную оценку рисков
d. Получить при расчетах отрицательный показатель ARO при качественной оценке.

67. Какая, из нижеперечисленных групп людей составляет наибольшие риски мошенничества и раскрытию конфиденциальной информации
a. Сотрудники
b. Хакеры
c. Внештатные сотрудники
d. Внешние консультанты

68. Кто несет полную ответственность за то что данные классифицированы и защищены?
a. Владельцы данных
b. Пользователи
c. Администраторы
d. Руководство

69. Как посчитать остаточный риск (residual risk)
a. [Угроза] x [Риск] x [Величина актива]
b. ([Угроза] x [Величина актива] x [Уязвимость]) x [Риск]
c. [SLE] x [Частота]
d. ([Угроза] x [Уязвимость] x [Величина актива]) x [Принятые меры]

70. Ценная информация была сохранена на CD-ROM, однако теперь этот носитель данных больше не нужен. Как лучше всего уничтожить информацию?
a. Стереть
b. Уничтожить физически
c. Перезаписать бесполезными данными
d. Размагнитить

71. В какой момент безопасность должна быть включена в проект по разработке ПО.
a. В процессе сбора требований
b. В процессе внедрения
c. В процессе разработки архитектуры
d. В момент финального тестирования

72. Что такое логическая бомба?
a. Это ПО которое перемещает данные с одного компьютера на другой
b. Это ПО которое активируется по какому-нибудь событию или по времени
c. Это самореплицирующиеся ПО
d. Это ПО которое выполняет полезные и вредоносные функции одновременно

73. Эмилия прослушивает сеть с целью перехвата паролей для последующей аутентификации к серверам. Как называется такой тип атаки?
a. Психологическая атака (Social Engineering)
b. Грубая сила (Brute Force)
c. Атака повтором (Replay attack)
d. Атака по словарю (Dictionary attack)

74. Какое утверждение лучше всего описывает процесс создания цифровой подписи.
a. Отправитель зашифровывает хеш-сумму документа своим секретным ключем
b. Отправитель зашифровывает хеш-сумму документа своим открытым ключем

c. Получатель зашифровывает хеш-сумму документа своим секретным ключем
d. Получатель Зашифровывает хеш-сумму документа своим открытым ключем

75. Что из ниже перечисленного не является частью процесса анализа последствий для деятельности (business impact analysis) при планировании неприрывности бизнеса?
a. Параллельное тестирование или тестирование с полным вовлечением.
b. Составление схемы классификации по уровню критичности.
c. Сбор информации с использованием интервью или опросов.
d. Документация бизнес функций.

76. Компания «Roga und Kopyta, ltd, inc, corp» хочет защитить свой логотип от неправомерного использования. Какой тип юридической защиты, из нижеперечисленных подойдет?
a. Патент
b. Copyright
c. Trademark
d. Торговый секрет

77. Какой тип, из нижеперечисленных, программных лицензий предполагает что программное обеспечение продается по сниженным ценам?
a. Shareware
b. Академические
c. Freeware
d. Коммерческие

78. Что из ниже перечисленного не является обязательным шагом для контроля изменений при управлении конфигурациями (Configuration Management)?
a. Проверка и представление
b. Одобрение SLA (Service-level agreement)
c. Отчеты по изменения для руководителей
d. Одобрение изменений

79. Вы восстанавливаете ваш основной офис после разрушительной катастрофы, какие функции должны быть перенесены из временного в основной офис в первую очередь?
a. Менеджмент
b. Наиболее критичные системы
c. Наиболее критичные функции
d. Наименее критичные функции

3. Организационно-педагогические условия реализации программы:

3.1 Материально-технические условия реализации программы:

При чтении лекций используется мультимедийное оборудование, позволяющее демонстрировать презентации в Microsoft Power Point. Практические занятия проходят в специализированных аудиториях, оснащенных компьютерным оборудованием.

3.2 Кадровое обеспечение образовательного процесса по программе:

№	Фамилия, Имя, Отчество	Образование (Вуз; Год окончания; Специальность)	Должность, ученая степень, звание, стаж работы в данной или аналогичной области, лет	Количество научных и учебно-методических публикаций
Руководитель программы				
1	Маховиков Алексей Борисович	Балтийский государственный технический университет; 1994; Системы управления ракетно-космическими объектами и комплексами летательных аппаратов	Декан факультета фундаментальных и гуманитарных дисциплин, к.т.н., доцент, 23 года	Более 180
Профессорско-преподавательский состав программы				
2	Катунцов Евгений Владимирович	Военный университет ПВО (филиал г. Санкт-Петербург), 2002, Радиоэлектронные системы; Санкт-Петербургское высшее военное училище радиоэлектроники (военный институт), 2006, Преподаватель высшей школы	Зам. зав. каф. информатики и компьютерных технологий, к.т.н., инструктор Сетевой Академии Cisco, 15 лет	Более 60
3	Бойков Алексей Викторович	Национальный минерально-сырьевой университет «Горный», 2013, Автоматизация технологических процессов и производств	Ассистент каф. автоматизации технологических процессов и производств, к.т.н., 3 года	Более 40
4	Котелева Наталья Ивановна	Санкт-Петербургский государственный горный институт имени Г.В. Плеханова (технический университет), 2007, Автоматизация технологических процессов и производств	Доцент кафедры автоматизации технологических процессов и производств, к.т.н., 8 лет	Более 50
5	Шарок Вероника Викторовна	Санкт-Петербургский государственный университет; 2006; Психология	Доцент кафедры социологии и психологии, к.псх.н., 7 лет	Более 50

4 Информационное обеспечение программы:

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

Интернет-ресурсы:

1. Электронные материалы Сетевой академии Cisco по курсу Основы Кибербезопасности: https://www.netacad.com/courses