Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
Воронежский государственный архитектурно-строительный университет

УТВЕРЖДАЮ
Директор института магистратуры
_____ Драпалюк Н.А.
«01» 09 **2015 г.**

РАБОЧАЯ ПРОГРАММА

дисциплины

«Хранение и защита информации»

Направление подготовки (специальность) 15.04.04 «Автоматизация технологических процессов и производств»

Профиль подготовки «Проектирование автоматизированных систем управления зданиями и сооружениями»

Квалификация (степень) выпускника «Магистр»

Нормативный срок обучения 2 года

Форма обучения очная

Автор программы д. э. н., профессор _____ / Е.Н.Десятирикова /

Программа обсуждена на заседании кафедры «Автоматизации технологических процессов и производств»

«31» 08 2015 года, протокол № 1/1

Зав. кафедрой, к. т. н., доцент _____ /Белоусов В. Е. /

г. Воронеж – 2015

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Целью дисциплины «Хранение и защита информации» является изучение основных понятий, приемов и методов хранения информации и защиты информации (ЗИ) в управляющих автоматизированных системах, приобретение студентами необходимых теоретических знаний по обеспечению информационной безопасности систем управления. В частности, рассматриваются различные способы защиты автоматизированных систем управления от несанкционированного доступа и различные модели управления доступом к информационным ресурсам, которые используются в современных защищенных системах.

1.2. Задачи освоения дисциплины

При преподавании учебной дисциплины «Хранение и защита информации» ставятся задачи: познакомить студентов с основами технологий хранения информации и обеспечения информационной безопасности (ИБ) и рассмотреть использование этих технологий для построения систем ИБ, снижающих риски, характерные для автоматизированных систем управления сложными техническими комплексами, в том числе, зданиями и сооружениями.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Дисциплина «Хранение и защита информации» относится к обязательным дисциплинам вариативной части учебного плана.

Изучение дисциплины «Хранение и защита информации» проводится в 3 семестре и требует входных знаний, полученных в курсе «Проектирование архитектурно-программных комплексов автоматизированных и автоматических систем управления», «Системы классификации и кодирования в многоуровневых автоматизированных системах управлениях».

Дисциплина « Современные проблемы теории управления » является предшествующей для дисциплины профессионального цикла «Способы сбора и обработки информации в системах автоматизированного управления»

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины «Хранение и защита информации» направлен на формирование следующих профессиональных компетенций:

– способность разрабатывать функциональную, логическую и техническую организацию автоматизированных и автоматических производств, их элементов, технического, алгоритмического и программного обеспечения на базе современных методов, средств и технологий проектирования (ПК-5);

– способность обеспечивать: необходимую жизнестойкость средств и систем автоматизации, контроля, диагностики, испытаний и управления при изменении действия внешних факторов, снижающих эффективность их функционирования, разработку мероприятий по комплексному использованию сырья, замене дефицитных ма-

териалов и изысканию рациональных способов утилизации отходов производства (ПК-7);

– способностью обеспечивать надежность и безопасность на всех этапах жизненного цикла продукции, выбирать системы экологической безопасности производства (ПК-9).

В результате изучения дисциплины студент должен:

Знать: основные понятия информационной безопасности; аксиому и формулировку задачи защиты информации; идеи и концепции ЗИ, угрозы и каналы утечки информации; способы и средства ЗИ.
Владеть современным средствами обеспечения безопасности хранения информации в автоматизированных системах управления.
Уметь проводить сравнительный анализ систем ЗИ; использовать стандарты ЗИ.

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Хранение и защита информации» составляет 4 зачетных единицы, 144 часа.

Вид учебной работы	Всего часов	Семестры
		3
Аудиторные занятия (всего)	36	36
В том числе:		
Лекции	8	8
Практические занятия (ПЗ)	28	28
Лабораторные работы (ЛР)	—	—
Самостоятельная работа (всего)	108	108
В том числе:		
Курсовая работа	—	—
Контрольная работа	—	—
Вид промежуточной аттестации (зачет, экзамен)		Зачет
Общая трудоемкость час	144	144
зач. ед.	4	4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Общие вопросы хранения информации и информационной безопасности	Предмет и задачи курса. Принципы построения защищенной АИС. Модели безопасности Угрозы информационной безопасности
2	Основы формальной теории защиты информации	Основные определения, монитор безопасности обращений, формальные модели управления доступом, несанкционированный доступ
3	Информационная безопасность и защита информации	Угрозы информационной безопасности, каналы утечки, способы и средства ЗИ, политика безопасности, идентификация и аутентификация
4	Криптология, стеганография	Криптография и криптоанализ, стеганография.
5	Стандарты информационной безопасности	Общие сведения. «Оранжевая книга». Общие критерии. Правовые аспекты защиты информации. Доктрина информационной безопасности

5.2 Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№ № разделов данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин				
		1	2	3	4	5
1.	Способы сбора и обработки информации в системах автоматизированного управления			+	+	

5.3. Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекц.	Практ. Зан.	СРС	Всего час
1	Общие вопросы хранения информации и информационной безопасности	1	4	20	25
2	Основы формальной теории защиты информации	1	6	20	27
3	Информационная безопасность и защита информации	2	6	22	30
4	Криптология, стеганография	2	6	24	32
5	Стандарты информационной безопасности	2	6	22	30
	всего	8	28	108	144

5.4. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

- не предусмотрен

5.5. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

№ п/п.	№ раздела дисциплины	Наименование практической работы	Трудоемкость (час)
1.	1	Защита от компьютерных вирусов	4
2.	2	Использование общесистемных и специализированных программных средств для шифрования файлов	6
3.	3	Использование специализированных программ по уничтожению остаточных данных	6
4.	4	Резервирование системных данных	6
5.	5	Защита ОС Windows	6
ИТОГО			28

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ И КОНТРОЛЬНЫХ РАБОТ

- не предусмотрены

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО И ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ЗНАНИЙ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

№ п/п	Компетенция (общекультурная – ОК; профессиональная - ПК)	Форма контроля	семестр
1	ПК-5: способность разрабатывать функциональную, логическую и техническую организацию автоматизированных и автоматических производств, их элементов, технического, алгоритмического и программного обеспечения на базе современных методов, средств и технологий проектирования	Тестирование (Т), Зачет	3
2	ПК-7: способность обеспечивать: необходимую жизнестойкость средств и систем автоматизации, контроля, диагностики, испытаний и управления при изменении действия внешних факторов, снижающих эффективность их функционирования, разработку мероприятий по комплексному использованию сырья, замене дефицитных материалов и изысканию рациональных способов утилизации отходов производства	Тестирование (Т), Зачет	3

3	ПК-9: способностью обеспечивать надежность и безопасность на всех этапах жизненного цикла продукции, выбирать системы экологической безопасности производства.	Тестирование (Т), Зачет	3

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Дескриптор компетенции	Показатель оценивания	Форма контроля	
		Т	Зачет
Знает	основные понятия информационной безопасности; аксиому и формулировку задачи защиты информации; идеи и концепции ЗИ, угрозы и каналы утечки информации; способы и средства ЗИ (ПК-5, ПК-7, ПК-9)	+	+
Умеет	проводить сравнительный анализ систем ЗИ; использовать стандарты ЗИ (ПК-5, ПК-7, ПК-9)	+	+
Владеет	современными средствами обеспечения безопасности хранения информации в автоматизированных системах управления (ПК-5, ПК-7, ПК-9)	+	+

7.2.1.Этап текущего контроля знаний

В третьем семестре результаты текущего контроля знаний оцениваются по четырехбальной шкале с оценками:

- «отлично»;
- «хорошо»;
- «удовлетворительно»;
- «не удовлетворительно».

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
Знает	основные понятия информационной безопасности; аксиому и формулировку задачи защиты информации; идеи и концепции ЗИ, угрозы и каналы утечки информации; способы и средства ЗИ (ПК-5, ПК-7, ПК-9)	отлично	Полное или частичное посещение лекционных и практических занятий, сданные на «отлично» тесты (не менее 90% правильных ответов).
Умеет	проводить сравнительный анализ систем ЗИ; использовать стандарты ЗИ (ПК-5, ПК-7, ПК-9)		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
Владеет	современными средствами обеспечения безопасности хранения информации в автоматизированных системах управления (ПК-5, ПК-7, ПК-9)		
Знает	основные понятия информационной безопасности; аксиому и формулировку задачи защиты информации; идеи и концепции ЗИ, угрозы и каналы утечки информации; способы и средства ЗИ (ПК-5, ПК-7, ПК-9)	хорошо	Полное или частичное посещение лекционных, практических занятий, сданные на «хорошо» тесты (75-90% правильных ответов).
Умеет	проводить сравнительный анализ систем ЗИ; использовать стандарты ЗИ (ПК-5, ПК-7, ПК-9)		
Владеет	современными средствами обеспечения безопасности хранения информации в автоматизированных системах управления (ПК-5, ПК-7, ПК-9)		
Знает	основные понятия информационной безопасности; аксиому и формулировку задачи защиты информации; идеи и концепции ЗИ, угрозы и каналы утечки информации; способы и средства ЗИ (ПК-5, ПК-7, ПК-9)	удовлетворительно	Полное или частичное посещение лекционных и практических занятий, сданные на «удовлетворительно» тесты (50-75% правильных ответов).
Умеет	проводить сравнительный анализ систем ЗИ; использовать стандарты ЗИ (ПК-5, ПК-7, ПК-9)		
Владеет	современными средствами обеспечения безопасности хранения информации в автоматизированных системах управления (ПК-5, ПК-7, ПК-9)		
Знает	основные понятия информационной безопасности; аксиому и формулировку задачи защиты информации; идеи и концепции ЗИ, угрозы и каналы утечки информации; способы и средства ЗИ (ПК-5, ПК-7, ПК-9)	неудовлетворительно	Частичное посещение лекционных и практических занятий, сданные на «неудовлетворительно» тесты (менее 50% правильных ответов).
Умеет	проводить сравнительный анализ систем ЗИ; использовать стандарты ЗИ (ПК-5, ПК-7, ПК-9)		
Владеет	современными средствами обеспечения безопасности хранения информации в автоматизированных системах управления (ПК-5, ПК-7, ПК-9)		
Знает	основные понятия информационной безопасности; аксиому и формулировку задачи защиты информации; идеи и концепции ЗИ, угрозы и каналы утечки информации; способы и средства ЗИ (ПК-5, ПК-7, ПК-9)	не аттестован	Непосещение лекционных и практических занятий.
Умеет	проводить сравнительный анализ систем ЗИ; использовать стандарты ЗИ (ПК-5, ПК-7, ПК-9)		
Владеет	современными средствами обеспечения безопасности хранения информации в авто-		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	матизированных системах управления (ПК-5, ПК-7, ПК-9)		

7.2.2. Этап промежуточного контроля знаний

В третьем семестре результаты промежуточного контроля знаний (зачет) оцениваются по двухбальной шкале с оценками:

- «зачтено»
- «незачтено»:

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
Знает	основные понятия информационной безопасности; аксиому и формулировку задачи защиты информации; идеи и концепции ЗИ, угрозы и каналы утечки информации; способы и средства ЗИ (ПК-5, ПК-, ПК-9)	зачтено	Студент знает программный материал в полном объеме, справляется с выполнением практических заданий. В ответе возможны несущественные ошибки, при указании на которые студент способен их исправить
Умеет	проводить сравнительный анализ систем ЗИ; использовать стандарты ЗИ (ПК-5, ПК-7, ПК-9)		
Владеет	современными средствами обеспечения безопасности хранения информации в автоматизированных системах управления (ПК-5, ПК-7, ПК-9)		
Знает	основные понятия информационной безопасности; аксиому и формулировку задачи защиты информации; идеи и концепции ЗИ, угрозы и каналы утечки информации; способы и средства ЗИ (ПК-5, ПК-7, ПК-9)	незачтено	Студент знаком с программным материалом не в полном объеме, допускает существенные ошибки при ответе на вопрос, не может правильно выполнить практическое задание
Умеет	проводить сравнительный анализ систем ЗИ; использовать стандарты ЗИ (ПК-5, ПК-7, ПК-9)		
Владеет	современными средствами обеспечения безопасности хранения информации в автоматизированных системах управления (ПК-5, ПК-7, ПК-9)		

7.3. Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

Текущий контроль успеваемости осуществляется на практических занятиях: в виде опроса теоретического материла и умения применять его при выполнении практического задания и в виде тестирования по отдельным темам.

7.3.1. Примерные тесты контроля качества усвоения дисциплины

Тест № 1

1. К какой разновидности моделей управления доступом относится модель Белла- ЛаПадулы?

а) модель дискреционного доступа;
б) модель мандатного доступа;
в) ролевая модель.

2. Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т. п.?

3. К каким мерам защиты относится политика безопасности?

а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.

4. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?

а) ACL;
б) списки полномочий субъектов;
в) атрибутные схемы.

5. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?

а) целостность;
б) апеллируемость;
в) доступность;
г) конфиденциальность;
д) аутентичность.

6. К основным принципам построения системы защиты АИС относятся:

а) открытость;
б) взаимозаменяемость подсистем защиты;
в) минимизация привилегий;
г) комплексность;
д) простота.

7. Какие из следующих высказываний о модели управления доступом RBAC справедливы?

а) с каждым субъектом (пользователем) может быть ассоциировано нескольк ролей;
б) роли упорядочены в иерархию;

в) с каждым объектом доступа ассоциировано несколько ролей ;

г) для каждой пары «субъект-объект» назначен набор возможных разрешений.

8. Диспетчер доступа...

а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;

б) ... использует атрибутные схемы для представления матрицы доступа;

в) ... выступает посредником при всех обращениях субъектов к объектам;

г) ... фиксирует информацию о попытках доступа в системном журнале;

9. Какие предположения включает неформальная модель нарушителя?

а) о возможностях нарушителя;

б) о категориях лиц, к которым может принадлежать нарушитель;

в) о привычках нарушителя;

г) о предыдущих атаках, осуществленных нарушителем;

д) об уровне знаний нарушителя.

10. Что представляет собой доктрина информационной безопасности РФ?

а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;

б) федеральный закон, регулирующий правоотношения в области информационной безопасности;

в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;

г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

11. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?

а) политика безопасности верхнего уровня;

б) политика безопасности среднего уровня;

в) политика безопасности нижнего уровня;

г) принцип минимизации привилегий;

д) защита поддерживающей инфраструктуры.

12. Какие из перечисленных ниже угроз относятся к классу преднамеренных?

а) заражение компьютера вирусами;

б) физическое разрушение системы в результате пожара;

в) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

е)вскрытие шифров криптозащиты информации.

Тест № 2

1. Каким образом проникают в систему макровирусы?

а) по электронной почте;

б) любым способом вместе с зараженными ими файлами;

в) злоумышленник должен вручную внести вирус в систему;

г) через Интернет, используя ошибки в сетевых программах;

д) через съемные носители данных при срабатывании автозагрузки с них.

2. Какому требованию должен удовлетворять пароль для противодействия атаке по персональному словарю?

а) при придумывании пароля не должны использоваться личные данные;

б) длина пароля должна составлять 12 и более символов;

в) пароль нельзя открывать никому;

г) разные сервисы должны защищаться разными паролями;

д) пароль должен включать символы разных алфавитов и регистров, цифры, знаки препинания и т. д.

3. Какие недостатки имеют системы обнаружения вторжений, работающие на основе обнаружения аномалий?

а) высокий процент ложных срабатываний;

б) не способны контролировать ситуацию во всей сети;

в) неспособны анализировать степень проникновения;

г) работа затруднена при высокой загрузке сети;

д) снижается эффективность работы сервера, на котором они установлены.

4. ... — канал между двумя узлами, защищенный за счет шифрования проходящего по нему трафика.

5. Как называются вирусы, которые автоматически запускаются в момент старта операционной системы и, таким образом, постоянно функционируют в оперативной памяти?

а) резидентные вирусы;

б) стелс-вирусы;

в) макровирусы;

г) полиморфные вирусы;

д) троянские кони.

6. К какому классу относятся межсетевые экраны, которые отслеживают текущие соединения и пропускают только такие пакеты, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений?

а) Работающие на сетевом уровне;

б) Работающие на сеансовом уровне;

в) Работающие на уровне приложений;

г) Stateless;

д) Stateful.

7. Как называются антивирусы, которые работают резидентно, предотвращая заражение файлов?

а) детекторы;

б) фаги;

в) ревизоры;

г) вакцины;

д) фильтры.

8. Какие вирусы заражают носители данных?

а) файловые вирусы;

б) загрузочные вирусы;

в) макровирусы;

г) сетевые черви;

д) троянские кони.

9. Как называются VPN, с помощью которых на основе ненадёжной сети создается надежная и защищенная подсеть?

а) Внутрикорпоративный;

б) Защищенные;

в) С удаленным доступом;

г) Доверительные;

д) Межкорпоративные.

10. Какому требованию должен удовлетворять пароль для противодействия фишингу?

а) пароль не должен быть производным от слов любого естественного языка;

б) длина пароля должна составлять 12 и более символов;

в) пароль нельзя открывать никому;

г) разные сервисы должны защищаться разными паролями;

д) пароль должен включать символы разных алфавитов и регистров, цифры, знаки препинания и т. д.

11. Что такое VPN?

а) система обнаружения вторжений;

б) протокол обмена ключами;

в) трансляция сетевых адресов;

г) виртуальная частная сеть;

д) протокол защиты передаваемого потока.

12. Каков основной недостаток обнаружения вирусов путем эвристического сканирования?

а) значительная вероятность ложного срабатывания;

б) крайне медленная работа антивируса;

в) невозможность обнаружения новых вирусов;

г)необходимость трудоемкой ручной настройки антивируса.

Тест № 3

1. Чтобы подписать сообщение электронной цифровой подписью, используются:

а) открытый ключ отправителя;

б) открытый ключ получателя;

в) закрытый ключ отправителя;

г) закрытый ключ получателя.

2. Какие утверждения о протоколе строгой двусторонней аутентификации на основе случайных чисел справедливы?

а) в основе протокола лежит симметричный алгоритм шифрования;

б) на первом шаге проверяющий B отправляет проверяемому A случайное число;

в) на втором шаге проверяемый A отправляет проверяющему B зашифрованное сообщение, содержащее полученное на первом шаге случайное число, а также новое случайное число.

г) всего протокол требует отправки двух сообщений.

3. Какова последовательность подписания сообщений с помощью ЭЦП?

а) вычисляется хэш, затем хэш зашифровывается;

б) сообщение зашифровывается, после чего результат хэшируется;

в) при подписании сообщение зашифровывается, при проверке вычисляется хэш;

г) вычисляется хэш исходного сообщения, после чего оно зашифровывается.

4. Линейный конгруэнтный генератор имеет параметры: m = 10, c =7, a = 2, x0 = 5. Каким будет второй член последовательности, выданной с помощью этого генератора?

5. В чем заключается такое свойство функции хэширования H как стойкость к коллизиям первого рода?

а) Для любого хэша h должно быть практически невозможно вычислить или подобрать такое x, что H(x) = h.

б) Должно быть практически невозможно вычислить или подобрать любую пару различных сообщений x и y для которых H(x) = H(y);

в) Длина хэша должна быть фиксированной независимо от длины входного сообщения;

г) Для любого сообщения x должно быть практически невозможно вычислить или подобрать другое сообщение y, такое что H(x) = H(y).

6. Доказательство корректности алгоритма RSA основано на:

а) теореме Эйлера;

б) теореме о сумме эллиптических кривых;

в) китайской теореме об остатках;

г) расширенном алгоритме Евклида.

7. Какими свойствами должен обладать генератор псевдослучайных чисел?

а) недетерминированность;

б) непредсказуемость;

в) независимость очередного элемента от предыдущего;

г) равномерное распределение элементов последовательности;

д) неповторяемость элементов последовательности (в пределах периода).

8. Какие из перечисленных алгоритмов являются алгоритмами электронной цифровой подписи?

а) DES;

б) ГОСТ Р 34.10—2001;

в) ГОСТ Р 34.11—94;

г) RSA.

9. Открытым ключом RSA является пара (15, 2). Зашифруйте число 4.

10. Эллиптическая кривая имеет вид:

а) $y2 = x3 + ax + b \pmod p$;

б) $y3 = x2 + ax + b \pmod p$;

в) $y = x3 + ax2 + b \pmod p$;

г) $x3 = y2 + ax + b \pmod p$.

11. Чтобы расшифровать сообщение с помощью асимметричного алгоритма шифрования используются:

а) открытый ключ отправителя;

б) открытый ключ получателя;

в) закрытый ключ отправителя;

г) закрытый ключ получателя.

12. К какой разновидности протоколов относится протокол опознания пользователя на основе пароля?

а) протокол аутентификации;

б) протокол обмена ключами;

в) протокол одновременной подписи;

г) протокол групповой подписи;

д) протокол голосования.

Тест № 4

1. Какие из этих утверждений, относящихся к шифру Плейфейра, верны?

а) шифр Плейфейера относится к моноалфавитным шифрам;

б) шифр Плейфейера относится к подстановочным шифрам;

в) единицей шифрования в шифре Плейфейера является биграмма;

г) шифр Плейфейера уязвим для взлома методом перебора ключей.

2. Зашифруйте сообщение 01010 скремблером 101 с ключом 011

3. В чем заключается главная слабость моноалфавитного шифра?

а) в небольшом количестве возможных ключей (уязвим к перебору)

б) зашифрованный текст сохраняет статистические особенности открытого текста;

в) если два текста зашифрованы одним и тем же ключом, шифр вскрывается автоматически;

г) противник может узнать ключ, получив достаточное количество образцов открытого и зашифрованного текстов.

4. Зашифруйте слово «КНИГА» шифром Гронсфельда с ключом 12.

5. Зашифруйте слово «КНИГА» шифром Цезаря.

6. Какой метод криптоанализа наиболее эффективен для взлома шифра Хилла?

а) Анализ с избранным текстом;

б) Анализ с избранным зашифрованным текстом;

в) Анализ с избранным открытым текстом;

г) Анализ с известным открытым текстом

д) Анализ только шифрованного текста.

7. Что такое симметричное шифрование?

а) способ шифрования, при котором каждый символ (или последовательность символов) исходного сообщения заменяются другим символом (или другой последовательностью символов);

б) способ шифрования, при котором один и тот же ключ используется и для шифрования и для расшифрования текста;

в) способ шифрования, при котором используются два свзяанных ключа: один для шифрования, другой для расшифрования;

г) способ шифрования, при котором символы открытого текста изменяют порядок следования в соответствии с правилом, которое определяется ключом.

8. Какой из перечисленных шифров является самым надежным?

а) шифр Плейфейера;

б) шифр Хилла;

в) одноразовый блокнот;

г) шифр Цезаря;

д) моноалфавитный шифр.

9. Как называется свойство современных симметричных алгоритмов: каждый бит открытого текста должен влиять на каждый бит зашифрованного текста?

10. В чем заключается основная проблема использования симметричных алгоритмов?

а) Сложность реализации на ЭВМ;

б) Легкость криптоанализа таких шифров с появлением ЭВМ;

в) Трудности при передаче ключей и управлении ими;

г) Работа этих алгоритмов на ЭВМ требует значительных вычислительных ресурсов.

11. Какой метод криптоанализа использует предположение о том, что если выполнить выполнить операцию XOR над некоторыми битами открытого текста, затем над некоторыми битами шифротекста, а затем над результатами, получится бит, который представляет собой XOR некоторых бит ключа?

а) дифференциальный;
б) статистический;
в) линейный.

12. Как называется режим шифрования блочных шифров, при котором текст разбивается на блоки и каждый блок шифруется с одним и тем же ключом?

а) Режим сцепления шифрованных блоков;
б) Режим шифрованной обратной связи;
в) Режим обратной связи по выходу;
г) Режим электронной шифровальной книги.

7.3.2. Примерный перечень вопросов для зачета

1. Международные стандарты информационного обмена. Понятие угрозы.
2. Информационная безопасность в условиях в условиях функционирования в РФ глобальных сетей.
3. Виды противников («нарушителей»).
4. 3 вида возможных нарушений ИС.
5. Назначение и задачи в сфере обеспечения ИБ на уровне государства.
6. Основные положения теории ИБ управляющих автоматизированных систем.
7. Модели безопасности и их применение.
8. Анализ способов нарушений ИБ.
9. Основные технологии построения защищенных управляющих автоматизированных систем.
10. Понятия и методы криптографии.
11. ЭЦП. Понятие, способы получения и основные сферы применения.
12. Концепции ИБ.
13. Эволюция технологии обеспечения безопасности передачи информации
14. Основные определения и классификация методов и средств обеспечения безопасности передачи информации
15. Основные концепции криптографии. Шифрование данных и проблема аутентификации информации
16. Теоретическая и практическая стойкость криптографических алгоритмов
17. Методы криптографической защиты информации
18. Общая характеристика угроз, служб и механизмов безопасности
19. Угрозы безопасности
20. Службы безопасности Механизмы безопасности
21. Компьютерные вирусы и вопросы их нейтрализации

22.Классификация методов шифрования информации
23.Шифры замены
24.Шифры перестановки
25.Блочные составные шифры
26.Абсолютно стойкий шифр. Гаммирование
27.Поточные шифры. Синхронное поточное шифрование
28.Поточные шифры. Самосинхронизирующееся поточное шифрование
29.Модель симметрничной криптосистемы
30.Классификация угроз противника. Основнные свойства криптосистемы
31.Классификация атак на криптосистему с секретным ключом
32.Криптосистема DES
33.Режимы использования блочных шифров
34.Отечественный стандарт криптографиической защиты ГОСТ
35.Криптостстемы с открытым ключом. Односторонние функции
36.Модель криптосистемы с открытым ключом
37.Открытое распределение ключей
38.Электронная подпись
39.Криптосистема RSA
40.Гибридые криптосистемы
41.Криптографические протоколы. Основные понятия
42.Аутентичность. Задача аутентификации информации
43.Имитозащита информации. Контроль целостности потока сообщений
44.Удостоверяющий центр
45.Подделка подписи
46.Файловые системы жестких дисков.
47.Парольная защита ОС Windows.
48.Парольная защита ОС UNIX.
49.Парольная защита ОС Linux.
50.Защита ПК от программных закладок.

7.3.4. Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Общие вопросы хранения информации и информационной безопасности	ПК-5, ПК-7, ПК-9	тестирование(Т-1) Зачет
2	Основы формальной теории защиты информации	ПК-5, ПК-7, ПК-9	тестирование(Т-2) Зачет
3	Информационная безопасность и защита информации	ПК-5, ПК-7, ПК-9	тестирование(Т-3) Зачет
4	Криптология, стеганография	ПК-5, ПК-7, ПК-9	тестирование(Т-4) Зачет
5	Стандарты информационной безопасности	ПК-5, ПК-7, ПК-9	Зачет

7.4. Порядок процедуры оценивания знаний, умений, навыков и (или) опыта деятельности на этапе промежуточного контроля знаний

Зачет может проводиться по итогам текущей успеваемости и (или) путем организации специального опроса, проводимого в устной и (или) письменной форме. Во время проведения зачета обучающиеся могут пользоваться программой дисциплины, а также вычислительной техникой.

8. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), РАЗРАБОТАННОГО НА КАФЕДРЕ

№ п/п	Наименование издания	Вид издания (учебник, учебное пособие, методические указания, компьютерная программа)	Автор (авторы)	Год издания	Место хранения и количество
1					

9. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Подготовка к зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и материал выполненных практических работ.

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

10.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля):

10.1.1 Основная литература:

1) Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Е.Б. Белов [и др.].— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 558 с. http://www.iprbookshop.ru/12014

2) Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с. http://www.iprbookshop.ru/33430

10.1.2 Дополнительная литература:

1) Голиков А.М. Сети и системы радиосвязи и средства их информационной защиты [Электронный ресурс]: учебное пособие/ Голиков А.М.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2007.— 392 с. http://www.iprbookshop.ru/13971

2) Ботуз С.П. Интеллектуальные интерактивные системы и технологии управления удаленным доступом. Методы и модели управления процессами защиты и сопровождения интеллектуальной собственности в сети Internet/Intranet [Электронный ресурс]: учебное пособие/ Ботуз С.П.— Электрон. текстовые данные.— М.: СОЛОН-ПРЕСС, 2014.— 340 с. http://www.iprbookshop.ru/26917

3) Ловцов Д.А. Информационное право [Электронный ресурс]: учебное пособие/ Ловцов Д.А.— Электрон. текстовые данные.— М.: Российская академия правосудия, 2011.— 228 с. http://www.iprbookshop.ru/5786

10.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем:

1. Консультирование посредством электронный почты.
2. Использование презентаций при проведении лекционных занятий.

10.3 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля):

1. Нормативно-правовые и организационные методы обеспечения информационной безопасности при разработке устройств, использующих средства криптозащиты : учебное пособие для вузов : [для студ. 4 курса днев. отд-ния, 4 курса вечер. отд-ния и для магистров 5 курса днев. отд-ния, для специальности 010501 – Прикладная математика и информатика] / Воронеж. гос. ун-т ; сост. : Б. Н. Воронков, А. В. Кузнецов . – Воронеж : ИПЦ ВГУ, 2011. – 135 с. : [текст]. –

(URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m11-01.pdf)

Для работы с электронными учебниками требуется наличие таких программных средств, как Adobe Reader для Windows и DjVuBrowserPlugin.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА:

Для проведения ряда лекционных занятий по дисциплине необходимы аудитории, оснащенные презентационным оборудованием (компьютер с ОС Windows и программой PowerPoint или Adobe Reader, мультимедийный проектор и экран).

Для обеспечения лабораторных занятий требуется компьютерный класс (ауд. 1305) с комплектом лицензионного программного обеспечения (при использовании электронных изданий – компьютерный класс с выходом в Интернет), стенды физического моделирования (ауд. 1308).

12. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ (образовательные технологии)

В соответствии с требованиями стандарта ВПО для формирования компетенций при изучении дисциплины предусматривается широкое использование в учебном процессе активных и интерактивных форм проведения занятий: информационные технологии, исследовательский метод обучения, метод проблемного изложения материала и проблемно-поисковая деятельность.

Лекция – традиционная форма организации учебной работы, несущая большую содержательную, информационную нагрузку. На лекционном занятии преподаватель обозначает основные вопросы темы и далее подробно их излагает, давая теоретическое обоснование определенных положений, а также используя иллюстративный материал. Преподаватель может дать иллюстративный материал (схемы, графики, рисунки и др.) на доске, предложив слушателям занести все это в конспект. Преподаватель должен использовать мультимедийную технику для демонстрации основных определений, понятий, схем. Преподаватель должен общаться с аудиторией вовлекая слушателей в диалог.

Лабораторный практикум ориентирован на практическое изучение основ хранения и защиты информации и их применения в системах и средствах автоматизации управления техническими системами.

Практические занятия имеют целью сформировать у студентов навыки проведения инженерных расчетов в области обеспечения работы с информационной средой функционирования технических систем управления в строительстве и промышленности.

Необходимо, чтобы студенты самостоятельно проводили расчеты и анализ полученных результатов, а отчет по каждой лабораторной работе оформлялся грамотно и аккуратно.

Самостоятельная работа студентов. Все разделы дисциплины с разной степенью углубленности изучения должны рассматриваться на лекционных и практических занятиях. Но для формирования соответствующих компетенций, необходима систематическая самостоятельная работа студента. Самостоятельная работа нужна

как для проработки лекционного (теоретического) материала, так и для подготовки к практическим занятиям, а также и при подготовке к контрольным мероприятиям.

На лекциях особое внимание следует уделять основным понятиям и принципам хранения и защиты информации. Дополнить материал лекций студент должен самостоятельно, пользуясь приведенными выше материалами учебно-методического и информационного обеспечение дисциплины.

Текущий контроль успеваемости осуществляется на лекциях и практических занятиях: в виде опроса теоретического материла и умения применять его к выполнению практических заданий; в виде проверки контрольной работы; в виде тестирования по отдельным темам.

Промежуточный контроль включает зачет и экзамен. Зачет проводится по итогам текущей успеваемости и/или в устной форме, включая подготовку ответа студента на вопросы. Экзамен проводится в форме письменного и устного ответа на билет, содержащий теоретические вопросы. К экзамену и зачету допускаются студенты, полностью выполнившие учебный план дисциплины.

Перечень рекомендуемых оценочных средств для текущего и промежуточного контроля приведен выше в п. 7.

СОГЛАСОВАНИЕ С ВЫПУСКАЮЩЕЙ КАФЕДРОЙ

согласование не требуется

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ПрОПОП ВО по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств

Руководитель основной образовательной программы
профессор, д.т.н., доцент _____ _____ Чепелев С.А.
(занимаемая должность, ученая степень и звание) (подпись) (инициалы, фамилия)

Рабочая программа одобрена учебно-методической комиссией факультета
_____

«01» 03 2015г., протокол № 1.

Председатель

д. т. н., профессор _____ / П.Н. Курочка /
учёная степень и звание, подпись инициалы, фамилия

Эксперт

д. т. н., профессор _____ / А.А. Кононов /
учёная степень и звание, подпись инициалы, фамилия

М.П. организации