Приложение 1

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

ОДОБРЕНО:
Методической комиссией по укрупненным группам специальностей и направлению подготовки 10.00.00- «Информационная безопасность»
Председатель МК
_____ Челехина Б.
подпись ИОФ

УТВЕРЖДАЮ:
Декан, председатель совета факультета Компьютерных технологий, вычислительной техники и энергетики
_____ **Ш.А.Юсуфов**
подпись ИОФ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Управление информационной безопасностью» для контроля знаний обучающихся по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем»

Составитель _____ Г.И.Качаева
подпись ИОФ

Фонд оценочных средств обсужден на заседании выпускающей кафедры ИБ «17.12.2018» от года, протокол №4

Фонд оценочных средств является приложением к рабочей программе по дисциплине С1.Б.32 Управление информационной безопасностью

Зав. кафедрой _____ Г.И.Качаева
подпись ИОФ

Махачкала 2018

Введение

Для проверки знаний составляющей компетенций, формируемых в рамках дисциплины «Управление информационной безопасностью» в фонде оценочных средств предусмотрены:

– вопросы для устного собеседования(опроса).

Для проверки деятельностной составляющей компетенций, формируемых в рамках дисциплины «Управление информационной безопасностью» в фонде оценочных средств размещены:

– профессионально-ориентированные задания.

Конкретные задания, выносимые для проведения текущего контроля и промежуточную аттестации по дисциплине, представлены в отдельном документе «Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации по дисциплине», прилагаемом к рабочей программе.

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Перечень компетенций, на освоение которых направлено изучение дисциплины «Управление информационной безопасностью», с указанием этапов их формирования в процессе освоения образовательной программы, представлен в п.3 настоящей рабочей программы.

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

Показатели и критерии оценивания компетенций, используемые шкалы оценивания

Элементы компетенций (знания, умения, владения)	Показатели оценивания	Критерии оценивания	Средства оценивания	Шкалы оценивания
Знать (ПК-18)	**Знание:** правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в информационных системах, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах. - основные принципы, понятия, факты, законы естественных и математических наук;	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1

Уметь (ПК-18)	**Умение** : -анализировать и оценивать угрозы информационной безопасности объекта; - применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях; - применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации.	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1
Владеть (ПК-18)	**Владение** : - поиска наиболее эффективных путей обработки информации; -методами использования основных положений теории информационной безопасности в различных информационных системах, а также иметь представление о направлении развития и перспективах защиты информации.	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, Промежуточная аттестация: Зачет.	Шкала 2
Знать (ПК-20)	**Знание:** - основные закономерности процесса, возникающие при постановке цели и выборов путей ее достижения в современном мире; - организационные основы, принципы, методы и технологии управления подразделением службы информационной безопасности; - основные методы противодействия «внутренним» угрозам информационной безопасности организации; - архитектуру основных стандартов защиты информации.	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1
Уметь (ПК-20)	**Умение**:- анализировать информационную безопасность многопользовательских систем; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня; - выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования; - использовать методы анализа процессов для определения актуальных угроз организации, методы оценки	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1

	уровня информационной безопасности организации.			
Владеть (ПК-20)	**Владение**: - использования методов построения политики безопасности; - проведения самообследования по информационной безопасности в системе защиты информации на предприятии; - использованием методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации.	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, Промежуточная аттестация: Зачет.	Шкала 2
Знать (ПК-21)	**Знание:** правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в информационных системах, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах. - основные принципы, понятия, факты, законы естественных и математических наук;	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1
Уметь (ПК-21)	**Умение** : -анализировать и оценивать угрозы информационной безопасности объекта; - применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях; - применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации.	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1

Владеть (ПК-21)	**Владение** : - поиска наиболее эффективных путей обработки информации; -методами использования основных положений теории информационной безопасности в различных информационных системах, а также иметь представление о направлении развития и перспективах защиты информации.	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, Промежуточная аттестация: Зачет.	Шкала 2
Знать (ПК-22)	**Знание:** - основные закономерности процесса, возникающие при постановке цели и выборов путей ее достижения в современном мире; - организационные основы, принципы, методы и технологии управления подразделением службы информационной безопасности; - основные методы противодействия «внутренним» угрозам информационной безопасности организации; - архитектуру основных стандартов защиты информации.	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1
Уметь (ПК-22)	**Умение:**- анализировать информационную безопасность многопользовательских систем; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня; - выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования; - использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации.	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1
Владеть (ПК-22)	**Владение:** - использования методов построения политики безопасности; - проведения самообследования по информационной безопасности в системе защиты информации на предприятии; - использованием методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации.	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, Промежуточная аттестация: Зачет.	Шкала 2

Знать (ПК-23)	**Знание:** правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в информационных системах, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах. - основные принципы, понятия, факты, законы естественных и математических наук;	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1
Уметь (ПК-23)	**Умение** : -анализировать и оценивать угрозы информационной безопасности объекта; - применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях; - применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации.	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1
Владеть (ПК-23)	**Владение** : - поиска наиболее эффективных путей обработки информации; -методами использования основных положений теории информационной безопасности в различных информационных системах, а также иметь представление о направлении развития и перспективах защиты информации.	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, Промежуточная аттестация: Зачет.	Шкала 2
Знать (ПК-27)	**Знание:** - основные закономерности процесса, возникающие при постановке цели и выборов путей ее достижения в современном мире; - организационные основы, принципы, методы и технологии управления подразделением службы информационной безопасности; - основные методы противодействия «внутренним» угрозам	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация:	Шкала 1

	информационной безопасности организации; - архитектуру основных стандартов защиты информации.		Зачет.	
Уметь (ПК-27)	**Умение**:- анализировать информационную безопасность многопользовательских систем; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня; - выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования; - использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации.	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1
Владеть (ПК-27)	**Владение**: - использования методов построения политики безопасности; - проведения самообследования по информационной безопасности в системе защиты информации на предприятии; - использованием методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации.	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, Промежуточная аттестация: Зачет.	Шкала 2
Знать (ПК-28)	**Знание:** правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в информационных системах, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах. - основные принципы, понятия, факты, законы естественных и математических наук;	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1

Уметь (ПК-28)	**Умение** *:* -анализировать и оценивать угрозы информационной безопасности объекта; - применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях; - применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации.	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: Зачет.	Шкала 1
Владеть (ПК-28)	**Владение** : - поиска наиболее эффективных путей обработки информации; -методами использования основных положений теории информационной безопасности в различных информационных системах, а также иметь представление о направлении развития и перспективах защиты информации.	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, Промежуточная аттестация: Зачет.	Шкала 2

Описание шкал оценивания степени сформированности элементов компетенций

Шкала 1.Оценка сформированности отдельных элементов компетенций

Обозначения		**Формулировка требований к степени сформированности компетенции**		
Цифр.	Оценка	**Знать**	**Уметь**	**Владеть**
1	Неуд.	Отсутствие знаний	Отсутствие умений	Отсутствие навыков
2	Неуд.	Фрагментарные знания	Частично освоенное умение	Фрагментарное применение
3	Удовл.	Общие, но не структурированные знания	В целом успешное, но не систематически осуществляемое умение	В целом успешное, но не систематическое применение
4	Хор.	Сформированные, но содержащие отдельные пробелы знания	В целом успешное, но содержащие отдельные пробелы умение	В целом успешное, но содержащее отдельные пробелы применение навыков

5	Отл.	Сформированные систематические знания	Сформированное умение	Успешное и систематическое применение навыков

Шкала 2. Комплексная оценка сформированности знаний, умений и владений

Обозначения		**Формулировка требований к степени сформированности компетенции**
Цифр.	Оценка	
1	Неуд.	Не имеет необходимых представлений о проверяемом материале
2	Удовл. или неуд. (*по усмотрению преподавателя)*	Знать на уровне **ориентирования**, представлений. Субъект учения знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает их в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3	Удовл.	Знать и уметь на **репродуктивном** уровне. Субъект учения знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4	Хор.	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5	Отл.	Знать, уметь, владеть на **системном** уровне. Субъект учения знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания учебной дисциплины, его значимость в содержании учебной дисциплины.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Типовые вопросы и задания для текущего контроля(оценка сформированности элементов (знаний, умений) компетенций ПК-22, ОК-8 в рамках текущего контроля по дисциплине) по разделам дисциплины

Примеры вопросов по разделу 1-5:

1. Охарактеризуйте информацию и ее основные показатели.

2. Основные положения закона об информации, информационных технологиях и защите информации.

3. Основные положения закона о государственной тайне.

4. Основные положения закона о защите персональных данных.

5. Основные положения закона об электронной цифровой подписи.

6. Что такое «политика безопасности»?

7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?

8. В каких случаях применяются модели безопасности?

9. Основные модели политик безопасности?

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Процедуры и средства оценивания элементов компетенций по дисциплине «Управление информационной безопасностью».

Процедура проведения	**Средство оценивания**				
	Текущий контроль				Промежуточный контроль
	Выполнение устных заданий	Выполнение письменных заданий	Выполнение практических заданий	Защита лабораторных работ	Экзамен
Продолжительность контроля	По усмотрению преподавателя	По усмотрению преподавателя	По усмотрению преподавателя	По усмотрению преподавателя	В соответствии с принятыми нормами времени
Форма проведения контроля	Устный опрос	Письменный опрос	Письменный опрос	Устная защита	В письменной форме
Вид проверочного задания	Устные вопросы	Письменные задания	Практические задания	Устные вопросы	экзаменационный билет
Форма отчета	Устные ответы	Ответы в письменной форме	Ответы в письменной форме	Ответы в устной форме	Ответы в письменной форме
Раздаточный материал	Нет	Справочная литература	Справочная литература	Справочная литература	Справочная литература

Методические указания для обучающихся по освоению дисциплины

Дисциплина «Управление информационной безопасностью» предусматривает лекции раз в неделю и практические занятия раз в неделю. Изучение дисциплины завершается зачетом. Успешное изучение дисциплины требует посещения лекций, активной работы на практических занятиях, выполнения учебных заданий преподавателя, ознакомления с основной и дополнительной литературой, нормативными правовыми актами и нормативными документами.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на практическое занятие и указания на самостоятельную работу.

При подготовке к лекционным занятиям студентам необходимо:

перед очередной лекцией необходимо просмотреть по конспект материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях.

Практические занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

При подготовке к практическому занятию студенты имеют возможность воспользоваться консультациями преподавателя.

При подготовке к практическим занятиям студентам необходимо:

приносить с собой рекомендованную преподавателем литературу к конкретному занятию;

до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;

при подготовке к практическим занятиям следует обязательно использовать не только лекции, учебную литературу, но и нормативно- правовые акты и материалы правоприменительной практики;

теоретический материал следует соотносить с правовыми нормами, так как в них могут быть внесены изменения, дополнения, которые не всегда отражены в учебной литературе;

в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;

в ходе семинара давать конкретные, четкие ответы по существу вопросов;

на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Студентам, пропустившим занятия (независимо от причин), не имеющие письменного решения задач или не подготовившиеся к данному практическому занятию, рекомендуется не позже чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшейся на занятии. Студенты, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу зачетной сессии, упускают возможность получить положенные баллы за работу в соответствующем семестре.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно– методическое обеспечение самостоятельной работы студентов

Вопросы входного контроля для проверки знаний студентов

1. Информация и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.

3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?

Аттестационная контрольная работа №1

1. Основы построения систем обеспечения информационной безопасности на предприятии.
2. Обеспечение информационной безопасности бизнеса.
3. Система управления информационной безопасностью бизнеса.
4. Анализ объекта защиты.
5. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса.

Аттестационная контрольная работа №2

1. Модель угроз и модель нарушителя.
2. Социальные аспекты системы управления информационной безопасностью бизнеса.
3. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.
4. Оценка рисков информационной безопасности.
5. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.

Аттестационная контрольная работа №3

1. Система управления информационной безопасностью
2. Политика информационной безопасности
3. Управление инцидентами информационной безопасности
4. Инфраструктура информационной безопасности
5. Аудит методов и средств обеспечения информационной безопасности организации

Перечень вопросов на экзамен

1. Основы построения систем обеспечения информационной безопасности на предприятии.
2. Обеспечение информационной безопасности бизнеса.
3. Система управления информационной безопасностью бизнеса.
4. Анализ объекта защиты.
5. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса.
6. Модель угроз и модель нарушителя.
7. Социальные аспекты системы управления информационной безопасностью бизнеса.
8. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.
9. Оценка рисков информационной безопасности.
10. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.
11. Система управления информационной безопасностью.
12. Политика информационной безопасности.
13. Управление инцидентами информационной безопасности.
14. Инфраструктура информационной безопасности.
15. Аудит методов и средств обеспечения информационной безопасности организации.
16. Физическая безопасность и безопасность окружающей среды.

17. Управление доступом к системам.

Вопросы проверки остаточных знаний

18. Система управления информационной безопасностью.
19. Политика информационной безопасности.
20. Управление инцидентами информационной безопасности.
21. Инфраструктура информационной безопасности.
22. Аудит методов и средств обеспечения информационной безопасности организации.
23. Физическая безопасность и безопасность окружающей среды.
24. Управление доступом к системам.

Учебно-методическое и информационное обеспечение дисциплины (модуля) «Управление информационной безопасности»

Рекомендуемая литература и источники информации

№	Виды заня-тий (лк, пр, лб, срс)	Комплект необходимой учебной лит-ры по дисциплинам (наименование учебника, пособия)	Авторы	Издат-во и год издания	Кол-во пособий, учебников и прочей литер-ры	
					в библ	на каф
ОСНОВНАЯ ЛИТЕРАТУРА						
1.	Лк, лб, срс	Теория информации и кодирования	Санников В.Г.	Московский технический университет связи и информатики, 2015.— 95 с	http://www.iprbookshop.ru/61558	
2.	Лк, пр, срс	Информационная безопасность и защита информации	Шаньгин, В. Ф.	Электрон. текстовые дан. – Москва : ДМК Пресс, 2014. – 702 с	http://www.iprbookshop.ru/29257	
3.	Лк, пр, срс	Современные системы управления информационной безопасностью: учебное пособие	А. Ж. Абденов, Г. А. Дронова, В. А.	Новосибирск: Новосибирский государственный технический университет, 2017. — 48 с. — ISBN 978-5-7782-3236-5.	http://www.iprbookshop.ru/91427.html	
4.		Управление информационной безопасностью: учебное пособие	А. К. Шилов	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018. — 120 с. — ISBN 978-5-9275-2742-7.	http://www.iprbookshop.ru/87643.html	
5.		Криптография и безопасность в технологии. NET [Электронный ресурс]	Торстейнсон П., Г.А. Ганеш.	М.: "Лаборатория знаний" (ранее "БИНОМ.Лаборатория знаний"), 2015. — 480 с.	http://e.lanbook.com/books/element.php?pl1_id=70724	
6.		Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие	Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин [и др.].	Воронеж: ВГУИТ (Воронежский государственный университет инженерных технологий), 2013. — 192 с.	http://e.lanbook.com/books/element.php?pl1_id=72884	
7.		Криптографическая защита информации. Учебное пособие [Электронный ресурс]: учебное пособие	Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев.	Спб.: НИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), 2012. — 142 с.	http://e.lanbook.com/books/element.php?pl1_id=40849	
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА						

8.	Лк, лб, срс	Интеллектуальные системы защиты информации [Электронный ресурс]: учебное пособие	Васильев В.И.	М.: Машиностроение, 2013. — 172 с.	http://e.lanbook.com/books/element.php?pl1_id=5792
9.	Лк, лб, срс	Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие	В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин [и др.]	М.: ФЛИНТА, 2011. — 187 с.	http://e.lanbook.com/books/element.php?pl1_id=60717
ИНТЕРНЕТ РЕСУРСЫ					
10.	ЛК,СР, КР	http://kmb.ufoctf.ru/index.html			
11.	ЛК,СР, КР	https://habrahabr.ru/hub/crypto/			
12.	ЛК,СР, КР	http://training.hackerdom.ru/			
13.	ЛК,СР, КР	http://fstec.ru/			
14.	ЛК,СР, КР	www.securitycode.ru - Код безопасности			
15.	ЛК,СР, КР	ru.wikipedia.org - википедия.			
16.	ЛК,СР, КР	www.rsl.ru - российская научная библиотека.			
17.	ЛК,СР, КР	www.iso27000.ru - Искусство управления информационной безопасностью. (Руководящие документы Гостехкомиссии, ФСТЭК, ФСБ).			