

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ
(СамГУПС)

УТВЕРЖДЕНА:

решением Учёного совета СамГУПС
протокол №27 от 22.02.17г.
в составе основной профессиональной
образовательной программы

АКТУАЛИЗИРОВАНА:

решением Учёного совета СамГУПС
протокол Учёного совета СамГУПС № 39 от 05.03.18 г.

решением Учёного совета СамГУПС
протокол Учёного совета СамГУПС № 50 от 27.03.19г.

решением Учёного совета СамГУПС
протокол Учёного совета СамГУПС № 59 от 25.02.20г.

решением Учёного совета СамГУПС
протокол Учёного совета СамГУПС № ____ от __.__.____г.

Защита информации

рабочая программа дисциплины

Кафедра **Мехатроника, автоматизация и управление на транспорте**

Направление подготовки **09.03.01 Информатика и вычислительная техника**

Направленность
(профиль)

Квалификация **бакалавр**

Форма обучения **очная**

Объем дисциплины **2 ЗЕТ**

Самара 2017

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цели освоения дисциплины (модуля)

Дисциплина Защита информации имеет своей целью: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах

1.2 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

ОПК-1 способностью устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем

Знать:

Уровень 1 (базовый)	основы построения и архитектуры ЭВМ.
Уровень 2 (продвинутый)	Современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и кодирования;
Уровень 3 (высокий)	Состав и организацию программных и аппаратных средств обеспечения информационной безопасности;

Уметь:

Уровень 1 (базовый)	инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем.
Уровень 2 (продвинутый)	конфигурировать программные и аппаратные средства защиты информации
Уровень 3 (высокий)	проектировать и создавать программное и организационное обеспечение для защиты информации

Владеть:

Уровень 1 (базовый)	навыками работы с различными операционными системами и их администрирования; навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств.
Уровень 2 (продвинутый)	навыками практического использования программных и аппаратных средств защиты информации
Уровень 3 (высокий)	навыками организации профилактических осмотров и текущего ремонта вычислительных систем; выполнения приемки и освоения вводимых средств вычислительной техники.

ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знать:

Уровень 1 (базовый)	сущность и значение информации в развитии общества; основы функционирования глобальных сетей.
Уровень 2 (продвинутый)	основные регламентирующие правовые акты в области защиты информации
Уровень 3 (высокий)	методы и средства обеспечения информационной безопасности компьютерных систем

Уметь:

Уровень 1 (базовый)	Использовать нормативные правовые акты и регламентирующие документы в области информационной безопасности для классификации информационных систем с точки зрения информационной безопасности
Уровень 2 (продвинутый)	Использовать средства защиты информации при разработке и эксплуатации информационных систем
Уровень 3 (высокий)	применять на практике методы обеспечения конфиденциальности, целостности, доступности компьютерной информации;

Владеть:

Уровень 1 (базовый)	навыками соблюдения требований информационной безопасности; навыками использования информации, полученной из сети Интернет.
Уровень 2 (продвинутый)	Навыками выбора средств и методов обеспечения информации для конкретных задач
Уровень 3 (высокий)	навыками оценки эффективности систем защиты информации в компьютерных системах

1.3. Результаты обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

Знать:

– правовые основы защиты компьютерной информации, организационные, технические и программные методы и средства защиты информации в АСОИУ и ИС, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; иметь представление о направлениях развития и перспективах защиты информации;

Уметь:

– применять методы защиты компьютерной информации при проектировании и эксплуатации АСОИУ и ИС в различных предметных областях;

Иметь навыки:																									
установки и настройки программного обеспечения, применяемого для защиты АСОИУ и ИС от несанкционированного доступа, как из сетей общего пользования, так и внутренних сетей предприятия.																									
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ																									
														Наименование дисциплины								Коды формируемых компетенций			
2.1. Осваиваемая дисциплина																									
Б1.Б.21		Защита информации														ОПК-1 ОПК-5									
2.2 Предшествующие дисциплины																									
Б1.Б.11		Информатика														ОПК-1 ОПК-5									
Б1.В.01		Математическая логика и теория алгоритмов														ОПК-2 ДПК-4									
Б1.В.06		Дискретная математика														ОПК-2 ДПК-4									
Б1.В.ДВ.13.02		Теория информации														ДПК-2 ДПК-4									
Б1.Б.16		Операционные системы														ОПК-1 ПК-2									
2.3 Осваиваемые параллельно дисциплины																									
2.4 Последующие дисциплины																									
Б2.В.02(П)		Производственная (практика по получению профессиональных умений и опыта профессиональной деятельности, в том числе технологическая)														ОК-5 ОПК-2 ДПК-1, ПК-2									
Б2.В.03(П)		Производственная (научно-исследовательская работа)														ОК-7 ОПК-4 ПК-3									
Б2.В.04(Пд)		Преддипломная практика														ДПК-2; ДПК-5; ОК-6; ОК-7; ОПК-1; ОПК-2; ОПК-4; ПК-2; ПК-3									
Б3.Б.01		Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты														ДПК-1; ДПК-2; ДПК-3; ДПК-4; ДПК-5; ОК-1; ОК-2; ОК-3; ОК-4; ОК-5; ОК-6; ОК-7; ОК-8; ОК-9; ОПК-1; ОПК-2; ОПК-3; ОПК-4; ОПК-5; ПК-2; ПК-3									
3. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ																									
3.1 Объем дисциплины (модуля)														2 ЗЕТ											
3.2 Распределение академических часов по семестрам (для офо)/курсам(для зфо) и видам учебных занятий																									
Вид занятий		№ семестра (для офо) / курса (для зфо)																							
		1		2		3		4		5		6		7		8		9		10		Итого			
		УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД		
Контактная работа:																32	32					32	32		
<i>Лекции</i>																16	16					16	16		
<i>Лабораторные</i>																16	16					16	16		
<i>Практические</i>																									
<i>Консультации</i>																									
<i>Инд. работа</i>																									
Контроль																									
Сам. работа																40	40					40	40		
ИТОГО																72	72					72	72		
3.3. Формы контроля и виды самостоятельной работы обучающегося																									
Форма контроля		Семестр (офо)/ курс(зфо)		Нормы времени на самостоятельную работу обучающегося																					
				Вид работы									Нормы времени, час												
Экзамен		8		Подготовка к лекциям									0,5 часа на 1 час аудиторных занятий												
Зачет				Подготовка к практическим/ Подготовка к зачету									1 час на 1 час аудиторных занятий 9 часов (офо)												
Курсовой проект				Выполнение курсового проекта									72 часа												
Курсовая работа				Выполнение курсовой работы									36 часов												
Контрольная работа				Выполнение контрольной работы									9 часов												
РГР				Выполнение РГР									18 часов												

Реферат/эссе		Выполнение реферата/эссе	9 часов
--------------	--	--------------------------	---------

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем	Вид занятия	Семестр / курс	К-во ак. часов	Компетенции	Литература	Часы в интерактивной форме	
							К-во ак. часов	Форма занятия
1	Раздел 1. Политика безопасности. Угроза безопасности. Нарушители.							
1.1	Основные проблемы компьютерной безопасности. Модели безопасности	Лек	8/4	2	ОПК-1 ОПК-5 Э1, Э2	Л1.1, Л1.2 Л2.2, Л2.3, Л2.4 Л2.5, Э1, Э2	2	лекция с применением видео- и аудиоматериалов
1.2	Установка паролей в Microsoft Office.	Лаб	8/4	4	ОПК-1 ОПК-5	Л1.1Л1.2 Л2.2 Л2.3 Л2.4 Л2.5М1 Э1, Э2		
1.3	Нарушители. Неформальная модель нарушителя в автоматизированной системе.	Ср	8/4	7	ОПК-1 ОПК-5	Л1.1 Л1.2Л2.2 Л2.3 Л2.4 Л2.5		
1.4	Управление доступом.	Лек	8/4	2	ОПК-1 ОПК-5	Л1.1 Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Э1, Э2	2	лекция с применением видео- и аудиоматериалов
2	Раздел 2. Модели защиты информации							
2.1	Модели секретности. Дискреционный контроль и управление доступом.	Лек	8/4	2	ОПК-1 ОПК-5	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5		
2.2	Изучение журналов просмотра событий ОС Windows 8.1	Лаб	8/4	4	ОПК-1 ОПК-5	Л 2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1, Э2		
2.3	Неформальное и формальное описание политики безопасности.	Лак	8/4	2	ОПК-1 ОПК-5	Л1.1 Л1.2 Л2.1. Л2.2 Л2.3 Л2.4 Л2.5		
2.4	Модели мондатного контроля и управления доступом. Контроль доступа базирующийся на ролях. Пользователи роли и операции	Лек.	8/4	2	ОПК-1 ОПК-5	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	2	лекция с применением видео- и аудиоматериалов
2.5.	Контроль доступа базирующийся на ролях. Пользователи роли и операции	Ср	8/4	2	ОПК-1 ОПК-5	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5		
2.6	Изучение структуры назначения привилегий в Windows/	Лаб	8/4	4	ОПК-1 ОПК-5	Л2.1.Л2.2 Л2.3 Л2.4 Л2.5 М1 Э1 Э2		
2.7	Модель китайской стены. Модели секретности.	Ср.	8/4	10	ОПК-1 ОПК-5	Л2.1 Л2.2 Л2.3 Л2.4 Л2.5		
3	Раздел 3. Модели целостности и доступности информации.							

3.1	Модель целостности Кларка Вильсона. Модель Липкера.	Лек	8/4	2	ОПК-1 ОПК-5	Л2.1 Л2.2 Л2.3 Л2.4 Л2.5		
3.2	Идентификация и аутентификация	Ср	8/4	4	ОПК-1 ОПК-5	Л2.1 Л2.2 Л2.3 Л2.4 Л2.5		
3.3	Реализация аудита в Windows. Уязвимость, атаки и вторжения.	Лек	8/4	2	ОПК-1 ОПК-5	Л2.1 Л2.2 Л2.3 Л2.4 Л2.5		
3.4	Работа с наиболее популярными антивирусными пакетами	Лаб	8/4	4	ОПК-1 ОПК-5	М1 Л2.2 Л2.3 Л2.4 Л2.5 Э1 Э2		
4	Раздел 4. Криптографические методы.							
4.1	Основные понятия криптологии. Криптографические системы DES. ГОСТ.	Лек	8/4	2	ОПК-1 ОПК-5	Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	1	лекция с применением видео- и аудиоматериалов
4.2	Модель невмешательства и модель невыводимости	Ср	8/4	8	ОПК-1 ОПК-5	Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	1	лекция с применением видео- и аудиоматериалов
	Раздел 5. Проверка знаний							
5.1	Подготовка к зачету	Ср	8/4	9	ОПК-1 ОПК-5	Л1.1 Л1.2 Л2.1, Л2.2 Л2.3 Л2.4 Л2.5 М1		

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

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

Основными этапами формирования компетенций в рамках дисциплин выступает последовательное изучение содержательно связанных между собой разделов (тем учебных занятий), которые отражены в разделе 4.

Матрица оценки результатов обучения по дисциплине

Код компетенции	Планируемые результаты обучения (показатели оценивания компетенций)	Оценочные средства/формы контроля		
		Отчет по лаб. раб.	Тестирование	Зачет
ОПК-1	Знает	+	+	+
	умеет	+	+	+
	владеет	+	+	+
ОПК-5	знает	+	+	+
	умеет	+	+	+
	владеет	+	+	+

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

Критерии формирования оценок по зачету

«Зачтено» - обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки, освоил вопросы практического применения полученных знаний, не допустил фактических ошибок при ответе, достаточно последовательно и логично излагает теоретический материал, допуская лишь незначительные нарушения последовательности изложения и некоторые неточности.

«Не зачтено» - выставляется в том случае, когда обучающийся демонстрирует фрагментарные знания основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. У экзаменуемого слабо выражена способность к самостоятельному аналитическому мышлению, имеются затруднения в изложении материала, отсутствуют необходимые умения и навыки, допущены грубые ошибки и незнание терминологии, отказ отвечать на дополнительные вопросы, знание которых необходимо для получения положительной оценки

Критерии формирования оценок по выполнению лабораторных работ

«Зачтено» – ставится за работу, выполненную полностью без ошибок и недочетов в соответствии с заданием, выданным для выполнения лабораторной работы. Обучающийся полностью владеет информацией о нормативных документах, регулирующих хозяйственные процессы в организации; на основании данных о финансовой деятельности может решить все поставленные в задании задачи.

«Не зачтено» - ставится за работу, если обучающийся правильно выполнил менее 2/3 всей работы, использовал при выполнении работы устаревшую нормативную базу, в качестве исходных данных выступили данные учебника, а не реальной организации.

Критерии формирования оценок по выполнению тестовых заданий

«Отлично» (5 баллов) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 100 – 90% от общего объема заданных тестовых вопросов.

«Хорошо» (4 балла) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 89 – 70% от общего объема заданных тестовых вопросов.

«Удовлетворительно» (3 балла) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 69 – 60% от общего объема заданных тестовых вопросов.

«Неудовлетворительно» (0 баллов) - получают обучающиеся с правильным количеством ответов на тестовые вопросы – 59% и менее от общего объема заданных тестовых вопросов.

5.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Вопросы к зачету

1. Деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации
2. Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства
3. Информация, для которой установлен специальный режим сбора, хранения, обработки, распространения и использования
4. Перечислить виды информации с ограниченным доступом
5. Перечислить сведения, составляющие государственную тайну и имеющие гриф секретности
6. Дать определение конфиденциальной информации
7. Какие виды защиты имеются от утечки
8. Как определяется степень соответствия результатов защиты информации поставленной цели защиты информации
9. Определить длину ключевого элемента в алгоритме шифрования DES
10. Чем определяется количество циклов шифрования в алгоритме DES
11. Определить объем ключа в алгоритме DES
12. Определить длина ключевого элемента в ГОСТ блочного шифрования
13. Определить количество циклов шифрования в ГОСТ блочного шифрования
14. Определить объем ключа в ГОСТ блочного шифрования
15. Какие преобразования лежат в основе композиционных блочных шифров
16. В каких криптосистемах открытый ключ и криптограмма могут передаваться по незащищенным каналам
17. Чему должны принадлежать в криптосистемах RSA открытый ключ, секретный ключ, сообщение и криптограмма
18. Как вычисляется секретный ключ в криптосистеме RSA
19. Какой алгоритм применяется для вычисления секретного ключа в криптосистеме RSA
20. Как определяется проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности
21. Определить функцию, осуществляющую отображение элементов некоторого множества в индекс линейного множества
22. Что включает в себя система электронной цифровой подписи
23. Что используется в качестве подписываемого документа
24. Что используется для сжатия подписываемого документа до нескольких десятков или сотен бит
25. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

Тестовые задания

Тестирование по дисциплине проводится с использованием ресурсов электронной образовательной среды «Moodle» (режим доступа: <http://do.samgups.ru/moodle/>)

5.4 Методические материалы, определяющие процедуры оценивания

Описание процедуры оценивания «Тестирование»

Тестирование по дисциплине проводится с использованием ресурсов электронной образовательной среды «Moodle» (режим доступа: <http://do.samgups.ru/moodle/>). Количество тестовых заданий и время задается системой. Во время проведения тестирования обучающиеся могут пользоваться программой дисциплины, справочной литературой, калькулятором. Результат каждого обучающегося оценивается в соответствии с универсальной шкалой, приведенной в пункте 5.2.

Описание процедуры оценивания «Защита отчета по лабораторным работам»

Оценивание итогов лабораторной работы проводится преподавателем, ведущим лабораторные работы.

По результатам проверки отчета по лабораторной работе обучающийся допускается к его защите при условии соблюдения перечисленных условий:

- выполнены все задания;
- отсутствуют ошибки;
- оформлено в соответствии с требованиями.

В том случае, если содержание отчета не отвечает предъявляемым требованиям, то он возвращается автору на доработку. Обучающийся должен переделать отчет с учетом замечаний. Если сомнения вызывают отдельные аспекты отчета, то в этом случае они рассматриваются во время устной защиты.

Защита отчета по лабораторной работе представляет собой устный публичный отчет обучающегося о результатах выполнения, ответы на вопросы преподавателя.

Ответ обучающегося оценивается преподавателем в соответствии с критериями, описанными в пункте 5.2

Описание процедуры оценивания «Зачет»

Зачет проводится в форме устного ответа на вопросы билета. При проведении зачета в форме устного ответа на вопросы билета обучающемуся предоставляется 20 минут на подготовку. Опрос обучающегося по билету не должен превышать 0,25 часа. Ответ обучающегося оценивается в соответствии с критериями, описанными в пункте 5.2.

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

6.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Кол-во
Л1.1	А. А. Корниенко	Информационная безопасность и защита информации на железнодорожном транспорте. В 2 ч. Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте [Текст] : учебник для вузов / рек. Минобрнауки России	Москва: УМЦ по образованию на железнодорожном транспорте, 2014.	20
Л1.2	А. А. Корниенко	Информационная безопасность и защита информации на железнодорожном транспорте. В 2 ч. Ч. 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте [Текст] : учебник для вузов / рек. Минобрнауки России ; под ред. -	Москва : УМЦ по образованию на железнодорожном транспорте, 2014.	20

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Кол-во
Л2.1	С.С.Корт	Теоретические основы защиты информации: учебное пособие	М: "Гелиос АРВ", 2004	10
Л2.2	Ю. А. Родичев	Компьютерные сети. Нормативно-правовые аспекты информационной безопасности. Ч. 1 [Текст] : учеб. пособие для вузов /	Самара : Универс-групп, 2007. - 344 с.	30
Л2.3	П. Б. Хорев ; -	Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие для вузов	рек. УМО вузов по унив. политехн. образов. - 3-е изд., стереотип. - М. : Академия, 2007. - 256 с.	9
Л2.4	В. И. Ярочкин	Информационная безопасность [Текст] : учебник для вузов	М-вом образ. РФ. - 5-е изд. - М. : Академ. Проект, 2008. - 544 с.	1
Л2.5	Ю. А. Родичев	Информационная безопасность: нормативно-правовые аспекты	СПб. : Питер, 2008. - 272 с	3

6.2 Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Кол-во
--	---------------------	----------	-------------------	--------

М1	Д. К. Тюмиков	Защита информации в WINDOWS Методические указания к выполнению лабораторных работ по дисциплине «Защита информации» для обучающихся по направлению подготовки 09.03.01 ИВТ, очной формы обучения.	Самара: СамГУПС, 2015.-30 с.	
-----------	---------------	---	------------------------------	--

6.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

	Наименование ресурса	Эл.адрес
Э1	Дистанционные образовательные ресурсы СамГУПС	http://do.samgups.ru/moodle/
Э2	Рекомендуемые поисковые системы	http://www.yandex.ru/ , http://www.google.ru/ , http://www.google.com/

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для освоения дисциплины «Защита информации» обучающемуся необходимо: выполнять лабораторные задания; успешно пройти все формы текущего контроля; успешно пройти промежуточную аттестацию (вопросы прилагаются п.6.4).

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа обучающихся, которая может осуществляться как индивидуально, так и под руководством обучающего. Данная работа предполагает самостоятельное изучение обучающимся отдельных тем, дополнительную подготовку к каждому лабораторному занятию.

Самостоятельная работа обучающихся является важной формой образовательного процесса. Она реализуется вне рамок расписания, а также в библиотеке, дома, при выполнении учебных задач.

Цель самостоятельной работы - научить обучающегося осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы повысить уровень освоения компетенций, а также привить умение в дальнейшем непрерывно повышать свою квалификацию.

8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Размещение учебных материалов в разделе «Защита информации» системы обучения Moodle: <http://do.samgups.ru/moodle/>

8.1 Перечень программного обеспечения и информационных справочных систем

8.1.1	Лицензионное ПО: Windows XP
8.1.2	АИС ДО MOODLE

9. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Лекционная аудитория (20 и более посадочных мест) и аудитория для проведения лабораторных занятий (25 и более посадочных мест) оборудованные учебной мебелью; неограниченный доступ к электронно-библиотечным системам (через ресурсы библиотеки СамГУПС), к электронной информационно-образовательной среде moodle и к информационно-телекоммуникационной сети «Интернет» в рамках самостоятельной работы обучающегося.

Для проведения лабораторных работ по дисциплине «Защита информации» необходимо: мультимедийное оборудование (проектор, экран, ноутбук или компьютер).