Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Пермский национальный исследовательский
политехнический университет»**

Лысьвенский филиал
(ЛФ ПНИПУ)

Специальность 09.02.01 Компьютерные системы и комплексы

УТВЕРЖДАЮ
Проректор по учебной работе
д.т.техн. наук
_____ П.В. Лобов
«___» _____ 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

Форма обучения - очная

Закреплена за ПЦК: естественнонаучных дисциплин

Курс: 3 **Семестр**: 6

Трудоёмкость:

Максимальная учебная нагрузка студента: 64 часа

Виды контроля:

Дифференцированный зачёт 6 семестр

Лысьва, 2016

Рабочая программа учебной дисциплины «Защита информации» разработана на основании:

– Федерального государственного образовательного стандарта среднего профессионального образования, утвержденного приказом Министерства образования и науки Российской Федерации «28» июля 2014 г. № 849 номер Государственной регистрации «33748» по специальности 09.02.01 Компьютерные системы и комплексы;

– Базисного учебного плана очной формы обучения по специальности 09.02.01 Компьютерные системы и комплексы, утвержденного «28» апреля 2016 г.

Разработчик:
преподаватель 1 категории Е.Л. Федосеева

Рецензент:
канд.тех.наук, кафедры ИТАС ПНИПУ А.Л. Погудин

Рабочая программа рассмотрена и одобрена на заседании предметной (цикловой) комиссии естественнонаучных дисциплин (ПЦК ЕНД) «07» сентября 2016 г., протокол № 01.

Председатель ПЦК ЕНД Е.Л. Федосеева

Рабочая программа одобрена методическим советом ЛФ ПНИПУ «26» 09 2016 г., протокол № 01.

Заведующий кафедрой,
ведущей дисциплину
канд. физ.-мат. наук, доц. И.Т. Мухаметьянов

СОГЛАСОВАНО
Заместитель начальника УОП ПНИПУ В.А. Голосов

Заместитель директора по УР ЛФ ПНИПУ
канд.пед.наук Н.Н. Третьякова

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

1.1 Область применения программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.01 Компьютерные системы и комплексы. Квалификация выпускника – техник по компьютерным системам.

1.2 Место учебной дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина Защита информации относится к общепрофессиональным дисциплинам профессионального цикла вариативной части ФГОС по специальности СПО 09.02.01 Компьютерные системы и комплексы. Предшествующими дисциплинами и междисциплинарными курсами (МДК) являются Информационные технологии, МДК.04.01 Практикум по рабочей профессии. Знания и умения, полученные при изучении дисциплины Защита информации, могут быть использованы при подготовке выпускной квалификационной работы.

1.3 Цели и задачи дисциплины – требования к результатам освоения учебной дисциплины:

Целью изучения учебной дисциплины является изучение методов и средств защиты информации, исключающих несанкционированный доступ к информации, хранящейся и обрабатываемой в ЭВМ, обеспечение информационной безопасности организации, обеспечение комплексной защиты объектов информации от различных угроз

Задачи освоения учебной дисциплины:

- освоение криптографических методов и средств защиты компьютерной информации;
- изучение методов защиты программ от несанкционированного доступа;
- изучение принципов построения комплексных систем защиты.

2 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Учебная дисциплина обеспечивает расширение и углубление части компетенций:

2.1 Требования к компонентному составу компетенций

Формулировка компетенции	Перечень компонентов
Техник по компьютерным системам должен обладать общими компетенциями, включающими в себя способность: ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	В результате освоения дисциплины студент (З1) Знает значение и место защита информации в своей будущей профессии
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	(У1) Умеет организовывать и проводить самооценку выполненных внеаудиторных самостоятельных работ по дисциплине
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	(У2) Умеет принимать решения в стандартных и нестандартных ситуациях в области защиты информации
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	(У3) Умеет формировать отчётные документы по выполненным внеаудиторным самостоятельным работам по дисциплине
ОК 5. Владеть информационной культурой, анализировать и оценивать информацию с использованием информационно-коммуникационных технологий	(У4) Умеет использовать информационно-коммуникационных технологий в области защиты информации
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями	(У5) Умеет организовать управленческую деятельность в коллективе
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий	(У6) Умеет брать ответственность за результаты коллективного труда в области защиты информации
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	(У7) Умеет самостоятельно заниматься самообразованием в области защиты информации
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности	(З2) Знает новые методы защиты информации в профессиональной деятельности

2.2 Дисциплинарная карта компетенции ПК 1.5

Формулировка компетенции	Формулировка дисциплинарной части компетенции
ПК 1.5. Выполнять требования нормативно-технической документации	ПК 1.5.ОП. 11. Выполнять требования нормативно-технической документации в области защиты информации

Требования к компонентному составу части компетенции ПК 1.5.ОП.11

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения дисциплины студент **знает:** – (З3) основные правовые понятия, законодательные акты и др. нормативные документы в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации; – (З4) методы и формы защиты информации; – (З5) виды и методы дестабилизирующего воздействия на защищаемую информацию **умеет:** – (У8) производить классификацию конфиденциальной информации по видам тайны и степени конфиденциальности; – (У9) оценивать степень угрозы конфиденциальной информации; – (У10) использовать методы шифрования	Теоретическое обучение. Самостоятельная работа студентов по изучению теоретического материала и по подготовке к дифференцированному зачёту Практические занятия. Самостоятельная работа студентов по изучению теоретического материала и подготовки к дифференцированному зачёту	Устный опрос. Тестирование. Вопросы к дифференцированному зачёту Защита отчётов по практическим занятиям. Тестирование. Выполнение индивидуального задания Вопросы к дифференцированному зачёту

3 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

3.1 Объём учебной дисциплины и виды учебной работы

Вид учебной работы	***Объём часов***
Максимальная учебная нагрузка (всего)	***64***
Обязательная аудиторная учебная нагрузка (всего)	***42***
в том числе:	
теоретическое обучение	***30***
лабораторные занятия	***-***
практические занятия	***12***
контрольные работы	***-***
курсовая работа (проект)	***-***
Самостоятельная работа обучающегося (всего)	***22***
в том числе:	
работа с конспектом лекций, учебным материалом	***16***
подготовка отчётов по практическим занятиям и их защита	***6***
Итоговая аттестация в форме дифференцированного зачёта	

3.2 Тематический план и содержание учебной дисциплины Защита информации

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа обучающегося	Объём часов	Уровень освоения
1	*2*	*3*	*4*
Введение	Цели и задачи курса. Общие проблемы безопасности. Роль и место информационной безопасности. История развития информационной безопасности. Перспективы и тенденции развития информационной безопасности. Основные области применения информационной безопасности. Необходимость обеспечения защиты информации	1	*1*
	Самостоятельная работа студентов Подготовить конспект по теме «Основные области применения информационной безопасности»	1	
Модуль 1	**Основные положения компьютерной безопасности**	**16**	
Раздел 1. Основные положения компьютерной безопасности		**16**	
Тема 1.1 Основные понятия и определения компьютерной безопасности	Основные понятия и определения компьютерной безопасности (политика безопасности, модели безопасности основных ОС, управление доступом, идентификация, аутентификация, адекватность, таксономия систем защиты, защита информации в сетях и др.). Угрозы безопасности компьютерных систем. Виды противников или «нарушителей»	1	*1*
	Самостоятельная работа студентов Подготовить словарь терминов	1	
Тема 1.2 Общие проблемы безопасности	Общие проблемы безопасности. Информационная безопасность в России в целом, а также в условиях функционирования глобальных сетей, в частности. Источники, риски и формы атак на информацию	1	*3*
	Практическое занятие № 1 Криптографические методы защиты информации	4	
	Самостоятельная работа студентов Подготовка отчёта по практическому занятию и его защита	2	
Тема 1.3 Требования к системе защиты информации	Виды вирусов и другого зловредного кода. Антивирусное программное обеспечение. Требования к системам защиты информации	1	*3*
	Практическое занятие № 2 Программы защиты от компьютерных вирусов	4	
	Самостоятельная работа студентов Подготовка отчёта по практическому занятию и его защита	2	
Модуль 2	**Нормативное обеспечение компьютерной безопасности**	**10**	
Раздел 2. Нормативное обеспечение компьютерной безопасности		**10**	

Тема 2.1 Международные стандарты компьютерной безопасности	Международные стандарты компьютерной безопасности (Критерии безопасности компьютерных систем министерства обороны США — «Оранжевая книга»; «Европейские критерии безопасности информационных технологий»). Руководящие документы Гостехкомиссии РФ	2	*2*
	Международные стандарты компьютерной безопасности («Федеральные критерии безопасности информационных технологий»; «Канадские критерии безопасности компьютерных систем»; «Единые критерии безопасности информационных технологий» и др.)		
	Самостоятельная работа студентов Подготовить конспект по теме «Единые критерии безопасности информационных технологий»	1	
Тема 2.2 Обеспечение компьютерной безопасности на уровне государства	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы («О государственной тайне», «О безопасности», «О федеральных органах правительственной связи и информации в РФ», «Об информации, информатизации и защите информации», др.). Назначение и задачи в сфере обеспечения компьютерной безопасности на уровне государства	2	*2*
	Самостоятельная работа студентов Изу́чить основные Федера́льные законы по ко́мпьютерной безопа́сности	2	
Тема 2.3. Виды нарушений компьютерной системы	Инвентаризация информационных систем. Классификация информационных систем. Модель информационных потоков. Три вида возможных нарушений компьютерной системы (угроза нарушения конфиденциальности; угроза нарушения целостности; угроза отказа служб). Защита от возможных нарушений	2	*2*
	Самостоятельная работа студентов Подготовить конспект по теме «Защита от возможных нарушений»	1	
Модуль 3.	**Основы обеспечения компьютерной безопасности**	**14**	
Раздел 3. Основы обеспечения компьютерной безопасности		**14**	
Тема 3.1 Формальные модели безопасности и их применение	Формальные модели безопасности и их применение: дискреционная модель Харрисона-Руззо-Ульмана; типизированная матрица доступа (TAM, HRU); мандатная модель Белла-ЛаПадула; модель безопасности информационных потоков; ролевая политика безопасности	2	*1*
	Самостоятельная работа студентов Подготовить конспект по теме «Ролевая политика безопасности»	1	

Тема 3.2 Нарушения компьютерной безопасности вычислительной системы	Таксономия нарушений компьютерной безопасности (изъянов защиты) вычислительной системы (источники появления изъянов защиты, время их внедрения, размещение в системе). Причины, обуславливающие наличие нарушений компьютерной безопасности (изъянов защиты).	2	*2*
	Самостоятельная работа студентов Подготовить конспект по теме «Причины, обуславливающие наличие нарушений компьютерной безопасности»	1	
Тема 3.3 Идентификация и аутентификация	Идентификация и аутентификация. Парольная аутентификация. Биометрическая аутентификация	2	*3*
	Практическое занятие № 3 Количественная оценка стойкости парольной защиты	4	
	Самостоятельная работа студентов Подготовка отчёта по практическому занятию и его защита	2	
Модуль 4	**Защита информации**	**22**	
Раздел 4. Защита информации		**22**	
Тема 4.1. Понятие и сущность защиты информации (ЗИ). Цели и концептуальные основы ЗИ	Доктрина информационной безопасности РФ. Лицензирование в области защиты информации. Сертификация в области защиты информации. Правовые основы защиты информации	2	*2*
	Самостоятельная работа студентов Изучить Доктрину информационной безопасности РФ	2	
Тема 4.2. Виды уязвимости информации и формы ее проявления	Структурная схема построения мест возможного вторжения в компьютерную сеть. Нарушение целостности информации. Блокирование доступа к объектам и ресурсам сети	2	*2*
	Самостоятельная работа студентов Подготовить конспект по теме «Нарушение целостности информации»	1	
Тема 4.3 Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию	Виды дестабилизирующих факторов. Системные методы решения. Полное и абсолютное требование к решению задач защиты информации. Источники дестабилизирующих факторов. Исследования в области причин повреждения электронной информации	2	*2*
	Самостоятельная работа студентов Подготовить конспект по теме «Исследования в области причин повреждения электронной информации»	1	

Тема 4.4 Каналы и методы несанкционированного доступа к защищаемой информации	КНСД относящиеся и не относящиеся к обработке информации. КНСД с доступом злоумышленника и без доступа злоумышленника. КНСД с изменением информации и без изменения информации. Обзор самых распространенных методов взлома информационных систем	2	*1*
	Самостоятельная работа студентов Подготовить конспект по теме «Обзор самых распространенных методов взлома информационных систем»	1	
Тема 4.5 Носители защищаемой информации. Объекты защиты. Виды защиты	Типовые структурные компоненты систем обработки, хранения и передачи информации. Программное обеспечение ЭВМ. Аппаратные средства ЭВМ. Сети передачи данных. Хранилища документов и машинных носителей. Требования к элементам и объектам защиты	2	*2*
	Самостоятельная работа студентов Подготовить конспект по теме «Требования к элементам и объектам защиты»	1	
Тема 4.6 Методологические подходы к защите информации и принципы ее организации. Системы защиты информации	Контроль доступа к аппаратуре. Использование простого пароля. Динамический пароль. Идентификация и установление подлинности объекта. Идентификация и установление подлинности документов. Способы определения модификаций информации. Регистрация действий пользователя	2	*2*
	Самостоятельная работа студентов Подготовить конспект по теме «Регистрация действий пользователя»	1	
Тема 4.7 Кадровое и ресурсное обеспечение ЗИ	Кадровая безопасность. Физическая защита. Дисциплинарные акции. Ответственность за нарушения в информационной сфере. Обучение персонала. Практическая подготовка для выполнения обязанностей	2	*2*
	Самостоятельная работа студентов Подготовить конспект по теме «Ответственность за нарушения в информационной сфере»	1	
	ИТОГО:	**64**	

4 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1. Специализированные лаборатории и классы

№ п.п.	Помещения			Площадь, м^2	Количество посадочных мест
	Название	Принадлежность (кафедра)	Номер аудитории		
1	Лаборатория информационных технологий	*Кафедра ЕН*	*103 В*	*108*	*42*

4.2. Основное учебное оборудование

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката)	Кол-во, ед.	Год изготовления	Форма владения, пользования (собственность, оперативное управление, аренда и т.п.)	№ аудитории
1	Мультимедиапроектор Aser P5390w	1	2007	Оперативное управление	103 В
2	Экран настенный Classic 240*180	1	2007		
3	Компьютеры Pentium(R) Dual-Core CPU E5400 2.7 GHz/ ASUS P5Q SE/R/ ОЗУ 2*1 Gb/ NVIDIA GeForce 9600 GT (512 Mb)/ Realtek ALC1200/ ST3160813AS 2*160 Gb/ Onboard	17	2009		

4.3 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1 Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере: учебник. – М.: Форум, 2009г.

2 Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие –М.: ИНФРА-М: ИД ФОРУМ, 2009 г.

Программное обеспечение

Антивирус Dr.Web Agent

Диспетчер виртуальных машин VMware Player

Microsoft Office Профессиональный плюс 2007

Базы данных, информационно-справочные и поисковые системы

Справочно-правовая система Консультант Плюс

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

5.1 Текущий контроль освоения заданных дисциплинарных компетенций

Текущий контроль освоения дисциплинарных компетенций проводится в следующих формах:

- устный опрос,
- тестирование;
- защита отчётов по практическим занятиям.

Уровень освоения частей компетенций подтверждается оценкой по дисциплине, определяемой исходя из количества средне набранных баллов по каждому результату обучения по дисциплине, в соответствии с показателями, критериями и шкалой оценивания, представленными в таблице 5.1.1.

Таблица 5.1.1 - Показатели, критерии, средства оценивания достижения запланированных результатов обучения при текущем контроле успеваемости и шкала оценки результатов формирования частей компетенций, приобретаемых в ходе освоения дисциплины Защита информации

Результаты обучения	Показатели и критерии оценивания сформированности частей компетенций		Средства оценивания	Шкала оценивания		
	показатели	критерии		5	4	3
ПК.1.5. ОП.11- З3 - знает основные правовые понятия, законодательные акты и др. нормативные документы в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации; З4 – знает методы и формы защиты информации; З5 – знает виды и методы дестабилизирующего воздействия на защищаемую информацию; У8 - умеет производить классификацию конфиденциальной информации по видам тайны и степени конфиденциальности; У9 - умеет оценивать степень угрозы конфиденциальной информации; У10 – умеет использовать методы шифрования	Понимание сути основных правовых понятий, законодательных актов и др. нормативных документов в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации, методов и форм защиты информации;	Количество правильных ответов в тесте на знание основных правовых понятий, законодательных актов и др. нормативных документов в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации, методов и форм защиты информации;	Тесты по модулям «Основные положения компьютерной безопасности», «Нормативное обеспечение компьютерной безопасности», «Основы обеспечения компьютерной безопасности», «Защита информации»	86-100	70-85	51-69
	Понимание сути основных правовых понятий, законодательных актов и др. нормативных документов в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации, методов и форм защиты информации;	Точность воспроизведение основных правовых понятий, законодательных актов и др. нормативных документов в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации, методов и форм защиты информации;	Устный ответ по модулям «Основные положения компьютерной безопасности», «Нормативное обеспечение компьютерной безопасности», «Основы обеспечения компьютерной безопасности», «Защита информации»	Точное, уверенное воспроизведение содержания основных правовых понятий, законодательных актов и др. нормативных документов в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации, методов и форм защиты информации;	Достаточно точное воспроизведение содержания основных правовых понятий, законодательных актов и др. нормативных документов в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации, методов и форм защиты информации;	Допущены отдельные ошибки, и неточности в ответе
	Правильно выполненные задания по методам шифрования и степени угроз конфиденциальной информации	Правильно выполненные и оформленные задания по методам шифрования и степени угроз конфиденциальной информации	Практические занятия № 1-3	Глубокие исчерпывающие выполненные и оформленные части исследовательской работ задания по методам шифрования и степени	Достаточно полные выполненные и оформленные задания по методам шифрования и степени угроз конфиденциальной	Понимание заданий по методам шифрования и степени угроз конфиденциальной информации

Результаты обучения	Показатели и критерии оценивания сформированности частей компетенций		Средства оценивания	Шкала оценивания		
	показатели	критерии		5	4	3
				угроз конфиденциальной информации ы	информации	
ОК.01.ОП.11- З1 - знает значение и место защиты информации в своей будущей профессии ОК.02.ОП.11- У1 -умеет организовывать и проводить самооценку выполненных внеаудиторных самостоятельных работ по дисциплине ОК.03.ОП.11- У2 -умеет принимать решения в стандартных и нестандартных ситуациях в области защиты информации ОК.04.ОП.11- У3 -умеет формировать отчётные документы по выполненным внеаудиторным самостоятельным работам по дисциплине ОК.05.ОП.11- У4 -умеет использовать информационно-коммуникационных технологий в области защиты информации ОК.06.ОП.11- У5 -умеет организовать	Правильно выполненная и вовремя сданная внеаудиторная самостоятельная работа по дисциплине	В сроки сданная внеаудиторная самостоятельная работа и правильно выполненная	Подготовка конспектов и отчётов по практическим занятиям	Глубокое исчерпывающее понимание содержания материала по дисциплине, в сроки сданная работа	Достаточно полное понимание содержания материала по дисциплине, в сроки сданная работа	Понимание основного содержание материала по дисциплине, работа сдана не в установленные сроки

Результаты обучения	Показатели и критерии оценивания сформированности частей компетенций		Средства оценивания	Шкала оценивания		
	показатели	критерии		5	4	3
исследовательскую деятельность в коллективе ОК.07.ОП.11- У6 -умеет брать ответственность за результаты коллективного труда в области защиты информации ОК.08.ОП.11- У7 -умеет самостоятельно заниматься самообразованием в области защиты информации ОК.09.ОП.11- З2 - новые методы защиты информации в профессиональной деятельности						

5.2 Промежуточный контроль освоения заданных дисциплинарных компетенций

а) Дифференцированный зачёт

Условия проставления дифференцированного зачёта по дисциплине: дифференцированный зачёт по дисциплине «Защита информации» выставляется по итогам проведённого текущего контроля знаний студентов и выставленной средней результирующей оценки по всем модулям текущего контроля:

- оценка «отлично» за дисциплину – средняя оценка по всем модулям не менее 4,5;
- оценка «хорошо» за дисциплину – средняя оценка по всем модулям не менее 4,0;
- оценка «удовлетворительно» за дисциплину – средняя оценка по всем модулям не менее 3,0

б) Экзамен – не предусматривается

5.3 Контрольно-измерительные материалы

Вопросы для подготовки к дифференцированному зачёту

1 История развития информационной безопасности.
2 Перспективы и тенденции развития информационной безопасности.
3 Доктрина ИБ РФ. ФЗ «Об информации, информационных технологиях и защите информации».
4 Характеристика составляющих информационной безопасности.
5 Классификация целей национальной безопасности по уровням.
6 Место информационной безопасности РФ в системе национальной безопасности РФ.
7 Государственная информационная политика. Основные угрозы безопасности России.
8 Внешние и внутренние источники угроз ИБ.
9 Организационная структура системы информационной безопасности РФ.
10 Государственная тайна. Федеральный Закон «О государственной тайне».
11 Коммерческая тайна.
12 Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
13 Виды доступа к информации.
14 Понятие и сущность защиты информации (ЗИ).
15 Цели и концептуальные основы ЗИ.
16 Виды уязвимости информации и формы ее проявления.
17 Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.
18 Исследования в области причин повреждения электронной информации.
19 Каналы и методы несанкционированного доступа к защищаемой информации.

20 Обзор самых распространенных методов взлома информационных систем.

21 Носители защищаемой информации. Объекты защиты. Виды защиты.

22 Методологические подходы к защите информации и принципы ее организации. Системы защиты информации.

23 Кадровое и ресурсное обеспечение ЗИ

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания ПЦК Подпись председателя ПЦК