Министерство науки и высшего образования Российской Федерации
Лысьвенский филиалфедерального государственного бюджетного образовательного учреждения высшего образования
«Пермский национальный исследовательский политехнический университет»

УТВЕРЖДАЮ
Зав. кафедрой ОНД
_____ Е.Н. Хаматнурова
«20» 03 2020 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по учебной дисциплине

ЗАЩИТА ИНФОРМАЦИИ

основной профессиональной образовательной программы
подготовки специалистов среднего звена
по специальности СПО 09.02.01 Компьютерные системы и комплексы

(базовая подготовка)

Лысьва, 2020

Фонд оценочных средств разработан на основе:

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

– рабочей программы учебной дисциплины «Защита информации», утвержденной «20» 03 2020 г.

Разработчик: преподаватель П.В. Кочнев

Фонд оценочных средств рассмотрен и одобрен на заседании предметной (цикловой) комиссии Естественнонаучных дисциплин (ПЦК ЕНД) «10» 03 2020 г., протокол № 7 .

Председатель ПЦК ЕНД  Е.Л. Федосеева

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

В результате освоения учебной дисциплины Защита информации обучающийся должен обладать предусмотренными ФГОС по специальности 09.02.01 «Компьютерные системы и комплексы» базовой подготовки следующими результатами обучения: знаниями и умениями , которые формируют профессиональные и общие компетенции.

Показатели, критерии, средства оценивания достижения запланированных результатов обучения и шкала оценки результатов формирования частей компетенций, проверяемых в при текущем и промежуточном контроле представлены в таблице 1.

Формой промежуточной аттестации по учебной дисциплине является **дифференцированный зачёт.**

КОНТРОЛЬ РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. ТЕКУЩИЙ И ПРОМЕЖУТОЧНЫЙ КОНТРОЛЬ ОСВОЕНИЯ ЗАДАННЫХ ДИСЦИПЛИНАРНЫХ КОМПЕТЕНЦИЙ

Текущий и промежуточный контроль освоения дисциплинарных компетенций проводится в следующих формах:

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

Уровень освоения частей компетенций подтверждается оценкой по четырехбалльной шкале во время текущего контроля успеваемости, определяемой исходя из количества средне набранных баллов по каждому результату обучения по дисциплине, в соответствии с показателями, критериями и шкалой оценивания, представленными в таблице 1.

Таблица 1 - Показатели, критерии, средства оценивания достижения запланированных результатов обучения 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
ОК 1-9, ПК.1.5. **Знать:** - основные правовые понятия, законодательные акты и др. нормативные документы в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации; - методы и формы защиты информации; - виды и методы дестабилизирующего воздействия на защищаемую информацию. **Уметь:** - производить классификацию конфиденциальной информации по видам тайны и степени конфиденциальности; - оценивать степень угрозы конфиденциальной информации;	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 разделам	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 разделам	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 угроз конфиденциальной информации ы	Достаточно полные выполненные и оформленные задания по методам шифрования и степени угроз конфиденциальной информации	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
- использовать методы шифрования.						

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ОЦЕНКИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. Типовые вопросы для устного опроса

Критерии и шкалы оценивания представлены в таблице 1.

Вопросы для устного опроса

Модуль «Основные положения компьютерной безопасности»

1. Основные понятия и определения компьютерной безопасности
2. Угрозы безопасности компьютерных систем
3. Общие проблемы безопасности
4. Информационная безопасность в России в целом, а также в условиях функционирования глобальных сетей, в частности.
5. Виды вирусов и другого зловредного кода.
6. Назовите основные особенности эксперимента.
7. Антивирусное программное обеспечение.
8. Требования к системам защиты информации

Модуль «Нормативное обеспечение компьютерной безопасности»

1. Международные стандарты компьютерной безопасности
2. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы
3. Инвентаризация информационных систем. Классификация информационных систем.

Модуль «Основы обеспечения компьютерной безопасности»

1. Формальные модели безопасности и их применение
2. Таксономия нарушений компьютерной безопасности вычислительной системы
3. Причины, обуславливающие наличие нарушений компьютерной безопасности
4. Идентификация и аутентификация. Парольная аутентификация. Биометрическая аутентификация

Модуль «Защита информации»

1. Доктрина информационной безопасности РФ.
2. Структурная схема построения мест возможного вторжения в компьютерную сеть.
3. Виды дестабилизирующих факторов. Системные методы решения.
4. Полное и абсолютное требование к решению задач защиты информации. Источники дестабилизирующих факторов.
5. КНСД относящиеся и не относящиеся к обработке информации.
6. Типовые структурные компоненты систем обработки, хранения и передачи информации.
7. Контроль доступа к аппаратуре. Использование простого пароля. Динамический пароль.

2. Типовые тесты по модулям

Критерии и шкалы оценивания представлены в таблице 1.

Типовой тест № 1

Модуль «Основные положения компьютерной безопасности»

Условия выполнения задания

- *тест выполняется в аудитории во время практических занятий;*

- для выполнения теста необходимо следующее оборудование: бланки ответов, ручки, карточки с тестами (для выполнения электронного варианта теста: компьютерный класс, тестировщик).

Инструкция: на выполнение теста отводится 30 минут, внимательно прочитайте вопрос, выберите один вариант ответа, ответы занесите в бланк ответов

1. .Информационная безопасность - это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы:
1) конфиденциальность
2) целостность
3) доступность
4) учет
5) неотрекаемость
6) мобильность
2. Сопоставьте понятия и их определения.
1) возможность ознакомиться с информацией имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями.
2) возможность внести изменение в информацию должны иметь только те лица, кто на это уполномочен.
3) возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкцианированный для работы период времени.
4) все значимые действия лица, выполняемые им в рамках, контролирумых системой безопасности, должны быть зафиксированы и проанализированы.
5) лицо, направившее информацию другому лицу, не может отречься от факта направления информации, а лицо, получившее информацию, не может отречься от факта ее получения.
__ конфиденциальность
__ целостность
__ доступность
__ учет
__ неотрекаемость
3.... - это набор формальных правил, которые регламентируют функционирование механизма информационной безопасности.
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация
4. ... - распознавание каждого участника процесса информационного взаимодействия перед тем, как к нему будут применены какие бы то ни было понятия информационной безопасности.
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

5. ... - обеспечение уверенности в том, что участник процесса обмена информацией определен верно, т.е. действительно является тем, чей идентификатор он предъявил.
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация
6. ... - создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа.
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация
7. ... - формирование профиля прав для конкретного участника процесса информационного обмена из набора правил контроля доступа.
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация
8. ... - обеспечение соответствия возможных потерь от нарушения информационной безопасности затратам на их построение.
1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости
9. ... - поддержание среды информационого обмена в минимально допустимом работоспособном состоянии и сооответствии требованиям информационной безопасности в услових деструктивны внешних или внутренних воздействий.
1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости
10. ... - совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационой безопасности.
1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости
11. Перечислите основные направления информационной безопасности.
1) Физическая безопасность
2) Компьютерная безопасность

3) Визуальная безопасность
4) Сензитивная безопасность
12. Перечислите состав службы информационной безопасности.
1) Руководитель службы
2) Операционный отдел
3) Исследовательский отдел
4) Методический отдел
5) Отдел общения с прессой
6) Отдел бухгалтерии
13. Какой считается по классификации информационных объектов устаревшая или неиспользуемая информация, не влияющая на работу субъекта.
1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной
14. Критериями определения уровня безопасности систем являются:
1) Оранжевая книга
2) Красная книга
3) Зеленая книга
4) Серо-буромалиновая книга
5) Белая книга
15. ... - выпущенные Министерством обороны США критерии оценки уровня безопасности компьютерных систем.
1) Оранжевая книга
2) Красная книга
3) Белая книга
4) Зеленая книга
5) Открытая книга
16. ... - выпущенные Министерством обороны США расширение критериев оценки уровня безопасности компьютерных систем для случаев использования компьютерных систем в информационной сети.
1) Оранжевая книга
2) Красная книга
3) Белая книга
4) Зеленая книга
5) Открытая книга
17. Перечислите модели классификации информационных объектов.
1) По наличию
2) По несанкционированной модификации (целостность)
3) По разглашению
4) По принадлежности
5) По аппелируемости
18. Какой считается информация, по классификации информационных объектов, если без нее можно работать, но очень короткое время.

1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной

19. Какой считается информация, по классификации информационных объектов, если без нее можно работать, но ее использование экономит ресурсы.

1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной

Типовой тест № 2

Модуль «Нормативное обеспечение компьютерной безопасности»

Условия выполнения задания

- тест выполняется в аудитории во время практических занятий;

- для выполнения теста необходимо следующее оборудование: бланки ответов, ручки, карточки с тестами (для выполнения электронного варианта теста: компьютерный класс, тестировщик).

Инструкция: на выполнение теста отводится 10 минут, внимательно прочитайте вопрос, выберите один вариант ответа, ответы занесите в бланк ответов

1. Авторское право это -

1) свое имя, псевдоним, анонимно
2) право считаться автором
3) защита программы и ее названия от искажений
4) выпуск программы в свет

2. Неправомерный доступ к компьютерной информации – это статья УК РФ

1) 271
2) 272
3) 273
4) 274

3. В каком году был принят закон Об информации, информационных технологиях и защите информации :

1) 2004
2) 2005
3) 2006
4) 2008

4. В каком году была принята доктрина информационной безопасности РФ

1) 2001
2) 1997
3) 1998
4) 2000

5. Назовите статьи конституции РФ по защите информации

1) 23,24,29,41,42
2) 28,34,21,24,29
3) 41,42,29,25,23
4) 38,20,21,29,23

Типовой тест № 3

Модуль «Основы обеспечения компьютерной безопасности»

Условия выполнения задания

- тест выполняется в аудитории во время практических занятий;

- для выполнения теста необходимо следующее оборудование: бланки ответов, ручки, карточки с тестами (для выполнения электронного варианта теста: компьютерный класс, тестировщик).

Инструкция: на выполнение теста отводится 15 минут, внимательно прочитайте вопрос, выберите один вариант ответа, ответы занесите в бланк ответов

1.Утечка информации

Выберите один из 3 вариантов ответа:

1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу

2) ознакомление постороннего лица с содержанием секретной информации

3) потеря, хищение, разрушение или неполучение переданных данных

2. Под изоляцией и разделением (требование к обеспечению ИБ) понимают

Выберите один из 2 вариантов ответа:

1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)

2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп

3. К аспектам ИБ относятся

Выберите несколько из 5 вариантов ответа:

1) дискретность

2) целостность

3) конфиденциальность

4) актуальность

5) доступность

4. Линейное шифрование -

Выберите один из 3 вариантов ответа:

1) несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу

2) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому

3) криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами

5. Угроза - это

Выберите один из 2 вариантов ответа:

1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов

2) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

6. Под ИБ понимают

Выберите один из 3 вариантов ответа:
1) защиту от несанкционированного доступа
2) защиту информации от случайных и преднамеренных воздействий естественного и исскуственного характера
3) защиту информации от компьютерных вирусов
7. Что такое криптография?
Выберите один из 3 вариантов ответа:
1) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
2) область доступной информации
3) область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом
8. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется
Выберите один из 4 вариантов ответа:
1) кодируемой
2) шифруемой
3) недостоверной
4) защищаемой
9. Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это
Выберите один из 4 вариантов ответа:
1) текст
2) данные
3) информация
4) пароль
10. Организационные угрозы подразделяются на
Выберите несколько из 4 вариантов ответа:
1) угрозы воздействия на персонал
2) физические угрозы
3) действия персонала
4) несанкционированный доступ
11. Виды технической разведки (по месту размещения аппаратуры)
Выберите несколько из 7 вариантов ответа:
1) космическая
2) оптическая
3) наземная
4) фотографическая
5) морская
6) воздушная
7) магнитометрическая
12. Основные группы технических средств ведения разведки
Выберите несколько из 5 вариантов ответа:
1) радиомикрофоны
2) фотоаппараты
3) электронные "уши"

4) дистанционное прослушивание разговоров
5) системы определения местоположения контролируемого объекта

Типовой тест № 4

Модуль «Защита информации»

Условия выполнения задания

- тест выполняется в аудитории во время практических занятий;

- для выполнения теста необходимо следующее оборудование: бланки ответов, ручки, карточки с тестами (для выполнения электронного варианта теста: компьютерный класс, тестировщик).

Инструкция: на выполнение теста отводится 15 минут, внимательно прочитайте вопрос, выберите один вариант ответа, ответы занесите в бланк ответов

1. Разновидности угроз безопасности
Выберите несколько из 6 вариантов ответа:
1) техническая разведка
2) программные
3) программно-математичекие
4) организационные
5) технические
6) физические
2. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется
Выберите один из 4 вариантов ответа:
1) угрозой;
2) опасностью;
3) намерением;
4) предостережением.
3. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?
Выберите один из 4 вариантов ответа:
1) операционной системы, сетевого программного обеспечения
2) операционной системы, сетевого программного обеспечения и системы управления базами данных;
3) операционной системы, системы управления базами данных;
4) сетевого программного обеспечения и системы управления базами данных.
4. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется
Выберите один из 4 вариантов ответа:
1) системой угроз;
2) системой защиты;
3) системой безопасности;
4) системой уничтожения.
5. К видам защиты информации относятся:
Выберите несколько из 4 вариантов ответа:
1) правовые и законодательные:
2) морально-этические;
3) юридические;
4) административно-организационные;
6. К методам защиты от НСД относятся
Выберите несколько из 5 вариантов ответа:

1) разделение доступа;
2) разграничение доступа;
3) увеличение доступа;
4) ограничение доступа.
5) аутентификация и идентификация
7. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется
Выберите один из 4 вариантов ответа:
1) политикой информации
2) защитой информации
3) политикой безопасности
4) организацией безопасности
8. Выделите группы, на которые делятся средства защиты информации:
Выберите один из 3 вариантов ответа:
1) физические, аппаратные, программные, криптографические, комбинированные;
2) химические, аппаратные, программные, криптографические, комбинированные;
3) физические, аппаратные, программные, этнографические, комбинированные;
9. Какие законы существуют в России в области компьютерного права?
Выберите несколько из 6 вариантов ответа:
1) О государственной тайне
2) об авторском праве и смежных правах
3) о гражданском долге
4) о правовой охране программ для ЭВМ и БД
5) о правовой ответственности
6) об информации, информатизации, защищенности информации

10. В чем заключается основная причина потерь информации, связанной с ПК?
Выберите один из 3 вариантов ответа:
1) с глобальным хищением информации
2) с появлением интернета
3) с недостаточной образованностью в области безопасности
11.Что такое несанкционированный доступ (нсд)?
Выберите один из 5 вариантов ответа:
1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
2) Создание резервных копий в организации
3) Правила и положения, выработанные в организации для обхода парольной защиты
4) Вход в систему без согласования с руководителем организации
5) Удаление не нужной информации

12. Что такое аутентификация?
Выберите один из 5 вариантов ответа:
1) Проверка количества переданной и принятой информации
2) Нахождение файлов, которые изменены в информационной системе несанкционированно
3) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).
4) Определение файлов, из которых удалена служебная информация
5) Определение файлов, из которых удалена служебная информация
13. Кодирование информации -
Выберите один из 2 вариантов ответа:
1) представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.

2) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

2. ИТОГОВЫЙ КОНТРОЛЬ ОСВОЕНИЯ ЗАДАННЫХ ДИСЦИПЛИНАРНЫХ КОМПЕТЕНЦИЙ

Итоговый контроль освоения заданных дисциплинарных компетенций проводится во время промежуточной аттестации в форме дифференцированного зачёта.

Дифференцированный зачёт по дисциплине основывается на результатах выполнения тестовых заданий и практических заданий студента по данной дисциплине и сдавшие выполненные задания по практическим работам и получившие оценки не ниже «удовлетворительно» по результатам текущего контроля успеваемости. Итоговая оценка выставляется с учётом результатов текущего контроля успеваемости.

Типовые вопросы и задания для дифференцированного зачёта по дисциплине

Типовые вопросы для контроля усвоенных знаний:

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, составляющая информационную безопасность
5. Классификация национальной безопасности по уровням
6. Место информационной безопасности в РФ в 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 сущности 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. Исследование в области причин повреждения электронной информации.
19. Каналы и методы несанкционированного доступа к защищаемой информации.
20. Обзор самых распространенных методов взломов информационный систем .
21. Носители защищаемой информации .Объекты зашиты.Виды защиты.
22. Методологические подходы к защите информации и принципы ее организации .Системы защиты информации
23. Кадровое и ресурсное обеспечение(ЗИ).

Типовые задания для контроля освоенных умений:

1. Зашифруйте открытый текст «Криптография – это наука о методах и способах преобразования информации с целью ее защиты от незаконных пользователей» с помощью полибианского квадрата и шифром Виженера, секретный ключ задайте сами.
2. Зашифруйте открытый текст «Система DES – это блочный шифр» шифром Цезаря со сдвигом 5 и полибианским квадратом.
3. Зашифруйте открытый текст «Английский математик Чарльз Бэббидж в девятнадцатом веке сказал: Всякий человек, даже если он не знаком с техникой вскрытия шифров, твердо

считает, что сможет изобрести абсолютно стойкий шифр, и чем более умен и образован этот человек, тем более твердо это убеждение. Я сам разделял эту уверенность в течение многих лет» шифром Цезаря со сдвигом 7 и шифром Виженера, для которого секретный ключ задайте сами

4. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

   Исходные данные – $P=10^{-6}$, T=7 дней = 1 неделя, V=10 паролей / минуту = 10*60*24*7=100800 паролей в неделю.

Лист регистрации изменений

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