ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ "ЦЕНТР ОБУЧЕНИЯ "СПЕЦИАЛИСТ" УНЦ ПРИ МГТУ ИМ. Н.Э. БАУМАНА (ОЧУ ДПО «СПЕЦИАЛИСТ»)

123317, г. Москва, Пресненская набережная, д 8, стр. 1, этаж 48, помещение 484с, комната 3,
ИНН 7701168244, ОГРН 1127799002990

Утверждаю:
Директор ОЧУ ДПО «Специалист»

_____/Е.В. Добрыднева/
«_1__» __февраля____ 2018 года

Дополнительная профессиональная программа повышения квалификации «Построение системы безопасности персональных данных в организации»

город Москва

Программа разработана в соответствии с приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. N 499 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам".

Повышение квалификации слушателей, осуществляемое в соответствии с программой, проводится с использованием модульного принципа построения учебного плана с применением различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения в соответствии с законодательством об образовании.

Дополнительная профессиональная программа повышения квалификации, разработана образовательной организацией в соответствии с законодательством Российской Федерации, включает все модули, указанные в учебном плане.

Содержание оценочных и методических материалов определяется образовательной организацией самостоятельно с учетом положений законодательства об образовании Российской Федерации.

Структура дополнительной профессиональной программы соответствует требованиям Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 1 июля 2013 г. N 499.

Объем дополнительной профессиональной программы вне зависимости от применяемых образовательных технологий, должен быть не менее 16 академических часов. Сроки ее освоения определяются образовательной организацией самостоятельно.

Формы обучения слушателей (очная, очно-заочная, заочная) определяются образовательной организацией самостоятельно.

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

Для определения структуры дополнительной профессиональной программы и трудоемкости ее освоения может применяться система зачетных единиц. Количество зачетных единиц по дополнительной профессиональной программе устанавливается организацией.

Образовательная деятельность слушателей предусматривает следующие виды учебных занятий и учебных работ: лекции, практические и семинарские занятия, лабораторные работы, круглые столы, мастер-классы, мастерские, деловые игры, ролевые игры, тренинги, семинары по обмену опытом, выездные занятия, консультации, выполнение аттестационной, дипломной, проектной работы и другие виды учебных занятий и учебных работ, определенные учебным планом.

1. Цель программы:

В результате прохождения обучения слушатель получит актуальные системные знания и практические навыки создания в Вашей организации максимально эффективной системы безопасности данных и защиту информационные ресурсы. Вы научитесь выполнять требования нормативных правовых актов, руководящих и методических документов по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, а также сможете эффективно планировать и реализовывать комплекс мероприятий по минимизации рисков, связанных с обеспечением безопасности персональных данных в вашей компании

Совершенствуемые компетенции

№	Компетенция	Направление подготовки

		ФГОС НАПРАВЛЕНИЕ ПОДГОТОВКИ 02.03.02 ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА
		Код компетенции
1	способностью разрабатывать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, а также методы и механизмы оценки и анализа функционирования средств и систем информационных технологий	ПК-7

Совершенствуемые компетенции в соответствии с трудовыми фикциями профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах» от 15.09.2016 № 522н

№	Компетенция	Направление подготовки
		Трудовые функции (код)
1	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (Диагностика систем защиты информации автоматизированных систем, Администрирование систем защиты информации автоматизированных систем, Управление защитой информации в автоматизированных системах)	B/01.6, B/02.6, B/03.6

Планируемый результат обучения:

После окончания обучения Слушатель будет знать:

Федеральное Законодательство
Постановления правительства
Нормативные документы регулятора в области защиты персональных данных
Нормативные документы регуляторов в области технической защиты информации по вопросам защиты персональных данных
о правилах обработки ПДн
как точно определить перечень необходимых к выполнению требований по защите ПДн и лежащую на них ответственность.

После окончания обучения Слушатель будет уметь:

Проводить процессы обработки персональных данных в соответствие требованиям Законодательства
Построить эффективную систему защиты персональных данных
Подтверждать выполнения требований по защите персональных данных при проверках регуляторами

Учебный план:
Категория слушателей: руководители, специалисты, менеджеры, сотрудники ИТ подразделений обслуживающие информационные системы, Сотрудники

подразделений ИБ ответственные за обработку персональных данных, Сотрудники HR служб предприятий, Разработчики информационных систем и программных продуктов

Требования к предварительной подготовке:

Опыт руководства или кураторства ИТ-подразделением или опыт работы в ИТ-службе на любой позиции

Срок обучения: 16 академических часов, 8 часов самостоятельно

Форма обучения: очная, очно-заочная, заочная. По желанию слушателя форма обучения может быть изменена и/или дополнена.

Режим занятий: дневной, вечерний, группы выходного дня.

№ п/п	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд.ч	В том числе		СРС,ч
				Лекций	Практ занятий	
1	**Модуль 1.** Нормативно правовая база	3	2	2	0	1
2	**Модуль 2.** Приведение процессов обработки персональных данных в соответствие требованиям Законодательства	4	3	2	1	1
3	Модуль 3. Порядок проведения работ по созданию системы защиты персональных данных	4	3	1	2	1
4	Модуль 4. Обзор технических средств защиты информации	3	2	1	1	1
5	Модуль 5. Подтверждение выполнения требований	5	3	2	1	2
6	Модуль 6. Проверки регуляторов	5	3	1	2	2
	Итог:	24	16	9	7	8
	Итоговая аттестация	тестирование				

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

2. Календарный учебный график

Календарный учебный график формируется при осуществлении обучения в течение всего календарного года. По мере набора групп слушателей по программе составляется календарный график, учитывающий объемы лекций, практики, самоподготовки, выезды на объекты.

Неделя обучения	1	2	3	4	5	6	7	Итого часов
	пн	вт	ср	чт	пт	сб	вс	
1 неделя	4	4	4	4 ИА	-	-	-	16
СРС	2	2	2	2				8
Итого:								16/8
Примечание: ИА – Итоговая аттестация (тестирование)								

3. Рабочие программы учебных предметов

Модуль 1. Нормативно правовая база

- Федеральное Законодательство
- Постановления правительства
- Нормативные документы регулятора в области защиты персональных данных
- Нормативные документы регуляторов в области технической защиты информации по вопросам защиты персональных данных

Модуль 2. Приведение процессов обработки персональных данных в соответствие требованиям Законодательства

- Инвентаризация процессов обработки персональных данных
- Определение видов обработки и требований к ним

Модуль 3. Порядок проведения работ по созданию системы защиты персональных данных

- Определение требуемого уровня защищённости персональных данных при их обработке в информационных системах
- Определение требуемых в соответствии с определённым уровнем защищённости механизмов защиты.
- Построение модели угроз

- Определение требований по защите персональных данных. Выбор технологий защиты:
    - управления доступом
    - регистрации и учёта
    - обеспечения целостности
    - криптографической защиты
    - антивирусной защиты
    - обнаружения вторжений
    - защита виртуальных сред

Модуль 4. Обзор технических средств защиты информации

- Обзор российского рынка технических средств защиты.
- Сертифицированные средства защиты информации.

Модуль 5. Подтверждение выполнения требований

- Декларирование соответствия.
- Аттестация систем защиты персональных данных

Модуль 6. Проверки регуляторов

- Федеральное законодательство определяющее порядок проведения проверок регуляторами.
- Плановый и внеплановые проверки.
- Права и обязанности проверяемого и проверяющего

4. Организационно-педагогические условия

Соблюдение требований к кадровым условиям реализации дополнительной профессиональной программы:

а) преподавательский состав образовательной организации, обеспечивающий образовательный процесс, обладает высшим образованием и стажем преподавания по изучаемой тематике не менее 1 года и (или) практической работы в областях знаний, предусмотренных модулями программы, не менее 3 (трех) лет;

б) образовательной организацией наряду с традиционными лекционно-семинарскими занятиями применяются современные эффективные методики преподавания с применением интерактивных форм обучения, аудиовизуальных средств, информационно-телекоммуникационных ресурсов и наглядных учебных пособий.

Соблюдение требований к материально-техническому и учебно-методическому обеспечению дополнительной профессиональной программы:

а) образовательная организация располагает необходимой материально-технической базой, включая современные аудитории, библиотеку, аудиовизуальные средства обучения, мультимедийную аппаратуру, оргтехнику, копировальные аппараты. Материальная база соответствует санитарным и техническим нормам и правилам и обеспечивает проведение всех видов практической и дисциплинарной подготовки слушателей, предусмотренных учебным планом реализуемой дополнительной профессиональной программы.

б) в случае применения электронного обучения, дистанционных образовательных технологий каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно-образовательной среде, содержащей все электронные образовательные ресурсы, перечисленные в модулях дополнительной профессиональной программы.

5. Формы аттестации и оценочные материалы

Образовательная организация несет ответственность за качество подготовки слушателей и реализацию дополнительной профессиональной программы в полном объеме в соответствии с учебным планом.

Оценка качества освоения дополнительной профессиональной программы слушателей включает текущий контроль успеваемости и итоговую аттестацию.

Результаты итоговой аттестации слушателей ДПП в соответствии с формой итоговой аттестации, установленной учебным планом, выставляются по двух бальной шкале («зачтено\незачтено»).

Слушателям, успешно освоившим дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Слушателям, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть дополнительной профессиональной программы и (или) отчисленным из образовательной организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому образовательной организацией.

Итоговая аттестация проводится по форме тестирования в соответствии с учебным планом. Результаты итоговой аттестации заносятся в соответствующие документы.

Тест «Построение системы безопасности персональных данных в организации»
Условия прохождения
Время(мин): 20
Количество вопросов: 20
Проходной балл(ПБ): 12
ПБ средний уровень: 15
ПБ эксперт: 18

Вопрос 1
Программные угрозы

- Установка и запуск сторонних приложений
- Изменение программной конфигурации

Вопрос 2
Компьютерные вирусы

- описание вирусов и другого вредоносного программного обеспечения
- Описание возможного ущерба, вследствие вирусных атак
- Методы защиты
- Способы определения и реагирования на вирусные атаки

Вопрос 3
Резервное копирование

- необходимость резервного копирования
- Основные принципы резервного копирования
- Угрозы, связанные с нарушением расписания резервного копирования

Вопрос 4
Работа с конфиденциальной информацией

- Формирование регламента работы
- Удаление или искажение информации
- Методы защиты

Вопрос 5
Парольная защита

- Идентификация, аутентификация и авторизация
- Способы проверки подлинности
- Многофакторный и биометрический методы аутентификации
- Рекомендации по созданию и изменению паролей
- Формирование политики паролей

Вопрос 6
Политика работы с корпоративной электронной почтой

- Использование личных почтовых ящиков
- Отправка конфиденциальной информации неверным адресатам
- Способы проникновения спама в организацию, защита от спама

- Антивирусная защита для почтовых сообщений
- Понятие фишинга

Вопрос 7

Зачем нужны виртуальные частные сети

- Предназначения виртуальных частных сетей
- Виды виртуальных частных сетей
- Методы обеспечения защиты информации в виртуальных частных сетях

Вопрос 8
Ключевые понятия

- Пошаговое построение модели бизнес-процессов верхнего уровня
- Как идентифицировать и описывать бизнес-процесс
- Владелец и менеджер бизнес-процесса

Вопрос 9
Пошаговое моделирование бизнес-процесса

- Вопросы, которые интересуют пользователей при моделировании процессов
- Качество процессов
- Модель процесса

Вопрос 10
Декомпозиция. Вложенные бизнес-процессы и алгоритмы

- Полезные рекомендации для описания бизнес-процессов
- Изображение процесса с указанием необходимых документов
- Степень детализации и взаимосвязи

Вопрос 11
Реестр требований безопасности.

- Законодательные требования
- Нормативные требования
- Контрактные обязательства
- Требования бизнеса

Вопрос 12
Каталоги угроз и контрмер

- Германский стандарт IT Baseline Protection Manual
- Классификация ресурсов, угроз и контрмер CRAMM
- ГОСТ Р ИСО/МЭК 27005-2010
- ГОСТ Р 52448-2005
- ГОСТ Р 51275-2006
- Базовая модель угроз безопасности ПДн при их обработке в ИСПДн

Вопрос 13

Способы реализации угроз НСД

- Источники угроз НСД
- Варианты описания угроз НСД

Вопрос 14

Общая классификация ТКУИ

- Технические каналы утечки информации при ее передаче по каналам связи
- Технические каналы утечки речевой (акустической) информации
- Технические каналы утечки виброакустической информации
- Технические каналы утечки видовой информации