Негосударственное образовательное учреждение
«Учебно-консалтинговый центр «Интерфейс»
(НОУ «УКЦ «Интерфейс»)

ИНН 5031045145 ОГРН 1035006108345

«Утверждаю»
Директор НОУ «УКЦ «ИНТЕРФЕЙС»

Тулякова О.А_____

22 ноября 2020 г.

Образовательная программа дополнительного профессионального образования (повышения квалификации) Управление информационной безопасностью предприятия

Содержание

Описание образовательной программы

Настоящая образовательная программа повышения квалификации (далее — Программа) разработана в соответствии с:

1. Федеральным законом от 29 декабря 20l2r. №273-ФЗ «Об образовании в Российской Федерации».
2. Приказом Минобрнауки России от 1 июля 2013г. №499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».
3. Уставом НОУ «УКЦ «Интерфейс»

Структура Программы включает цели, планируемые результаты обучения, учебный план, календарный учебный график, рабочую программу, организационно-педагогические условия, формы аттестации и оценочные материалы.

Цели Программы содержат описание целевой аудитории, целей обучения и необходимых начальных знаний и навыков слушателей.

Планируемые результаты обучения представлены в виде перечня профессиональных компетенций в рамках имеющейся квалификации (с отсылкой к профессиональному стандарту), качественное изменение которых осуществляется в результате обучения.

Учебный план определяет перечень, трудоемкость, последовательность и распределение модулей, иных видов учебной деятельности обучающихся и формы аттестации.

Календарный учебный график определяет основные параметры учебного процесса при организации занятий по освоению настоящей Программ ы, включая форм ы обучения, расписание занятий очных групп и т.п.

Рабочая программа раскрывает рекомендуемую последовательность изучения разделов (модулей).

Описание организационно-педагогических условий реализации Программы определяет организационные и методические требования НОУ «УКЦ «Интерфейс» к организации и проведению обучения по Программе.

Формы аттестации и оценочные материалы определяют формы проведения промежуточной и итого вой аттестации по Программе и форму учебно-методических материалов, необходимых для проведения указанных видов аттестации.

Цели программы

Данная Программа предназначена для:

- руководителей компаний и их заместителей; руководителей подразделений и бизнес-единиц;
- руководителей и сотрудников служб безопасности предприятия; специалистов по информационной безопасности; специалистов по ИТ-безопасности и кибербезопасности;
- специалистов HR-подразделений; корпоративных юристов; сотрудников, участвующих в организации конфиденциального делопроизводства на предприятии.

Целью обучения является формирование у слушателей знаний и навыков, необходимых для создания комплексной системы защиты информации на предприятии, с учетом требований российского и международного законодательства, а также отечественных и международных стандартов. Особое внимание уделено защите персональных данных и режим у коммерческой тайны.

Для изучения данной Программы предварительная подготовка не требуется.

Планируемые результаты обучения

Реализация Программы направлена на повышение профессионального уровня в рамках имеющейся квалификации, определяемой профессиональным стандартом «06.033 Специалист по защите информации в автоматизированных системах», утвержденным Приказом Минтруда России от 15.09.2016 N 522н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах».

Результатами обучения по Программе станут знания и умения, соответствующие следующим обобщенным трудовым функциям указанного профессионального стандарта:

- Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации.
- Внедрение систем защиты информации автоматизированных систем.
- Формирование требований к защите информации в автоматизированных системах.

Совершенствуемые компетенции в соответствии с трудовыми функциями профессионального стандарта:

Компетенция	**Содержание компетенции** Трудовые функции	Код
Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	Диагностика систем защиты информации автоматизированных систем	B/01.6
	Мониторинг защищенности информации в автоматизированных системах	B/05.6
	Аудит защищенности информации в автоматизированных системах	B/06.6
Внедрение систем защиты информации автоматизированных систем	Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	C/02.6
	Внедрение организационных мер по защите информации в автоматизированных системах	C/04.6
Формирование требований к защите информации в автоматизированных системах	Обоснование необходимости защиты информации в автоматизированной системе	E/01.8
	определение угроз безопасности информации, обрабатываемой автоматизированной системой	E/02.8

После обучения слушатель сможет:

- Выполнять требования законодательства Российской Федерации в области защиты информации;
- Организовывать комплекс мероприятий по защите конфиденциальной информации на предприятии;
- Использовать для защиты информации международные и национальные стандарты безопасности информационных систем;
- Обеспечить безопасную обработку персональных данных на предприятии;
- Организовать внедрение и соблюдение режима коммерческой тайны на предприятии;

- Внедрить конфиденциальное делопроизводство на предприятии;
- Эффективно взаимодействовать с государственным и органами для обеспечения информационной безопасности на предприятии, в том числе при проведении проверок и других административных процедур.

Учебный план

Учебный план Программы определяет перечень, трудоем кость, последовательность и распределение модулей, иных видов учебной деятельности обучающихся и формы аттестации.

№ *п.п*	**Наименование разделов (модулей)**	**Всего, час**	**В том числе**		**Форма аттестации**
			Лекции	**Практические занятия**	
1.	Политика информационной безопасности на предприятии	4	3	1	Опрос, практические занятия
2	Система мероприятий по защите конфиденциальной информации. Ответственность за ее разглашение	4	3	1	Опрос, практические занятия
3.	Защита персональных данных на предприятии	4	3	1	Опрос, практические занятия
4.	Алгоритмы и регламенты защиты персональных данных на предприятии	4	3	1	Опрос, практические занятия
5.	Режим коммерческой тайны на предприятии	4	3	1	Опрос, практические занятия
6.	Особенности внедрения режима коммерческой тайны	3	2,5	0,5	Опрос, практические занятия
7.	**Итоговая аттестация**	**1**		**1**	Опрос
	ИТОГО	**24**	**17,5**	**6,5**	

Допускается формирование индивидуального учебного плана для каждого слушателя в пределах осваиваемой Программы в порядке, установленном Положением об организации образовательного процесса в НОУ «УКЦ «Интерфейс».

Календарный учебный график

Учебный год: круглогодичное обучение.

Продолжительность Программы: 24 академических часа.

Форма организации образовательного процесса: очная, очно-заочная (вечерняя) и заочная формы обучения, в том числе, с применением дистанционных образовательных технологий и электронного обучения.

Сменность занятий (при очной форме обучения): 1 смена.

Количество учебных дней в неделю при очном обучении: 3 дня.

Начало учебных занятий: 9.30

Окончание учебных занятий: 17.00

Продолжительность урока: 45 минут (1 академический час).

Продолжительность перемен: 15 минут, перерыв на обед — 60 минут.

Расписание занятий для очных групп:

	№ урока	Время
Конкретный день недели согласовывается во время учебного процесса	1-2	09:30 - 11:00
	3-4	11:15 - 12:45
	5 6	13:45 - 15:15
	7-8	15:30 - 17:00

Рабочая программа

Модуль 1. Политика информационной безопасности на предприятии

- Законодательство Российской Федерации в области защиты информации. Термины и определения. Правовые основы наличия на предприятии конфиденциальной информации. Информация, доступ к которой не может быть ограничен.
- Порядок создания корпоративной нормативно-правовой базы по защите информации. Методика разработки политики информационной безопасности на предприятии.
- Создание службы информационной безопасности (СИБ). Разделение функций между СИБ, СБ и ИТ-подразделением. Место СИБ в структуре предприятия.
- Менеджмент информационной безопасности. Порядок проведения аудита информационной безопасности на предприятии.
- Структура конфиденциальных информационных массивов. Источники конфиденциальной информации. Угрозы информационных ресурсам и варианты их реализации.
- Основные направления защиты конфиденциальной информации. Системный подход к защите информации.

Модуль 2. Система мероприятий по защите конфиденциальной информации. Ответственность за ее разглашение

- Организационные мероприятия по защите конфиденциальной информации. Анализ информационных ресурсов на предприятии. Оптимизация информационных потоков. Определение формы представления информационных ресурсов, подлежащих защите.
- Режимные, технические и инженерно-технические мероприятия по защите конфиденциальной информации. Создание внутри объектового и пропускного режимов. Физическая защита охраняемых информационных ресурсов. Способы хранения информации вне территории предприятия.
- Кадровые мероприятия по защите конфиденциальной информации. Распределение прав доступа к информации. Разглашение информации через «человечески й фактор», как основной канал утеч ки конфиденциальной информации.
- ИТ-мероприятия по защите конфиденциальной информации. Защита компьютерных сетей. Применение средств криптографической защиты информации.
- Правовые мероприятия по защите конфиденциальной информации. Создание на предприятии правовых режимов по защите информации. Возможность использование правовых режимов для привлечения сотрудников к юридической ответственности за разглашение информации или неправомерному доступу к информации.
- Международные и национальные стандарты безопасности информационных систем. Основные положения ИСО27000. Американская концепция системного подхода к обеспечению защиты конфиденциальной информации (OPSEC Operation Security).
- Виды юридической ответственности за разглашение конфиденциальной информации, а также за ее незаконное получение. Уголовная, административная и гражданско-правовая ответственность. Обзор судебной практики.

Модуль 3. Защита персональных данных на предприятии

- Международные конвенции по защите персональных данных физических лиц. Законодательство РФ в сфере персональных данных. Основные правовые акты регуляторов, определяющих политику по защите персональных данных.
- Права субъекта персональных данных и обязанности оператора персональных данных. Виды юридической ответственности за разглашение персональных данных, а также за невыполнение требований по их защите.
- Формирование правового режима защиты персональных данных. Порядок *пол* учения, хранения, предоставления и уничтожения (обезличивания) персональных данных. Требования по защите персональных данных.
- Организационные, технические и инженерно-технические мероприятия, проводимые при обработке персональных данных. Создание локальной базы организационно-распорядительных документов.
- Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, и их защита.
- Особенности обработки персональных данных, осуществляемой в информационных системах персональных данных. Формирование модели угроз безопасности персональных данных. Методика определения актуальных угроз. Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз.
- Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Модуль 4. Алгоритмы и регламенты защиты персональных данных на предприятии

- Пошаговый алгоритм действий по созданию на предприятии системы обработки персональных данных, удовлетворяющей требованиям регуляторов.
- Административный регламент исполнения государственной функции по осуществлению государственного контроля за соответствием обработки персональных данных требованиям законодательства.
- Права и обязанности должностных лиц, осуществляющих государственный контроль и лиц, в отношении которых осуществляются мероприятия по контролю. Психологические приемы общения с проверяющими.
- Требования к порядку исполнению государственной функции по контролю за обработкой персональных данных. Состав, последовательность и сроки выполнения административных процедур.
- Порядок и формы контроля за исполнением государственной функции по контролю за обработкой персональных данных. Досудебный (внесудебный) порядок обжалования решений и действий (бездействий) проверяющих должностных лиц.

Модуль 5. Режим коммерческой тайны на предприятии

- Подготовительные мероприятия перед созданием режима коммерческой тайны. Оптимизация защищаемых информационных потоков. Определение формы представления информации, включаемой в режим коммерческой тайны.
- Составление перечня сведений, составляющих коммерческую тайну. Практические советы по составлению перечня. Возможные аналитические приемы, применяемые при составления этого перечня (диверсионный анализ, анализ с позиции ущерба, анализ по аналогии, экспертный анализ и т.д.).
- Установление сроков защиты информации, составляющей коммерческую тайну. Определение времени и процедур оценки конфиденциальности документов. Установление порядка вывода документов из режима коммерческой тайны.
- Изменения и дополнения, вносимые в нормативно-правовые документы предприятия при введении режима коммерческой тайны.
- Определение перечня должностей, при назначении на которые сотрудники будут допущены к коммерческой тайне. Практические рекомендации по составлению перечня.
- Обязательства сотрудников по сохранению коммерческой тайны на предприятии. Что понимается под разглашением коммерческой тайны. Обязан ли сотрудник хранить коммерческие секреты после увольнения.

Модуль 6. Особенности внедрения режима коммерческой тайны

- Разделение коммерческой тайны на группы по принципу конфиденциальности с установлением процедур работы и защиты информации, попадающей в различные группы.
- Особенности включения в режим коммерческой тайны информации, представленной в электронном виде.
- Защита коммерческой тайны. Комплексный и системный подход к защите информации. Организационные, кадровые, технические, режимные и иные мероприятия по защите коммерческой тайны.
- Особенности создания режима коммерческой тайны в организациях, представляющих разные сферы бизнеса (промышленные предприятия, сфера услуг и т.д.).
- Соблюдение режима коммерческой тайны в гражданско-правовых отношениях с контрагентами. Как прописать в договоре. Компенсация ущерба или штрафные санкции — что применять к контрагенту за нарушение конфиденциальности переданной ему информации, составляющей коммерческую тайну.
- Создание конфиденциального делопроизводства, как необходимый элемент защиты документов, в которых представлена коммерческая тайна. Определение процедур создания, перемещения, хранения и уничтожения конфиденциальных документов.

Организационно-педагогические условия реализации Программы

При реализации Программы применяется форма организации образовательной деятельности, основанная на модульном принципе представления содержания образовательной программы и построения учебных планов, использовании различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения.

Организационные условия реализации программы в разных формах обучения регулируются следующими локальными нормативными актами:

- Положение об организации образовательного процесса в НОУ «УКЦ «Интерфейс».
- Положение о порядке применения электронного обучения, дистанционныхобразовательных технологий в НОУ «УКЦ «Интерфейс».

Учебные материалы по Программе включают: рабочую программу, раздаточные материалы по курсу, методические материалы по курсу, данные примеров по курсу. Учебное пособие по Программе выдается слушателям в бумажном или электронное виде в зависимости от формы обучения в порядке, установленном Положением о библиотеке в НОУ «УКЦ «Интерфейс».

К реализации ДПП ПК НОУ «УКЦ «Интерфейс» привлекаются педагогические работники, квалификация которых соответствует требованиям Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей работников образования»:
«Высшее профессиональное образование или среднее профессиональное образование по направлению подготовки «Образование и педагогика» или в области, соответствующей преподаваемому предмету, без предъявления требований к стажу работы или высшее профессиональное образование или среднее профессиональное образование и дополнительное профессиональное образование по направлению деятельности в образовательном учреждении без предъявления требований к стажу. Занятия по Программе проводятся преподавателями, предварительно подтвердившими свою квалификацию. В числе базовых требований ко всем преподавателям – требование сдачи технических сертификационных тестов по продукту или технологии, рассматриваемым в курсе.

Освоение Программы сопровождается промежуточной аттестацией обучающихся в формах, определенных учебным планом, и в порядке, установленном Положением об организации образовательного процесса в НОУ «УКЦ «Интерфейс».

Освоение Программы завершается итоговой аттестацией обучающихся в форме, определенной учебным планом, и в порядке, установленном Положением об организации образовательного процесса в НОУ «УКЦ «Интерфейс».

Слушателям, успешно освоившим соответствующую Программу и прошедшие итоговую аттестацию, выдается удостоверение о повышении квалификации на бланке, образец которого самостоятельно устанавливается организацией.

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

Оценочные материалы для промежуточной аттестации по Программе разрабатываются в форме практических занятий и опроса после изучения каждого модуля.

Оценочные материалы для итоговой аттестации по Программе разрабатываются в форме опроса.

Контрольные задания и вопросы для оценки знаний и навыков слушателей задаются и выполняются в следующих областях:

- Законодательство Российской Федерации в области защиты информации.
- Правовые основы наличия на предприятии конфиденциальной информации.
- Информация, доступ к которой не может быть ограничен.
- Порядок создания корпоративной нормативно-правовой базы по защите информации.
- Создание службы информационной безопасности (СИБ).
- Порядок проведения аудита информационной безопасности на предприятии.
- Структура конфиденциальных информационных массивов
- Угрозы информационным ресурсам и варианты их реализации.
- Основные направления защиты конфиденциальной информации.
- Организационные мероприятия по защите конфиденциальной информации.
- Анализ информационных ресурсов на предприятии.
- Режимные, технические и инженер но-технические мероприятия по защите конфиденциальной информации.
- Создание внутриобъектового и пропускного режимов.
- Физическая защита охраняемых информационных ресурсов.
- Способы хранения информации вне территории предприятия.
- Кадровые мероприятия по защите конфиденциальной информации.
- ИТ-мероприятия по защите конфиденциальной информации.
- Правовые мероприятия по защите конфиденциальной информации.

- Международные и национальные стандарты безопасности информационных систем.
- Виды юридической ответственности за разглашение конфиденциальной информации, а также за ее незаконное получение.
- Международные конвенции по защите персональных данных физических лиц.
- Законодательство РФ в сфере персональных данных.
- Права субъекта персональных данных и обязанности оператора персональных данных.
- Порядок получения, хранения, предоставления и уничтожения (обезличивания) персональных данных.
- Организационные, технические и инженер но-технические мероприятия, проводимые при обработке персональных данных.
- Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, и их защита.
- Особенности обработки персональных данных, осуществляемой в информационных системах персональных данных.
- Требования к материальным носителям биометрических персональных данных.
- Пошаговый алгоритм действий по созданию на предприятии системы обработки персональных данных, удовлетворяющей требованиям регуляторов.
- Административный регламент исполнения государственной функции по осуществлению государственного контроля за соответствием обработки персональных данных требованиям законодательства.
- Права и обязанности должностных лиц, осуществляющих государственный контроль *n* лиц, в отношении которых осуществляются мероприятия по контролю.
- Психологические приемы общения с проверяющими.
- Подготовительные мероприятия перед созданием режима коммерческой тайны.
- Составление перечня сведений, составляющих коммерческую тайну.
- Установление сроков защиты информации, составляющей коммерческую тайну.
- Изменения и дополнения, вносимые в нормативно-правовые документы предприятия при введении режима коммерческой тайны.
- Определение перечня должностей, при назначении на которые сотрудники будут допущены к коммерческой тайне. Практические рекомендации по составлению перечня.
- Обязательства сотрудников по сохранению коммерческой тайны на предприятии.
- Особенности включения в режим коммерческой тайны информации, представленной в электронном виде.
- Защита коммерческой тайны.
- Особенности создания режима коммерческой тайны в организациях, представляющих разные сферы бизнеса (промышленные предприятия, сфера услуг и т.д.).
- Соблюдение режима коммерческой тайны в гражданско-правовых отношениях с контрагентами.
- Создание конфиденциального делопроизводства.