ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«АКАДЕМИЯ ИНФОВОТЧ»

Утверждена

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0238DBC800C9B04981437026D4A6E6EAF2
Владелец: ХАРИТОНОВ СЕРГЕЙ ВЛАДИМИРОВИЧ
Действителен: с 29.11.2023 до 28.02.2025

Генеральный директор
С.В. Харитонов

МП

Дополнительная профессиональная программа повышения квалификации «Персональные данные в действии»

Форма обучения: заочная
с применением дистанционных образовательных технологий

Москва 2024

Оглавление

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая образовательная программа (далее – Программа) представляет собой совокупность требований, обязательных при реализации программы дополнительного профессионального образования повышения квалификации «Персональные данные в действии».

Программа разработана в соответствии с требованиями профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н, также на основании Приказа Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. № 499 г. Москва "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам" и на основании Федерального закона "Об образовании в Российской Федерации" от 29.12.2012 № 273-ФЗ.

Цели:

- формирование знаний и навыков по вопросам применения законодательства в сфере защиты персональных данных, организации защиты персональных данных, применения действующей нормативной базы в области обеспечения безопасности информации, разработки и применения внутренних нормативных документов организации по вопросам защиты персональных данных.
- практическая подготовка по защите персональных данных и обеспечению их безопасной обработки в информационных системах персональных данных (ИСПДн), построенных на базе компьютерных систем и сетей.

Категория слушателей:

- руководители подразделений по защите персональных данных
- ответственные специалисты за организацию обработки персональных данных
- специалисты по защите информации I категории
- специалисты по защите информации II категории
- специалисты по защите информации
- администраторы информационной безопасности
- специалисты комплаенс информационной безопасности
- юрисконсульты

Организационно-педагогические условия

Образовательный процесс осуществляется на основании учебного плана и регламентируется расписанием занятий для каждого слушателя.

Срок обучения: 58/4/1 (ак. час, нед., мес.).

Режим занятии: 32 академических часа самостоятельного обучения, 24 академических часа видеолекции с использованием дистанционных образовательных технологий, 2 академических часа итоговой аттестации с использованием дистанционных образовательных технологий.

Форма обучения: заочная с применением дистанционных образовательных технологий

Характеристика профессиональной деятельности слушателей

Область профессиональной деятельности слушателей (на основании «Реестра областей и видов профессиональной деятельности» Минтруд России):

- Обеспечение безопасности информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости.
- Руководители в области определения политики и планирования деятельности.

Специалист по защите персональных данных от утечек готовится к следующим видам деятельности: к участию в организации оценки рисков информационной безопасности, классификации и оценке угроз информационной безопасности для объекта информатизации, разработке политик безопасности, разработке нормативных документов с учётом законодательства в области защиты персональных данных, к участию в обеспечении безопасности информации с учетом требования эффективного функционирования автоматизированной системы, к участию в выявлении угроз безопасности информации в автоматизированных системах, к участию в принятии мер защиты информации при выявлении новых угроз безопасности информации в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Требования к результатам освоения дополнительной профессиональной образовательной программы

Специалист должен обладать общими компетенциями, включающими в себя способность:

- Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес.
- Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
- Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

- Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий.

Специалист должен обладать профессиональными компетенциями, соответствующими основным видам профессиональной деятельности:

- Применять действующую нормативную базу в области обеспечения безопасности информации.
- Разрабатывать модели угроз безопасности информации и модели нарушителя в автоматизированных системах.
- Разрабатывать модели автоматизированных систем и подсистем безопасности автоматизированных систем.
- Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации.
- Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах.
- Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.
- Анализировать характер обрабатываемой информации и определять перечень информации, подлежащей защите.
- Формировать разделы технических заданий на создание систем защиты информации автоматизированных систем.
- Планировать мероприятия по обеспечению защиты информации в автоматизированной системе.
- Определять требуемый класс (уровень) защищенности автоматизированной системы.
- Вносить изменения в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы.
- Выявлять угрозы безопасности информации в автоматизированных системах.
- Принимать меры защиты информации при выявлении новых угроз безопасности информации.
- Анализировать недостатки в функционировании системы защиты информации автоматизированной системы.
- Определять комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем.

- Определять оценку возможностей внешних и внутренних нарушителей
- Обосновывать перечен сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы.
- Проводить анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации.

Требование к слушателям

Требования к образованию и обучению	Высшее профессиональное образование/среднее профессиональное образование

Для реализации программы задействован следующий кадровый потенциал:

Преподаватели учебных дисциплин - обеспечивается необходимый уровень компетенции преподавательского состава, включающий высшее образование в области соответствующей дисциплины программы или высшее образование в иной области и стаж преподавания по изучаемой тематике не менее трех лет; использование при изучении дисциплин программы эффективных методик преподавания, предполагающих выполнение слушателями практических заданий.

Административный персонал - обеспечивает условия для эффективной работы педагогического коллектива, осуществляет контроль и текущую организационную работу.

Информационно-технологический персонал - обеспечивает функционирование информационной структуры (включая ремонт техники, оборудования, макетов иного технического обеспечения образовательного процесса).

Содержание программы повышения квалификации определяется учебным планом и календарным учебным графиком программы дисциплин (модулей), требованиями к итоговой аттестации и требованиями к уровню подготовки лиц, успешно освоивших Программу.

Текущий контроль знаний проводится в форме наблюдения за работой обучающихся и контроля их активности на образовательной платформе, проверочного тестирования.

Промежуточный контроль знаний, полученных обучающимися посредством самостоятельного обучения (освоения части образовательной программы), проводится в виде тестирования и оценки выполнения практических работ.

Итоговая аттестация по Программе проводится в форме зачета посредством тестирования и должна выявить теоретическую и практическую подготовку специалиста.

Слушатель допускается к итоговой аттестации после самостоятельного изучения дисциплин Программы в объеме, предусмотренном для обязательных внеаудиторных занятий и подтвердивший самостоятельное изучение сдачей тестов, а также выполнением практических работ.

Лица, освоившие Программу и успешно прошедшие итоговую аттестацию, получают удостоверение о повышении квалификации.

Оценочными материалами по Программе являются блоки контрольных вопросов и используемые при текущем контроле знаний (тестировании), задания для практических работ для промежуточной аттестации.

Методическими материалами к Программе являются нормативные правовые акты и регуляторные требования в области защиты персональных данных, положения которых изучаются при освоении дисциплин Программы. Перечень методических материалов приводится в рабочей программе образовательной организации.

УЧЕБНЫЙ ПЛАН
ПО
ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЕ
повышения квалификации

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ДЕЙСТВИИ.
(профстандарт «Специалист по защите информации в автоматизированных системах»)

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции с использованием дистанционных технологий (самостоятельная работа)	Внеаудиторная (самостоятельная работа)	Промежуточная/ итоговая аттестация	
1	**Нормативные и правовые основы защиты персональных данных**	**9**	2	5	2	Тестирование, Практическая работа
2	**Ключевые нормативные акты организации по защите персональных данных**	**12**	4	5	3	Тестирование, Практическая работа
3	**Организация защиты персональных данных: теория и практика**	**18**	6	9	3	Тестирование, Практическая работа
4	**Отраслевые кейсы. Опыт защиты персональных данных от ведущих экспертов по информационной безопасности**	**17**	12	4	1	Тестирование

5	**ИТОГОВАЯ АТТЕСТАЦИЯ**	**2**			2	Зачет
	Всего:	**58**	**24**	**23**	**11**	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
ПО
ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЕ
повышения квалификации

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ДЕЙСТВИИ.

(профстандарт «Специалист по защите информации в автоматизированных системах»)

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции с использованием дистанционных технологий (самостоятельная работа)	Внеаудиторная (самостоятельная работа)	Промежуточная /итоговая аттестация	
1	**Нормативные и правовые основы защиты персональных данных**	**9**	**2**	**5**	**2**	Тестирование, Практическая работа
1.1	Информация ограниченного доступа. Место и роль персональных данных в организации	1,35	0,35	1		
1.2	Основные регуляторы и их полномочия	2,45	0,45	2		
1.3	Основы правового регулирования в области защиты ПДн	3,2	1,2	2		
2	**Ключевые нормативные акты организации по защите персональных данных**	**10**	**4**	**5**	**3**	Тестирование, Практическая работа
2.1	Правовые основания для обработки ПДн	1,3	0,3	1		

2.2	Ответственность за нарушение законодательства в области персональных данных	2,3	1,3	1		
2.3	Перечень внутренних НПА организации при защите ПДн	1,7	0,7	1		
2.4	Политика в отношении обработки ПДн	1,5	0,5	1		
2.5	Правоприменительная практика по привлечению к ответственности сотрудников за нарушения в области защиты персональных данных	2,2	1,2	1		
3	**Организация защиты персональных данных: теория и практика**	**18**	**6**	**9**	**3**	Тестирование, Практическая работа
3.1	Инциденты при обработке персональных данных. Регламент реагирования. Уведомления регулятора	2,5	0,5	2		
3.2	Управление рисками компьютерной безопасности	4,2	2,2	2		
3.3	Организация защиты персональных данных в организации	1,6	0,6	1		
3.4	Проведение обследования организации для выявления угроз, перечня и объёмов персональных данных в кис	1,4	0,4	1		
3.5	Определение уровня защищенности и угроз ИБ	1,4	0,4	1		
3.6	GDPR и трансграничная передача	1,6	0,6	1		
4	**Отраслевые кейсы. Опыт защиты персональных**	**17**	**12**	**4**	**1**	Тестирование

	данных от ведущих экспертов по информационной безопасности					
4.1	Отраслевой кейс: маркетплейс крупной корпорации	4	3	1		
4.2	Отраслевой кейс: крупная компания - производитель ПО	4	3	1		
4.3	Отраслевой кейс: Опыт организации защиты ПДн при трансграничной передаче данных	4	3	1		
4.4	DLP-системы для защиты персональных данных: возможности, внедрение, практика применения	4	3	1		
5	**ИТОГОВАЯ АТТЕСТАЦИЯ**	**2**			**2**	**Зачет**
	Всего:	**58**	**24**	**23**	**11**	

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный график обучения является примерным, составляется и утверждается для каждого слушателя.

Срок освоения программы - 4 недели. Начало обучения - по мере набора слушателей. Примерный режим занятий: в среднем 2,0 академических часа в день. Промежуточная и итоговая аттестации проводятся согласно графику.

№	Наименование модулей / дни	ВР	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	**Нормативно-правовая база для защиты персональных данных.**	**СР**	1	1	1	2	2	2																								
2	**Организационно-правовые вопросы защиты персональных данных в организации**	**СР**							2	2	2	2	2																			
3	**Организация защиты персональных данных: теория и практика**	**СР**												2	2	2	2	2	2	2	2	2										
4	**Отраслевые кейсы: опыт организация и ведения работ по защите ПДн**	**СР**																					2	2	2	2	2	2	2	2	1	
5	**Итоговая аттестация**																															2

Рабочая программа учебной дисциплины
«Нормативные и правовые основы защиты персональных данных»

Цель: обеспечение глубоких знаний обучающихся в области нормативно-правовой базы по работе с информацией ограниченного доступа, иерархии нормативных правовых актов в России в области защиты информации, понимание ключевых терминов и определений в области персональных данных, перечня полномочий регуляторных органов, теории и практики прохождения проверочных мероприятий, юридические основания для обработки персональных данных в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.
- Знать ключевые нормативные и правовые акты в области защиты персональных данных, их иерархию.
- Понимать юридические основания для обработки персональных данных в организации.

Место дисциплины в структуре программы

Слушатели получают основу для понимания юридических и нормативных основ вопросов защиты персональных данных в России: знакомятся с нормативно-правовой базой в сфере защиты персональных данных, с ключевыми регуляторными документами, стандартами, терминологией, определениями.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Информацию ограниченного доступа. Термины и определения.
- Ключевые положения федеральных законов в области защиты информации.
- Федеральный закон ФЗ-152 «О персональных данных».
- Основные требования нормативных правовых актов и методических документов ФСБ России, ФСТЭК России и Роскомнадзора России по защите персональных данных.
- Перечень и полномочия регуляторных и надзорных органов в сфере защитыперсональных данных и информации ограниченного доступа.
- Вопросы использования и сертификации средств защиты информации.

Уметь:

- Использовать знание нормативно-правовой базы при прохождении проверочных мероприятий в области персональных данных.

- Комбинировать методы сбора требований с целью обеспечения полноты и оперативности получения информации.
- Определять информацию, подлежащую защите, порядок хранения и передачи информации, подлежащей защите.
- Определять угрозы защищаемой информации, а также технологии и способы предотвращения утечки защищаемой информации.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 9 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 5 академических часов.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции с использованием дистанционных технологий (самостоятельная работа)	Внеаудиторная (самостоятельная работа)	Промежуточная аттестация	
1	**Нормативные и правовые основы защиты персональных данных**	**9**	**2**	**5**	**2**	Тестирование, Практическая работа
1.1	Информация ограниченного доступа. Место и роль персональных данных в организации	1,35	0,35	1		
1.2	Основные регуляторы и их полномочия	2,45	0,45	2		
1.3	Основы правового регулирования в области защиты ПДн	3,2	1,2	2		

Тема 1.1 Информация ограниченного доступа. Место и роль персональных данных в организации

- Информация ограниченного доступа. Термины и определения.
- Место и роль персональных данных в организации.
- Правовая база защиты конфиденциальной информации.
- Категории персональных данных.
- Категории субъектов ПДн.

Тема 1.2. Основные регуляторы и их полномочия

- Основные регуляторные органы.
- Полномочия регуляторов.
- Уполномоченный орган по защите прав субъектов ПДн.

- Проверочные мероприятия.
- План прохождения проверочных мероприятий. Проверки РКН, ФСБ, ФСТЭК.
- Подготовка к прохождению проверочных мероприятий.

Тема 1.3. Основы правового регулирования в области защиты ПДн

- Стратегические нормативно-правовые акты.
- Системообразующие документы.
- Ключевые НПА и документы по сертификации СЗИ.
- Ключевые НПА и документы по аттестация объектов информатизации.
- Ключевые НПА и документы по лицензированию деятельности в области ИБ.
- Ключевые НПА и документы, определяющие требования к кадрам.
- НПА, определяющие требования к подразделению по информационной безопасности Организации.
- Ключевые документы ФСТЭК.
- Ключевые стандарты.

Литература

1. А.И. Савченко. Комментарий к федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (постатейный): Деловой двор, 2023.
2. А.В. Спичак Конфиденциальное делопроизводство. Учебное пособие. Нижневартовск: НВГУ, 2020.

Интернет-сайты

https://kontur.ru/articles/6742
https://kontur.ru/articles/1775
https://habr.com/ru/articles/432466/

Рабочая программа учебной дисциплины «Ключевые нормативные акты организации по защите персональных данных»

Цель: обеспечение глубоких знаний обучающихся по нормативным правовым актам в области защиты информации и персональных данных в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Задачи:

- Знать нормативные правовые акты в области обеспечения защиты информации.
- Применять действующую нормативную базу в области обеспечения защиты информации.
- Формировать политику защиты персональных данных.

- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить требования законодательства по составу и содержанию внутренних организационно-распорядительных документов (нормативных актов) организации в области защиты персональных данных, научиться разрабатывать такие документы, знать правовые основания для организации защиты, создавать политику защиты персональных данных в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Нормативные документы, связанные с обработкой ПДн.
- Статьи кодексов РФ, связанные с ответственность за нарушение законодательства в области персональных данных.

Уметь:

- Использовать знание нормативно-правовой базы для разработки внутренних нормативных (организационно-распорядительных) документов в области персональных данных.
- Комбинировать методы сбора требований с целью обеспечения полноты и оперативности получения информации.
- Определять информацию, подлежащую защите, порядок хранения и передачи информации, подлежащей защите.
- Определять степень ответственности за нарушение законодательства в области персональных данных.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 12 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 5 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции с использо-ванием дистанци-онных технологий (самостоя-	Внеауди-торная (самостоя-тельная работа)	Промеж у-точная атте-стация	

			тельная работа)			
2	**Ключевые нормативные акты организации по защите персональных данных**	**12**	**4**	**5**	**3**	Тестирование, Практическая работа
2.1	Правовые основания для обработки ПДн	1,3	0,3	1		
2.2	Ответственность за нарушение законодательства в области персональных данных	2,3	1,3	1		
2.3	Перечень внутренних нормативных актов организации при защите ПДн	1,7	0,7	1		
2.4	Политика в отношении обработки ПДн	1,5	0,5	1		
2.5	Правоприменительная практика по привлечению к ответственности сотрудников за нарушения в области защиты персональных данных	2,2	1,2	1		

Тема 2.1 Правовые основания для обработки ПДн

- Термины и определения.
- Основания для обработки ПДн. Общие.
- Основания для обработки ПДн. Трудовые отношения. Особенности.
- Основания для обработки ПДн. Учебные заведения.
- Направление уведомления о начале обработки ПДн. Исключения.
- Особенности обработки разрешенных для распространения ПДн.

Тема 2.2 Ответственность за нарушение законодательства в области персональных данных

- Основные моменты, учитываемые при разработке НПА.
- Нормативные документы, на основании которых разрабатывается внутренняя документация.
- Виды документов, разрабатываемых в организации.
- Перечень основных нормативных актов в организации. Общие.
- Перечень основных нормативных актов в организации. Приказы.
- Перечень основных нормативных актов в организации. Регламенты.

- Перечень основных нормативных актов в организации. Инструкции.
- Перечень основных нормативных актов в организации. Журналы и Формы.
- Перечень основных нормативных актов в организации. Акты.
- Пояснения необходимости выборочных нормативных актов в организации.

Тема 2.3 Перечень внутренних нормативных актов организации при защите ПДн.

- Обязанности организации.
- Внутренние нормативные документы организации.
- Жизненный цикл ПДн в организации и его нормативное обеспечение.

Тема 2.4 Политика в отношении обработки ПДн.

- Политика в отношении обработки ПДн.
- Права и обязанности оператора.

Тема 2.5 Правоприменительная практика по привлечению к ответственности сотрудников за нарушения в области защиты персональных данных.

- Современная уголовная практика привлечения сотрудников к ответственности за нарушения в области ПДн.
- Основание для привлечения к уголовной ответственности за нарушение законодательства в области ПДн по материалам уголовных дел.

Литература

1. А.И. Савченко. Комментарий к федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (постатейный): Деловой двор, 2023.
2. 3. А.В. Спичак Конфиденциальное делопроизводство. Учебное пособие. Нижневартовск: НВГУ, 2020.
3. А. В. Терехов и др. Информационная безопасность и правовые основы защиты персональных данных [Электронное издание] : учебное пособие / А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2023.

Интернет-сайты

1. https://www.consultant.ru/document/cons_doc_LAW_61801/
2. https://kontur.ru/articles/1775
3. https://legal-box.ru/152fz-docs

Рабочая программа учебной дисциплины
«Организация защиты персональных данных: теория и практика»

Цель: обеспечение глубоких знаний обучающихся по: управлению рисками информационной безопасности, планированию, разработке, применению комплекса мер по защите персональных данных в организации, используя актуальную нормативную правовую базу в области защиты информации в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Задачи:

- Планировать мероприятия по обеспечению защиты информации в автоматизированной системе.
- Определять требуемый уровень защищенности автоматизированной системы.
- Выявлять уязвимости информационно-технологических ресурсов.
- Оценивать информационные риски безопасности информации.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям познакомиться с методами по управлению рисками информационной безопасности, комплексом организационных мероприятий, теорией и практикой организации защиты персональных данных в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Нормативные документы, связанные с обработкой ПДн и аттестацией объектов информатизации.
- Методику определения уровня защищенности персональных данных.
- Полномочия организации и этапы при проведении аудита и аттестации.
- Основы нормативного регулирования при использовании GDPR и трансграничной передачи персональных данных.

Уметь:

- Организовывать процессы защиты персональных данных в организации.
- Управлять рисками информационной безопасности.

- Проводить обследования организации для выявления угроз, перечня и объёмов персональных данных.
- Определять уровни защищенности, угрозы информационной безопасности.
- Определять информацию, подлежащую защите, порядок хранения и передачи информации, подлежащей защите.
- Определять полноту и достоверность проведения аттестации и аудита.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 18 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 9 академических часов.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции с использованием дистанционных технологий (самостоятельная работа)	Внеаудиторная (самостоятельная работа)	Промежуточная аттестация	
3	**Организация защиты персональных данных: теория и практика**	**18**	**6**	**9**	**3**	Тестирование, Практическая работа
3.1	Инциденты при обработке персональных данных. Регламент реагирования. Уведомления регулятора	2,5	0,5	2		
3.2	Управление рисками компьютерной безопасности	4,2	2,2	2		
3.3	Организация защиты персональных данных в организации	1,6	0,6	1		
3.4	Проведение обследования организации для выявления угроз, перечня и объёмов персональных данных в информационных системах	1,4	0,4	1		
3.5	Определение уровня защищенности и угроз ИБ	1,4	0,4	1		

3.6	GDPR и трансграничная передача	1,6	0,6	1		

Тема 3.1 Инциденты при обработке персональных данных. Регламент реагирования. Уведомления регулятора

- Понятие инцидента в отношении ПДн, виды инцидентов, источники информации об инциденте.
- Практика по работе с инцидентами.
- Уведомление Уполномоченного органа об инциденте.

Тема 3.2 Управление рисками компьютерной безопасности (далее – КБ)

- Методология управления риском КБ и перечень внутренних нормативных документов.
- Модели оценки рисков ИБ для организация разных видов деятельности. Оценка потенциального ущерба.
- Обоснование принятия мер по защите информации в организации.

Тема 3.3 Организация защиты персональных данных в организации

- Этапы организации защиты.
- Разработка модели угроз ИБ.

Тема 3.4 Проведение обследования организации для выявления угроз, перечня и объёмов персональных данных в информационных системах

- Стадии построения системы защиты информации объекта информатизации.
- Этапы проведения аудита. Цели, задачи.
- Аудит в сфере защиты персональных данных. Анализ документации. Анализ защищенности систем. Привлечение сторонних организаций.
- Объекты аттестации. Проведение аттестации. Этапы аттестации.

Тема 3.5 Определение уровня защищенности и угроз ИБ

- Понятие ИСПД.
- Определение типов угроз.
- Определение уровня защищенности.

Тема 3.6 GDPR и трансграничная передача

- Введение в GDPR.
- Трансграничная передача персональных данных.

Литература

1. А.И. Савченко. Комментарий к федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (постатейный): Деловой двор, 2023
2. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018.
3. А.В. Спичак Конфиденциальное делопроизводство. Учебное пособие. Нижневартовск: НВГУ, 2020
4. А. В. Терехов и др. Информационная безопасность и правовые основы защиты персональных данных [Электронное издание] : учебное пособие / А. В. Терехов, В. Н.

Чернышов, А. В. Платенкин, А. В. Селезнев. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2023.

Сайты

1. https://www.consultant.ru/document/cons_doc_LAW_61801/
2. https://kontur.ru/articles/6742
3. https://pdmaster.ru/services/audit-personalnyh-dannyh-2/

Рабочая программа учебной дисциплины
«Отраслевые кейсы. Опыт защиты персональных данных от ведущих экспертов по информационной безопасности»

Цель: обеспечение глубоких знаний обучающихся по: практике организации защиты персональных данных в организациях различных отраслей деятельности, применению различных организационных мер защиты информации в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Задачи:

- Выявлять степень участия персонала в обработке защищаемой информации.
- Планировать мероприятия по обеспечению защиты персональных данных в организации.
- Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Слушатели получают передовую экспертизу и реальные отраслевые сценарии по организации защиты персональных данных в различных организациях, знакомятся с лучшими практиками, типовыми ошибками и лучшими подходами по применению нормативно-правовой базы в сфере защиты персональных данных на практике.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 17 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 4 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции с использованием дистанционных технологий (самостоятельная работа)	Внеаудиторная (самостоятельная работа)	Промежуточная аттестация	

4	**Отраслевые кейсы. Опыт защиты персональных данных от ведущих экспертов по информационной безопасности**	**17**	**12**	**4**	**1**	Тестирование
4.1	Отраслевой кейс: маркетплейс крупной корпорации	4	3	1		
4.2	Отраслевой кейс: крупная компания - производитель ПО	4	3	1		
4.3	Отраслевой кейс: Опыт организации защиты ПДн при трансграничной передаче данных	4	3	1		
4.4	DLP-системы для защиты персональных данных: возможности, внедрение, практика применения	4	3	1		

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации.
- Организационные меры по защите информации.
- Принципы формирования и реализации политики безопасности информации в автоматизированных системах.
- Последствия от нарушения свойств безопасности информации.
- Способы реализации угроз безопасности в автоматизированных системах.

Уметь:

- Определять комплекс мер для обеспечения информационной безопасности в автоматизированных системах.
- Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем.
- Классифицировать и оценивать угрозы безопасности информации для автоматизированной системы.
- Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем.

Литература

1. А.И. Савченко. Комментарий к федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (постатейный): Деловой двор, 2023
2. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018.

3. А.В. Спичак Конфиденциальное делопроизводство. Учебное пособие. Нижневартовск: НВГУ, 2020

ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

Формы аттестации

Для проведения промежуточной и итоговой аттестации программы разработан фонд оценочных средств по программе, являющийся неотъемлемой частью учебно-методического комплекса.

Объектами оценивания выступают:

- степень освоения теоретических знаний;
- уровень овладения практическими умениями и навыками по всем видам учебной работы, активность на занятиях.

Текущий контроль знаний проводится в форме наблюдения за работой обучающихся и контроля их активности на образовательной платформе, проверочного тестирования.

Промежуточная аттестация - оценка качества усвоения обучающимися содержания учебных блоков непосредственно по завершении их освоения, проводимая в форме зачета посредством тестирования и выполнения практических работ.

Итоговая аттестация - процедура, проводимая с целью установления уровня знаний, обучающихся с учетом прогнозируемых результатов обучения и требований к результатам освоения образовательной программы. Итоговая аттестация обучающихся осуществляется в форме зачета посредством тестирования.

Слушатель допускается к итоговой аттестации после изучения тем образовательной программы в объеме, предусмотренном для лекционных и практических занятий.

Лицам, освоившим образовательную программу повышения квалификации «Персональные данные в действии» и успешно прошедшим итоговую аттестацию, выдается **удостоверение о повышении квалификации** установленного образца с указанием названия программы, календарного периода обучения, длительности обучения в академических часах.

Для аттестации обучающихся на соответствие их персональных достижений требованиям соответствующей ОП созданы фонды оценочных средств, включающие типовые задания, тесты и методы контроля, позволяющие оценить знания, умения и уровень приобретенных компетенций.

Фонды оценочных средств соответствуют целям и задачам программы подготовки специалиста, учебному плану и обеспечивают оценку качества общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся.

Критерии оценки обучающихся

Предмет оценивания (компетенции)	**Объект оценивания (навыки)**	**Показатель оценки (знания, умения)**
Специалист должен обладать общими компетенциями (ОК), включающими в себя способность: - Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес. - Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. - Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. - Осуществлять поиск и использование информации, необходимой для эффективного выполнения - профессиональных задач,	**Специалист должен обладать профессиональными компетенциями (ПК), соответствующими основным видам профессиональной деятельности:** - Применять действующую нормативную базу в области обеспечения безопасности информации - Разрабатывать модели угроз безопасности информации и модели нарушителя в автоматизированных системах - Разрабатывать моделей автоматизированных систем и подсистем безопасности автоматизированных систем - Разрабатывать проектов нормативных документов, регламентирующих работу по защите информации - Разрабатывать предложений по совершенствованию системы управления безопасностью	**Знания:** - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - Принципы формирования политики информационной безопасности в автоматизированных системах - Нормативные правовые акты в области защиты информации - Организационные меры по защите информации - Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации - Угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах **Умения:** - Формировать политику

профессионального и личностного развития. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. Ориентироваться в условиях частой смены технологий в профессиональной деятельности. Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий	информации в автоматизированных системах Анализировать характер обрабатываемой информации и определение перечня информации, подлежащей защите Планирование мероприятий по обеспечению защиты информации в автоматизированной системе Определение требуемого класса (уровня) защищенности автоматизированной системы Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы Выявление угроз безопасности информации в автоматизированных системах Принятие мер защиты информации при выявлении новых угроз безопасности информации	безопасности программных компонентов автоматизированных систем Разрабатывать модели угроз безопасности информации и нарушителей в автоматизированных системах Классифицировать и оценивать угрозы информационной безопасности Определять класс защищенности автоматизированных систем и ее составных частей

Оценка качества освоения учебных модулей проводится в процессе промежуточной аттестации в форме тестирования и выполнения практических работ.

Оценка	Критерии оценки
Зачтено	Оценка **«Зачтено»** выставляется слушателю, если он твердо знает материал курса, грамотно и по существу использует его, не допуская существенных неточностей в ответе на тестовые вопросы. Не менее 50% правильных ответов при решении тестов. Не более 2-х ошибок при решении практических задач.
Не зачтено	Оценка **«Не зачтено»** выставляется слушателю, который не знает значительной части программного материала, допускает существенные ошибки. Менее 50% правильных ответов при решении тестов. Более 2-х ошибок при решении практических задач.

Оценка качества освоения учебной программы проводится в процессе итоговой аттестации в форме зачета посредством тестирования.

Оценка (стандартная)	**Критерии оценки**
Зачтено	Оценка **«Зачтено»** выставляется слушателю, продемонстрировавшему твердое и всесторонние знания материалы, умение применять полученные в рамках занятий практические навыки и умения. Достижения за период обучения и результаты текущей аттестации демонстрировали отличный уровень знаний и умений слушателя. Не менее 70% правильных ответов при решении тестов.
Не зачтено	Оценка **«Не зачтено»** выставляется слушателю, который в недостаточной мере овладел теоретическим материалом по дисциплине, допустил ряд грубых ошибок при выполнении практических заданий, а также не выполнил требований, предъявляемых к промежуточной аттестации. Достижения за период обучения и результаты текущей аттестации демонстрировали неудовлетворительный уровень знаний и умений слушателя. Менее 70% правильных ответов при решении тестов.

Фонд оценочных средств
Оценочные материалы

ТЕСТОВЫЕ ВОПРОСЫ

Дисциплина «Нормативные и правовые основы защиты персональных данных»

1. Порядок и условия взаимодействия с Роскомнадзором приведены в …
- Приказе Роскомнадзора от 14 ноября 2022 г. №187;
- Приказе ФСТЭК №21;
- Федеральном законе №152-ФЗ;
- Постановлении Правительства РФ №1119.

2. Что такое информация:
- Сведения (сообщения, данные), переписка, телефонные и телеграфные разговоры;
- Сведения (сообщения, данные) независимо от формы их представления;
- Данные на бумажных и магнитных носителях информации.

3. Что из перечисленного не может быть информаций ограниченного доступа в соответствии с законодательством РФ:
- Паспортные данные гражданина;
- Информация, накапливаемая в открытых фондах библиотек, музеев, архивов;
- Себестоимость продукта и объем сбыта;
- Контактные данные клиентов.

4. Что из перечисленного относится к конфиденциальной информации:
- Персональные данные;
- Служебная тайна;
- Государственная тайна;
- Данные о деятельности предпринимателя (юридического лица, ИП).

5. Согласно Федеральному закону от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» информация делится на...
- общедоступную и ограниченного доступа;
- секретную и несекретную;
- ограниченную и секретную;
- общедоступную и недоступную;
- общедоступную и секретную.

6. В каком документе определены требования к защите персональных данных при их обработке в информационных системах персональных данных?
- Постановление Правительства РФ №1119;
- Постановление Правительства РФ №687;
- Гражданский кодекс РФ.

7. В каком документе устанавливаются требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных?
- Федеральный закон №152-ФЗ;
- Постановление Правительства РФ от 01.11.2012 №1119;
- Федеральный закон №149.

8. Выберете и подставьте верные ответы из списков. Информационная система является информационной системой, обрабатывающей (специальные, биометрические, иные, общедоступные) категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния (эффекта, самочувствия, недвижимости, здоровья), интимной жизни субъектов персональных данных.

Дисциплина «Ключевые нормативные акты организации по защите персональных данных»

1. Выберете верные ответы из списка. Контроль за выполнением требований безопасности организуется и проводится (Роскомнадзором, ФСТЭК России, оператором, уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих (право, лицензию , аттестат) на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 (2, 4) года в сроки, определяемые (оператором, уполномоченным лицом).
2. Сопоставить термины и определения:

Информационная система является информационной системой, обрабатывающей **специальные категории** персональных данных, если в ней ….	обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.
Информационная система является информационной системой, обрабатывающей **биометрические** персональные данные, если в ней ….	обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.
Информационная система является информационной системой, обрабатывающей **общедоступные** персональные данные, если в ней …	обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».
Информационная система является информационной системой, обрабатывающей **иные категории персональных данных**, если в ней ….	не обрабатываются персональные данные, относящиеся к специальным, биометрическим и общедоступным.

3. Какой документ является основополагающим в организации в процессе обработки ПДн и определяет политику оператора?

- Инструкция пользователя информационной системы персональных данных;
- Памятка кадровика;
- Политика оператора в отношении персональных данных;
- Главный регламент оператора в отношении персональных данных;
- Политика защиты от внутренних угроз информационной безопасности.

4. Какой приказ ФСТЭК утверждает требования о защите информации, не составляющей государственную тайну, содержащихся в ГИС?

- Приказ ФСТЭК № 53;
- Приказ ФСТЭК № 21;
- Приказ ФСТЭК № 17;
- Приказ ФСТЭК № 12.

Дисциплина «Организация защиты персональных данных: теория и практика»

1. Лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования называется:
- оператор;
- кадровик;
- пользователь.

2. Может ли организация провести аудит (обследование) организационно-правовой подготовки на соответствие законодательству в области защиты ПДн, если у организации нет лицензии:
- Да;
- Нет.

3. Сколько установлено уровней защищенности в Постановлении Правительства №1119?
- 3;
- 4;
- 5.

4. Сколько типов угроз определено в Постановлении Правительства №1119?
- 3;
- 4;
- 5.

5. К какой категории нарушителей относятся бывшие работники (пользователи)?
- внутренние;
- внешние;
- вообще не рассматриваются при построении модели угроз и нарушителя.

6. Аудит соответствия организации общим требованиям законодательства о персональных данных выполняется в соответствии с …
- 152-ФЗ;
- 1119-ПП;
- 687-ПП;
- Все указанные.

7. Информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям, называются:
- субъектами воздействия;
- объектами воздействия;
- нарушителями.

8. Что такое идентификация риска?
- выявление риска;
- оценка риска;
- митигация риска.

Дисциплина «Отраслевые кейсы.
Опыт защиты персональных данных от ведущих экспертов по информационной безопасности»

1. Цели обработки персональных данных достигнуты, законодательно обоснованных обязательств по дальнейшей обработке нет. Компания должна …
   - Уничтожить персональные данные;
   - Уничтожить персональные данные, составить акт;
   - Уничтожить персональные данные, составить акт и незамедлительно направить его в РКН;
   - Уничтожить персональные данные и носители информации с ПДн;
   - Составить акт об окончании обработки персональных данных.

2. Предполагает ли российское законодательство дисквалификацию руководителя за выявленные нарушения в области защиты персональных данных?
   - Да;
   - Нет;
   - Только при утечках от 100 000 уникальных субъектов.

3. Предполагает ли российское законодательство уголовное преследование руководителя организации за выявленные нарушения в области защиты персональных данных по вине сотрудников?
   - Да;
   - Нет;
   - Только при утечках от 100 000 уникальных субъектов

4. Факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных – это …:
   - Кража персональных данных;
   - Утечка персональных данных;
   - Потеря персональных данных.

5. Какое взыскание может быть наложено на работника, при нарушении правил трудового распорядка?
   - Штраф;
   - Увольнение;
   - Выговор;
   - Замечание;
   - Депремирование.

6. Необходима ли аттестация информационной системы и ввод её в действие?
   - Да, обязательно;
   - Нет, не обязательно;
   - По желанию руководства компании;
   - По требованию надзорных органов.

ИТОГОВАЯ АТТЕСТАЦИЯ

1. Порядок и условия взаимодействия с Роскомнадзором приведены в …:
- Приказе Роскомнадзора от 14 ноября 2022 г. №187;
- Приказе ФСТЭК №21;
- Федеральном законе №152-ФЗ;
- Постановлении Правительства РФ №1119.

2. Что из перечисленного относится к конфиденциальной информации:
- Персональные данные;
- Служебная тайна;
- Государственная тайна;
- Данные о деятельности предпринимателя (юридического лица, ИП).

3. Согласно Федеральному закону от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» информация делится на:
- общедоступную и ограниченного доступа;
- секретную и несекретную;
- ограниченную и секретную;
- общедоступную и недоступную;
- общедоступную и секретную.

4. Цели обработки персональных данных достигнуты, законодательно обоснованных обязательств по дальнейшей обработке нет. Компания должна …
–Уничтожить персональные данные;
–Уничтожить персональные данные, составить акт;
–Уничтожить персональные данные, составить акт и незамедлительно направить его в РКН;
–Уничтожить персональные данные и носители информации с ПДн;
–Составить акт об окончании обработки персональных данных.

5. Какое взыскание может быть наложено на работника, при нарушении правил трудового распорядка?
–Штраф;
–Увольнение;
–Выговор;
–Замечание;
–Депремирование.

6. Необходима ли аттестация информационной системы и ввод её в действие?
–Да, обязательно;
–Нет, не обязательно;
–По желанию руководства компании;
–По требованию надзорных органов.

7. Аудит соответствия организации общим требованиям законодательства о персональных данных выполняется в соответствии с …
- 152-ФЗ;
- 1119-ПП;

- 687-ПП;
- Все указанные.

8. Какой документ является основополагающим в организации в процессе обработки ПДн и определяет политику оператора?
- Инструкция пользователя информационной системы персональных данных;
- Памятка кадровика;
- Политика оператора в отношении персональных данных;
- Главный регламент оператора в отношении персональных данных;
- Политика защиты от внутренних угроз информационной безопасности.

9. В каком документе определены требования к защите персональных данных при их обработке в информационных системах персональных данных?
- Постановление Правительства РФ №1119;
- Постановление Правительства РФ №687;
- Гражданский кодекс РФ.

10. Сколько установлено уровней защищенности в Постановлении Правительства №1119?
- 3;
- 4;
- 5.

11. Сколько типов угроз определено в Постановлении Правительства №1119?
- 3;
- 4;
- 5.

12. Лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования называется:
- оператор;
- кадровик;
- пользователь.

13. Какой приказ ФСТЭК утверждает требования о защите информации, не составляющей государственную тайну, содержащихся в ГИС?
- Приказ ФСТЭК № 53;
- Приказ ФСТЭК № 21;
- Приказ ФСТЭК № 17;
- Приказ ФСТЭК № 12.

14. Что такое идентификация риска?
- выявление риска;
- оценка риска;
- митигация риска.

15. Информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям, называются:
- субъектами воздействия;

- объектами воздействия;
- нарушителями.

ПРАКТИЧЕСКАЯ РАБОТА

Дисциплина «Нормативные и правовые основы защиты персональных данных»

Практическое задание «Определение нормативной базы при работе с заданными типами ИСПДн и персональными данными»

Цель

Научиться определять какой нормативной базой необходимо руководствоваться при работе с заданными типами ИСПДн и персональными данными.

Задание

Необходимо определить правовое основание обработки ПДн разных категорий граждан, а также на какие категории ПДн необходимо взять согласие на обработку ПДн, а на какие нужно взять согласие на распространение.

В одном из государственных ВУЗов проведен аудит информационной безопасности. В ходе проведения аудита выяснилось, что обеспечивать бизнес-процессы ВУЗа позволяют три информационные системы персональных данных (ИСПДн) самого ВУЗа:

- ИС «Работники и штатное расписание» – система учета сотрудников
- ИС «Образовательная среда» – система учета студентов
- ИС «Учет посетителей» – система учета посетителей

На сайте ВУЗа необходимо публиковать данные о преподавателях.

Все ИСПДн ВУЗа находятся на территории Российской Федерации в одном здании.

Здание на регулярной основе охраняется, на вход в здание установлена пропускная система.

Ход работы

1. Ознакомьтесь с заданием;
2. Изучите ФЗ-152 «О персональных данных», ФЗ-273 «Об образовании в Российской Федерации», Трудовой кодекс РФ;
3. Исходя из входной информации, определите правовое основание обработки ПДн;
4. Исходя из входной информации, определите необходимость в согласии на обработку ПДн и в согласии на распространение;
5. Результат впишите в таблицу, прикрепленную вместе с этим файлом на странице задания (файл формата .XLSX с названием «Таблица для заполнения ПР1»).

Наименование ИСПДн	Перечень ПДн
«Работники и штатное расписание»	– Фамилия, Имя, Отчество – Год, месяц и дата рождения – Место рождения – Пол – Реквизиты документа, удостоверяющего личность – Реквизиты водительского удостоверения – Дата и номер доверенности (при наличии выданных доверенностей) – Адрес регистрации – Адрес фактического проживания – Гражданство – ИНН – СНИЛС
«Образовательная среда»	– Фамилия, Имя, Отчество – Пол – Гражданство – Год, месяц и дата рождения – Данные паспорта – Место жительства – Место регистрации – Домашний телефон – Мобильный телефон – E-Mail – СНИЛС – Прочие данные связанные с образовательным процессом
«Учет посетителей»	– Фамилия, Имя, Отчество – Паспортные данные (номер, серия)

Дисциплина «Ключевые нормативные акты организации по защите персональных данных»

Практическое задание «Разработка инструкции для лиц, ответственных за обработку ПДн»

Цель

Научиться разрабатывать инструкции для лиц, ответственных за обработку ПДн.

Задание

Необходимо определить права и обязанности лица, ответственного за обработку ПДн в ВУЗе.

В одном из государственных ВУЗов проведен аудит информационной безопасности. В ходе проведения аудита выяснилось, что обеспечивать бизнес-процессы ВУЗа позволяют три информационные системы персональных данных (ИСПДн) самого ВУЗа и две государственные ИСПДн:

- ИС «Работники и штатное расписание» – система учета сотрудников.
- ИС «Образовательная среда» – система учета студентов.
- ИС «Учет посетителей» – система учета посетителей.
- ФИС Документы об образовании – система учета выданных документов об образовании.
- ФИС Результаты аттестации и приема – система учета данных итоговой аттестации абитуриентов и зачисления в учебные заведения.

На сайте ВУЗа обязательны к опубликованию данные преподавателей (ФИО, должность, квалификация, стаж работы).

Все ИСПДн ВУЗа находятся на территории Российской Федерации в одном здании, к государственным ИСПДн ВУЗ имеет удаленный доступ.

Здание на регулярной основе охраняется, на вход в здание установлена пропускная система.

Наименование ИСПДн	Перечень ПДн
«Работники и штатное расписание»	– Фамилия, Имя, Отчество – Год, месяц и дата рождения – Место рождения – Пол – Реквизиты документа, удостоверяющего личность – Реквизиты водительского удостоверения – Дата и номер доверенности (при наличии выданных доверенностей) – Адрес регистрации – Адрес фактического проживания – Гражданство – ИНН – СНИЛС
«Образовательная среда»	– Фамилия, Имя, Отчество – Пол – Гражданство – Год, месяц и дата рождения – Данные паспорта – Место жительства – Место регистрации – Домашний телефон – Мобильный телефон – E-Mail – СНИЛС – Прочие данные связанные с образовательным процессом
«Учет посетителей»	– Фамилия, Имя, Отчество – Паспортные данные (номер, серия)

Наименование ИСПДн	Перечень ПДн
«ФИС Документы об образовании»	– Фамилия, Имя, Отчество – Год, месяц и дата рождения – Место рождения – Пол – Реквизиты документа, удостоверяющего личность – Реквизиты диплома – Специальность, квалификация – СНИЛС
«ФИС Результаты аттестации и приема»	– Фамилия, Имя, Отчество – Год, месяц и дата рождения – Место рождения – Пол – Реквизиты документа, удостоверяющего личность – Приказ о зачислении и наименование ВУЗа – Результат итоговой аттестации

Ход работы

1. Ознакомьтесь с заданием;

2. Изучите следующий пакет документов:

– Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ

– Постановление Правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 20.03.2012 г. N 211

– Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 г. N 21

– Постановление Правительства Российской Федерации от 01.11.2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

3. Исходя из входной информации, составьте инструкцию для лица, ответственного за обработку ПДн, а также определите функции, задачи, права, ответственность. Результат оформите в виде файла-инструкции

Итоговый результат

Итоговый результат необходимо оформить в виде файла-инструкции для лица, ответственного за обработку ПДн.

Дисциплина «Организация защиты персональных данных: теория и практика»

Практическое задание «Разработка модели угроз и нарушителя согласно Методическому документу ФСТЭК России «Методика оценки угроз безопасности информации»»

Цель. Научиться разрабатывать модель угроз и нарушителя согласно Методическому документу ФСТЭК России «Методика оценки угроз безопасности информации».

Задание.

В одной из крупных государственных поликлиник проведен аудит информационной безопасности. В ходе проведения аудита выяснилось, что обеспечивать бизнес-процессы поликлиники позволяют три информационные системы персональных данных (ИСПДн): «Кадровик», «Пациент», «Учет медикаментов».

Закупка системного и прикладного программного обеспечения (ПО) производится исключительно у доверенных и проверенных поставщиков и вендеров.

Закупка средств защиты информации (СЗИ) производится исключительно у доверенных и проверенных поставщиков и вендеров СЗИ. Установку и настройку осуществляет специализированная организация-лицензиат ФСТЭК России.

В ИСПДн существуют только непривилегированные пользователи, привилегированные пользователи отсутствуют, поскольку данная функция передана на аутсорс (установку и настройку осуществляет специализированная организация-лицензиат ФСТЭК России).

Все ИСПДн находятся на территории Российской Федерации в одном здании.

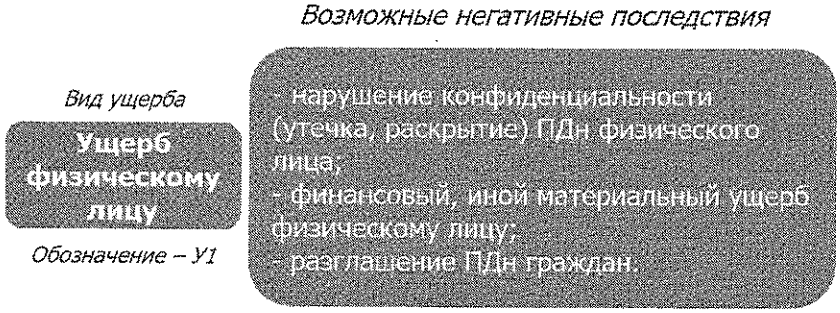
Здание на регулярной основе охраняется, на вход в здание установлена пропускная система.

Наименование ИСПДн	Перечень ПДн	Используемые СЗИ	Системное ПО	Кол-во записей
«Пациент»	– фамилия, имя, отчество; – год, месяц и дата рождения; – место рождения; – пол; – реквизиты документа, удостоверяющего личность; – адрес регистрации; – адрес фактического проживания; – СНИЛС; – Информация о диагнозе; – Анамнез лечения; – Информация о результатах проведенных медицинских исследований, анализов и т.д.	Антивирус. Система управления правами доступа.	ОС Windows	Более 100 000

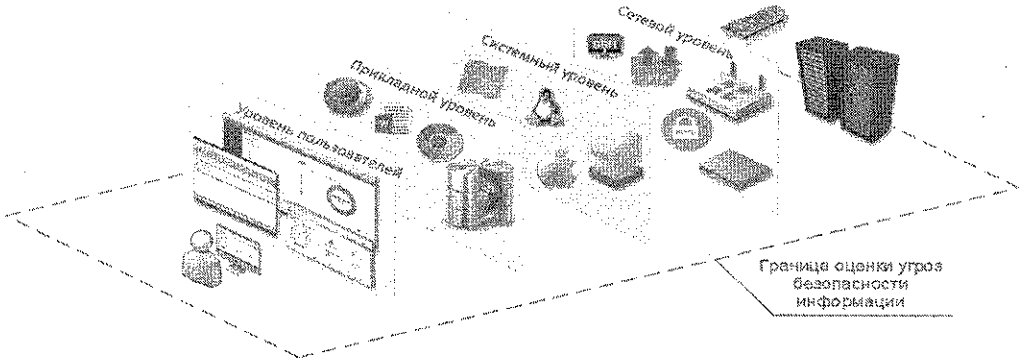
Необходимо для ИСПДн «Пациент» разработать модель угроз и нарушителя.

Ход работы.

1. Ознакомится с заданием.
2. Изучить Методический документ ФСТЭК России «Методика оценки угроз безопасности информации» (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g).
3. Определить негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.
   Например,



4. Определение возможные объекты воздействия угроз безопасности информации. Объекты воздействия определяются на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей.
   Например,



5. Произвести оценку возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.
   Для этого выделить источники угроз безопасности информации и способы реализации (возникновения) угроз безопасности информации.
   5.1 Источниками угроз зачастую являются нарушители (внешние и внутренние). Необходимо определить какие виды и типы нарушителей актуальны для системы, указать их потенциал.
   5.2 Воспользовавшись Банком данных угроз ФСТЭК России (https://bdu.fstec.ru/threat), сформировать перечень угроз безопасности информации и произвести их оценку.

Итоговый результат.

Итоговый результат записать в виде таблицы.

Наименование угрозы	Актуальность

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Требования к квалификации педагогических кадров, представителей предприятий и организаций, обеспечивающих реализацию образовательного процесса

Требования к образованию и обучению лица, занимающего должность преподавателя: высшее образование - специалитет или магистратура, направленность (профиль) которого, как правило, соответствует преподаваемому учебному курсу, дисциплине (модулю).

Дополнительное профессиональное образование на базе высшего образования (специалитета или магистратуры) - профессиональная переподготовка, направленность (профиль) которой соответствует преподаваемому учебному курсу, дисциплине (модулю).

Педагогические работники обязаны проходить в установленном законодательством Российской Федерации порядке обучение и проверку знаний и навыков в области охраны труда.

Рекомендуется обучение по дополнительным профессиональным программам по профилю педагогической деятельности не реже чем один раз в три года.

Требования к опыту практической работы: при несоответствии направленности (профиля) образования преподаваемому учебному курсу, дисциплине (модулю) – наличие у преподавателей опыта работы в области профессиональной деятельности, осваиваемой обучающимися или соответствующей преподаваемому учебному курсу, дисциплине (модулю).

Преподаватель: стаж работы в образовательной организации не менее одного года; при наличии ученой степени (звания) - без предъявления требований к стажу работы.

Особые условия допуска к работе: отсутствие ограничений на занятие педагогической деятельностью, установленных законодательством Российской Федерации.

Прохождение обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также внеочередных медицинских осмотров (обследований) в порядке, установленном законодательством Российской Федерации.

Прохождение в установленном законодательством Российской Федерации порядке аттестации на соответствие занимаемой должности.

Требования к материально-техническим условиям

Образовательный процесс осуществляется с применением дистанционных образовательных технологий, с учетом чего созданы условия для функционирования электронной информационно-образовательной среды.

Требования к оборудованию слушателя для проведения занятий

- персональный компьютер под управлением операционной системы Windows 10 и выше;
- видеокамера, микрофон и аудиосистема (колонки или наушники), подключенные к компьютеру;
- пакет MS Office 2016 и выше;
- выход в Интернет;
- Интернет браузер.

Требования к информационным и учебно-методическим условиям
Список литературы

Нормативные правовые акты

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ
2. Конституция Российской Федерации принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020
3. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ
5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ
6. Федеральный закон "О коммерческой тайне" от 29.07.2004 № 98-ФЗ
7. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ
8. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. N 21
9. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. N 17
10. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15 февраля 2008 г.

Интернет-ресурсы

1. http://www.consultant.ru/
2. https://www.infowatch.ru/
3. https://habr.com/ru/all/
4. https://мойассистент.рф