ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС)
Академия корпоративного образования (АКО)
Институт дополнительного профессионального образования (ИДПО)

УТВЕРЖДАЮ:
Директор АКО УрГУПС
_____ И.Л. Васильев
«01» 07 2022 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Актуальные проблемы защиты информации и коммерческой тайны на железнодорожном транспорте. Защита экономических интересов ОАО «РЖД» и Свердловской железной дороги

Екатеринбург
2022

Содержание

Общая характеристика программы

Программа «Актуальные проблемы защиты информации и коммерческой тайны на железнодорожном транспорте. Защита экономических интересов ОАО «РЖД» и Свердловской железной дороги» (далее ДПП ПК) предназначена для дополнительного профессионального образования путем освоения программы повышения квалификации (ПК) различными категориями руководителей и специалистов ОАО «РЖД» по вопросам защиты информации, коммерческой тайны и персональных данных на железнодорожном транспорте.

ДПП разработана в ИДПО АКО УрГУПС и утверждается только директором АКО, если иное не установлено Федеральным законом «Об образовании в Российской Федерации» от 29.12.12 № 273-ФЗ.

Программа рассчитана на широкий круг руководителей, а также на специально назначенных работников, занимающихся организацией защиты коммерческой тайны или ведением делопроизводства документов с грифом «коммерческая тайна» в подразделениях дороги, других филиалах и ДЗО ОАО «РЖД», расположенных в границах Свердловской железной дороги.

Настоящая ДПП разработана в соответствии с приказом Министерства образования и науки РФ от 1 июля 2013г. №499 «Порядок организации и осуществления образовательной деятельности по дополнительным профессиональным программам», с распоряжением ОАО «РЖД» от 19.01.2016г. №86р «Положение о требованиях к дополнительным профессиональным программам, заказываемым ОАО «РЖД», с учетом потребности открытого акционерного общества «Российские железные дороги» в дополнительном профессиональном образовании работников.

ДПП ПК разработана в соответствии с профессиональным стандартом 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 15.09.2016 N 522н.

Реализация программы направлена на совершенствование компетенций, необходимых для профессиональной деятельности, и повышение профессионального уровня в рамках имеющейся квалификации.

Оптимальное количество слушателей в группе 20 человек.

ДПП ПК трудоемкостью 40 часов реализуется по очной форме обучения. Срок освоения 5 дней.

К освоению ДПП ПК допускаются лица, имеющие среднее профессиональное образование и (или) высшее образование; лица, получающие среднее профессиональное и (или) высшее образование. При освоении ДПП ПК параллельно с получением среднего профессионального образования и (или) высшего образования удостоверение о повышении квалификации выдается одновременно с получением соответствующего документа об образовании и о квалификации.

Освоение ДПП ПК завершается итоговой аттестацией слушателей в виде тестирования по системе «зачет / незачет». Лицам, успешно освоившим ДПП ПК и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

1 Цель

Совершенствование профессиональных компетенций руководителя и специалиста, необходимых для эффективной работы в области защиты конфиденциальной информации, коммерческой тайны и персональных данных работников железнодорожного транспорта.

2 Планируемый результат обучения

2.1 Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения:

Профессиональный стандарт	Обобщенная трудовая функция (Виды деятельности)	Трудовые функции (Профессиональные компетенции)	Характеристика профессиональных компетенций		
			необходимые знания	необходимые умения	трудовые действия
06.033 «Специалист по защите информации в автоматизированных системах», утвержден Приказ Минтруда России от 15.09.2016 N 522н	Внедрение систем защиты информации автоматизированных систем	С/04.6 Внедрение организационных мер по защите информации в автоматизированных системах	Реализовывать правила разграничения доступа персонала к объектам доступа Анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации Осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации	Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты автоматизированных систем Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации Методики сертификационных испытаний технических средств защиты информации от утечки по техническим каналам на соответствие требованиям по безопасности информации	Проведение проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне Подготовка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации Проведение проверки готовности персонала к

			Конфигурировать аттестованную информационную систему и системы защиты информации информационной системы	Методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем	эксплуатации системы защиты информации автоматизированной системы Подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе Подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз и системой защиты информации информационной системы
	Формирование требований к защите информации в автоматизированных	Е/01.8Обоснование необходимости защиты информации в автоматизированной системе	Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации	Основные информационные технологии, используемые в автоматизированных системах Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах Методы защиты информации от утечки по техническим каналам Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных	Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите Выявление степени участия персонала в обработке защищаемой информации Планирование мероприятий по обеспечению защиты информации в автоматизированной системе Определение требуемого класса (уровня)

			Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем Использовать рисковую методологию управления защитой информации в автоматизированной системе Определять класс защищенности автоматизированных систем и ее составных частей	систем Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем Принципы формирования политики информационной безопасности в автоматизированных системах Нормативные правовые акты в области защиты информации Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации Методики сертификационных испытаний технических средств защиты информации от утечки по техническим каналам на соответствие требованиям по безопасности информации Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации	защищенности автоматизированной системы Обоснование необходимости использования криптографических средств защиты информации Разработка отчетных документов и разделов технических заданий
		E/02.8 Определение угроз безопасности информации, обрабатываемой автоматизированной системой	Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня	Основные информационные технологии, используемые в автоматизированных системах Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных	Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем Разработка систем защиты информации

			защищенности информации в автоматизированной системе Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы Систематизировать результаты проведенных исследований Анализировать возможные уязвимости информационных систем Выявлять известные уязвимости информационных систем Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах	сетях Программно-аппаратные средства обеспечения защиты информации автоматизированных систем Способы реализации угроз безопасности в автоматизированных системах Последствия от нарушения свойств безопасности информации Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Методики сертификационных испытаний технических средств защиты информации от утечки по техническим каналам на соответствие требованиям по безопасности информации Методы защиты информации от утечки по техническим каналам Принципы формирования и реализации политики безопасности информации в автоматизированных системах	автоматизированных систем с учетом действующих нормативно-правовых документов Определение комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем Определение оценки возможностей внешних и внутренних нарушителей Разработка модели угроз безопасности информации автоматизированной системы Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации

3 Учебный план

Категория слушателей: руководители и специалисты ОАО «РЖД».
Форма обучения: очная.
Трудоемкость: 40 часов.
Срок освоения: 5 дней.
Режим занятий: 6 - 10 академических (45 мин.) часов в день.

№ п/п	Тема занятия	Всего часов	В том числе				Преподаватель
			ЛК		ПЗ		
			ОО	ЭО	ОО	ЭО	
1	«Методологические основы экономической безопасности».	6	6				УрГУПС
2	«Роль железнодорожного транспорта в обеспечении экономической безопасности страны».	4	4				УрГУПС
3	«Конкурентоспособность железнодорожного транспорта, как стратегический фактор обеспечения экономической безопасности».	4	4				УрГУПС
4	«Мотивационные аспекты экономической безопасности железнодорожного транспорта».	4	4				УрГУПС
5	«Законодательная и нормативная база правового регулирования вопросов защиты информации, составляющей коммерческую тайну ОАО «РЖД» и персональных данных работников дороги».	4	4				Св.РЦБ
6	«Порядок отнесения информации к конфиденциальной».	4	4				Св.РЦБ
7	«Порядок обращения с информацией, составляющей коммерческую тайну ОАО «РЖД»».	4	4				Св.РЦБ
8	«Организация контроля за соблюдение режима коммерческой тайны».	4	4				Св.РЦБ
9	«Актуальность проблемы защиты персональных данных».	4	4				Св.РЦБ
	Итоговая аттестация: тестирование на компьютерах	2			2		УрГУПС Св.РЦБ
	Итого:	**40**	**38**		**2**		

ЛК - лекции; ПЗ - практики; ОО - очное обучение, в том числе по видеоконференциям; ЭО - электронное самостоятельное обучение.

Электронное обучение проводится на сервере модульной объектно-ориентированной динамической учебной среды ИОС Blackboard в сети ИНТЕРНЕТ. Адрес сайта – http://bb.usurt.ru.

Для работы понадобится компьютер, подключенный к сети Интернет и любая программа-браузер (Microsoft Internet Explorer v.7 и выше, Opera, Mozilla FireFox или др.)

4 Календарный учебный график

Количество часов									
РД1		РД2		РД3		РД4		РД5	
ОО	ЭО	ОО	ЭО	ОО	ЭО	ОО	ЭО	ОО	ЭО
6		10		10		8		6	

РД1- РД5 (ОО) – проведение лекционных занятий.

РД5 (ОО) – итоговая аттестация.

5 Рабочие программы учебных предметов, курсов, дисциплин (модулей)

Тема 1. «Методологические основы экономической безопасности»

Основные понятия, критерии и показатели экономической безопасности.

Тема 2. «Роль железнодорожного транспорта в обеспечении экономической безопасности страны»

Роль железнодорожного транспорта в обеспечении экономической безопасности государства.

Методы управления безопасностью ж.д. транспорта»

Тема 3. «Конкурентоспособность железнодорожного транспорта, как стратегический фактор обеспечения экономической безопасности»

Конкурентоспособность железнодорожного транспорта

Стратегический фактор обеспечения экономической безопасности

Тема 4. «Мотивационные аспекты экономической безопасности железнодорожного транспорта».

Мотивационные аспекты экономической безопасности железнодорожного транспорта.

Профессиональная этика руководителя и специалиста в аспекте экономической безопасности.

Тема 5. «Законодательная и нормативная база правового регулирования вопросов защиты информации, составляющей коммерческую тайну ОАО «РЖД» и персональных данных работников дороги»

Тема 6. «Порядок отнесения информации к конфиденциальной».

Обязанности работников и должностных лиц.

Прием и учет документов с грифом «КТ».

Ведение учетных журналов.

Порядок снятия и регистрации копий с документа.

Тема 7. «Порядок обращения с информацией, составляющей коммерческую тайну ОАО «РЖД».

Порядок обращения с информацией, составляющей коммерческую тайну ОАО «РЖД.

Обеспечение режима коммерческой тайны при ведении делопроизводства документов, содержащих информацию, составляющую коммерческую тайну.

Тема 8. «Организация контроля за соблюдение режима коммерческой тайны».

Основные положения по защите информации при работе с информационными ресурсами дороги.

Тема 9. «Актуальность проблемы защиты персональных данных».

Основные понятия, термины и определения в области защиты персональных данных.

Подготовка ответов на запросы правоохранительных органов.

6 Организационно-педагогические условия

6.1 Общие положения

Реализация ДПП ПК проходит в полном соответствии с требованиями законодательства Российской Федерации в области образования, нормативными правовыми актами, регламентирующими данные направления деятельности.

В обучении используются такие технические средства, как, компьютеры, видеопроекторы, видеофильмы и мультимедийные программы, способствующие лучшему усвоению учебного материала.

Для закрепления изучаемого материала проводятся занятия на специальном оборудовании. Основные методические материалы размещаются на электронном носителе или в сети интернет для последующего использования слушателями.

Для работы на занятиях и для самостоятельной подготовки слушателям на период занятий выдаётся учебное пособие, разработанное Свердловским региональным центром безопасности по организации режима коммерческой тайны и делопроизводства с документами, содержащими информацию, составляющую коммерческую тайну в ОАО «РЖД».

Для индивидуального использования в качестве раздаточного материала слушателям выдаются CD – диски с основными учебно-методическими материалами.

6.2 Организационные условия

Для обучения слушателей системы дополнительного профессионального образования университет располагает отдельным зданием ИДПО (Одинарка 1А).

При реализации программ используется учебно-производственная база университета, которая оснащена самым современным оборудованием и новейшими техническими средствами обучения.

Кроме того, что слушатели ИДПО в процессе обучения обеспечиваются необходимой нормативно-справочной и учебно-методической литературой, информационными материалами, они имеют возможность пользоваться научно-технической библиотекой, имеющей три читальных зала с книжным фондом более 600 тысяч экземпляров.

Желающие в свободное от учебы время могут под руководством опытных тренеров заниматься в спортивным комплексом университета.

При необходимости (в условиях пандемии, чрезвычайных ситуаций и т.п.), по согласованию с заказчиком, обучение по очной форме может быть реализовано и без выезда в ИДПО АКО УрГУПС. В этом случае проведение занятий будет организовано при помощи видеоконференций. Для участия в видеоконференции слушатель должен иметь web-камеру, микрофон, аудио-колонки или наушники. Возможно использование мобильных устройств (смартфонов или планшетов). Для подключения к видеоконференции у слушателя должен быть в обязательном порядке доступ к сети «Интернет» со скоростью, позволяющей принимать он-лайн видеотрансляцию в удовлетворительном качестве. Слушатель на протяжении всей видеоконференции должен быть к ней подключен.

Занятия осуществляются в пределах рабочего дня с 8.30 до 19.35, обеденный перерыв с 11.50 до 12.45, имеется возможность питания в пунктах общественного питания университетского комплекса.

Социальная инфраструктура жизнеобеспечения слушателей включает в себя общежитие гостиничного типа на 109 номеров (35 трехместных, 62 двухместных и 12 одноместных), комбинат общественного питания с сетью столовых и кафе.

Главный учебный корпус университета, здание ИДПО, общежитие слушателей, комбинат общественного питания расположены в живописном месте г. Екатеринбурга (т.н. «генеральские дачи») в непосредственной близости друг от друга.

6.3 Педагогические условия

Реализация ДПП обеспечивается научно-педагогическими кадрами, имеющими базовое образование, соответствующее профилю преподаваемой дисциплины, и ученую степень или опыт деятельности в соответствующей профессиональной сфере и систематически занимающимися научной и/или научно-методической деятельностью. К преподавательской деятельности также привлекаются руководители и специалисты ОАО «РЖД».

6.4 Материально–техническое обеспечение

Здание ИДПО имеет 20 учебных аудиторий общей площадью 1000 м^2. Из них шесть компьютерных классов, которые оснащены 81 компьютером. Все аудитории оборудованы мультимедийными средствами.

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Аудитория Д2-13	Лекции	Компьютер, видеопроектор, экран, классная доска
Компьютерный класс Д2-15	самостоятельная работа, итоговое тестирование на компьютерах	Компьютеры, пакеты компьютерных программ, видеопроектор, экран, классная доска, доступ к электронной библиотеке АСПИЖТ

7 Формы аттестации

Освоение ДПП ПК завершается итоговой аттестацией слушателей, которая проводится в виде тестирования на компьютерах по системе «зачет / незачет». Для зачёта должно быть не менее 80% правильных ответов. Количество вопросов — 75.

8 Оценочные материалы

8.1 Вопросы для тестов:

1. Каким нормативным правовым актом необходимо руководствоваться при обращении с информацией, составляющей коммерческую тайну?

2. По каким журналам учета осуществляется регистрация сопроводительного письма к документу с грифом «Коммерческая тайна», если письмо не содержит информацию, составляющую коммерческую тайну?

3. Кто утверждает перечень информации, составляющий коммерческую тайну ОАО «РЖД»?

4. Какие Вы знаете основные законодательные акты Российской Федерации, регулирующие деятельность железнодорожного транспорта?

5. Порядок регистрации документов с грифом «КТ» в учетном журнале.

6. Что должно определяться в разделе «Конфиденциальность» договора на проведение работы Контрагентом с использованием информации, составляющей коммерческую тайну ОАО «РЖД»?

8. На кого возлагается ответственность за установление режима коммерческой тайны в ОАО «РЖД»?

9. Какие мероприятия относятся к защите коммерческой тайны?

10.Что является одним из наиболее уязвимых ресурсов любого предприятия?

11. Наиболее вероятные способы сбора информации

12. Какие меры являются основными в вопросе защиты информации?

13. Порядок уничтожения документов с грифом «КТ»

14. Как осуществляется контроль за обеспечением режима коммерческой тайны в ОАО «РЖД»?

15.Что относится к информации, составляющей коммерческую тайну (секрет производства)?

16. Какие сведения не могут составлять коммерческую тайну?

17. Кто устанавливает режим коммерческой тайны?

18. Что такое коммерческая тайна?

19. Кто является обладателем информации, составляющей коммерческую тайну?

20.Что такое доступ к информации, составляющей коммерческую тайну?

21. Что такое передача информации, составляющей коммерческую тайну?

22. Понятие «контрагент»

23. Какой разновидностью информации являются персональные данные?

24. В каких случаях согласие работника на передачу персональных данных не требуется?

25. В каких случаях работник дает согласие на передачу своих персональных данных?

26. В чьи обязанности входит предоставление информации, составляющей коммерческую тайну?

27. К какой тайне относится частная жизнь работников Компании?

28. Какую ответственность несут работники Компании, допущенные к работе с информацией, составляющей коммерческую тайну?

29. На основании чего предоставляется доступ пользователям к информационным ресурсам Компании?

30. Какой ФЗ является правовой основой работы комплекса информационной безопасности в Компании?

31. Наличие каких признаков необходимо для признания информации коммерческой тайной?

32. Для чего осуществляется защита информации на предприятии?

33. Какие виды ответственности применяются в области информационных правоотношений?

34. Какие требования к оформлению документа с грифом «Коммерческая тайна» применяются при его регистрации?

35. Кто утверждает акт ежегодной проверки документов с грифом «Коммерческая тайна»?

36. На какие типы подразделяются подключения пользователей в соответствии с Порядком предоставления доступа к ИС ОАО «РЖД»?

37. Что представляет собой информация?

38. Перечислите наиболее распространенные способы овладения информацией, составляющей коммерческую тайну.

40.Что необходимо указывать на обложке дел, содержащих документы с грифом «Коммерческая тайна»?

41. На каком основании осуществляется доступ к информационным системам ОАО «РЖД» в соответствии с Порядком предоставления доступа?

42. Как следует поступить при получении документа с грифом «Коммерческая тайна», адресованного в другое подразделение?

43. Назовите задачу установления режима коммерческой тайны в организации?

44. Где проставляется гриф «Коммерческая тайна» в случае, если информация, составляющая коммерческую тайну, содержится в документе, зафиксированном на бумажном носителе?

45. Укажите срок действия заявки на подключение для внутренних пользователей ИС ОАО «РЖД»?

46. В каких случаях подлинник электронного документа считается не существующим?

47. Что необходимо сделать в случае разглашения сведений, содержащихся в документе с грифом «Коммерческая тайна»?

48. Какие меры по защите информации применяются при проведении совещаний конфиденциального характера?

49. Кто относятся к внутренним пользователям ИС ОАО «РЖД»?

50. Кто имеет право вырабатывать определенные механизмы защиты ИС, а также разрабатывать конкретную технологию обработки информации и концепцию по использованию ИС другими лицами, при установленных правах собственности?

51. Где проставляется регистрационный штамп подразделения при учете входящих документов с грифом «Коммерческая тайна»?

52. Что обязательно указывается на обороте последнего листа документа, содержащего сведения, составляющие коммерческую тайну?

53. Что такое разглашение информации, составляющей коммерческую тайну?

54. Где регистрируются приложения без грифа «Коммерческая тайна» к подготовленному документу, содержащему сведения, составляющие коммерческую тайну?

55. Какие меры необходимо предпринять для установления режима коммерческой тайны на предприятии?

56 .Необходимо ли ведение журналов учета документов с грифом «Коммерческая тайна» при использовании электронного документооборота?

57. Укажите самый распространенный источник угроз информационной безопасности?

58. В каком году принят Федеральный закон «О коммерческой тайне»?

59. Кто является распорядителем информационной системы ОАО «РЖД»?

61. Назовите принципы установления режима коммерческой тайны в организации

62. Кем осуществляется снятие грифа коммерческая тайна с документа, содержащего информацию, составляющую коммерческая тайна?

63. На основании чего проводится проверка обеспечения режима коммерческой тайны?

64. Кто отвечает за оформление заявок на доступ к ИС ОАО «РЖД»?

65. В каком месте поступившего документа с грифом «Коммерческая тайна» при регистрации проставляется штамп «Коммерческая тайна»?

66. Имеет ли право работник, ведущий делопроизводство документов с грифом «Коммерческая тайна», знакомиться с содержанием конвертов с пометкой «КТ», если вопросы, рассматриваемые в данных документах, не относятся к его непосредственным функциональным обязанностям?

67. Назовите условия по охране информации, составляющей коммерческую тайну, которые необходимо включать в договоры на выполнение работ в соответствии с нормами законодательства Российской Федерации.

68. Какие законодательные акты Российской Федерации регулируют вопросы защиты информации, составляющей коммерческую тайну?

69. Кто несет ответственность за неправильное присвоение грифа «Коммерческая тайна»?

70. К какому виду пользователей относятся пользователи дочерних или зависимых обществ?

71.Кем осуществляется подключение работников ОАО «РЖД» к сети Интернет?

72. С чем связаны отношения, которые регулирует Федеральный закон «О коммерческой тайне»?

73. Какая информация относится к информации без ограничения права доступа?

74. Какие виды тайн не относятся к охраняемым законом тайнам?

75. Как часто должны проводиться проверки наличия документов с грифом «Коммерческая тайна» в подразделении?

8.2 Пример тестового вопроса

Вопрос № 1

По каким журналам учета осуществляется регистрация сопроводительного письма к документу с грифом «Коммерческая тайна», если письмо не содержит информацию, составляющую коммерческую тайну?

Варианты ответов:

а) по журналам учета документов, содержащих информацию, составляющую коммерческую тайну;

б) по журналам учета документов, не содержащих информацию, составляющую коммерческую тайну;

в) регистрация не осуществляется.

Список используемых источников

По вопросам организации защиты коммерческой тайны и обращения с нею.

1. Указ Президента РФ от 06.03.1997г. №188 «Об утверждении перечня сведений конфиденциального характера»
2. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
3. Приказ ОАО «РЖД» от 27.12.2004 № 240 «О порядке обращения с информацией, составляющей коммерческую тайну, в ОАО «РЖД»
4. Приказ ОАО «РЖД» от 20.02.2014 № 11 «О внесении изменений в Перечень информации, составляющей коммерческую тайну ОАО «РЖД»
5. Приказ ОАО «РЖД» от 15.02.2009 № 14 «О внесении изменений в Перечень информации, составляющей коммерческую тайну ОАО «РЖД»
6. Приказ ОАО «РЖД» от 19.11.2006 № 267 «О внесении изменений в Перечень информации, составляющей коммерческую тайну ОАО «РЖД», и в Инструкцию о порядке обращения с информацией, составляющей коммерческую тайну, утвержденные приказом ОАО «РЖД» от 27 декабря 2004 г. № 240»
7. Регламент охраны конфиденциальности информации, составляющей коммерческую тайну, при проведении совещаний в ОАО «РЖД» от 17.10.2007 № 1350
8. Распоряжение ОАО «РЖД» от 28.11.2014 № 2782р «Об утверждении регламента беспатентной формы охраны созданных разработок в режиме коммерческой тайны»
9. Распоряжение ОАО «РЖД» от 6.10.2014 № 2349р «Об обеспечении конфиденциальности информации, составляющей коммерческую тайну, в ОАО «РЖД» при ее пересылке в электронном виде»
10. Распоряжение ОАО «РЖД» от 21.06.2016 № 1201р «О работе с документами, содержащими информацию ограниченного доступа»
11. Приказ Свердловской железной дороги от 18.05.2015 №СВЕРД-185 «О совершенствовании работы с информацией, составляющей коммерческую тайну ОАО «РЖД»
12. Приказ Свердловской железной дороги от 10.08.2015 №СВЕРД-283 «Об утверждении обязательства о неразглашении коммерческой тайны.
13. Положение по защите информации ограниченного доступа при проведении работ по транспортной безопасности в ОАО «РЖД» от 19.02.2016 № 179.
14. Методические разъяснения Департамента безопасности ОАО «РЖД» от 06.09.2016 №3737/ЦБЗ «О работе с документами, содержащими информацию ограниченного доступа»

По вопросам защиты персональных данных работников ОАО «РЖД»

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
2. Распоряжение ОАО «РЖД» от 23.10.2015 № 2524р «Об утверждении политики ОАО «РЖД» по обработке и защите персональных данных».
3. Приказ ОАО «РЖД» от 20.07.2016 № 60 «Об обеспечении защиты персональных данных в ОАО «РЖД».
4. Распоряжение ОАО «РЖД» от 12.10.2016 № 2085р «О контроле за соблюдением режима защиты персональных данных в ОАО «РЖД»
5. Указание Управления по защите персональных данных ОАО «РЖД» от 19.07.2016 №121/ЦУЗПД «О передаче персональных данных в электронном виде»
6. Указание Управления по защите персональных данных ОАО «РЖД» от 11.11.2016 №232/ЦУЗПД «О передаче персональных данных в электронном виде»
7. Приказ Свердловской железной дороги от 01.09.2016 № СВЕРД-342 «О защите персональных данных работников Свердловской железной дороги»
8. Распоряжение Свердловской железной дороги от 29.11.2016 №СВЕРД-1473/р «О контроле за соблюдение режима защиты персональных данных на Свердловской железной дороге»

По вопросам предоставления информации на запросы правоохранительных органов и других надзорных организаций

1. Федеральный закон «О полиции» от 07.11.2011 № 3-ФЗ
2. Федеральный закон «О федеральной службе безопасности» от 03.04.1995 № 40-ФЗ
3. Приказ ОАО «РЖД» от 19.02.2007 № 20 «Об утверждении Регламента взаимодействия подразделений аппарата управления, филиалов, других структурных подразделений и негосударственных учреждений ОАО «РЖД» в случае обращения правоохранительных органов»
4. Распоряжение ОАО «РЖД» от 9.03.2016 № 375р «Об утверждении Положения о порядке действий подразделений при проведении проверок органами, уполномоченными на осуществление государственного контроля (надзора) и муниципального контроля, при исполнении и обжаловании актов и предписаний этих органов и устранения причин, послуживших основанием для привлечения ОАО «РЖД» к административной ответственности

5. Приказ Свердловской железной дороги от 30.06.2010 № 378/Н «Об утверждении Регламента действий работников Свердловской железной дороги при осуществлении государственного контроля (надзора)
6. Приказ Свердловской железной дороги от 29.04.2013 №СВЕРД-116 «Об утверждении Регламента взаимодействия подразделений Свердловской железной дороги – филиала ОАО «РЖД»№ (регионального центра корпоративного управления) и территориальных подразделений функциональных филиалов ОАО «РЖД» в случае обращения правоохранительных органов
7. Приказ Свердловской железной дороги от 10.07.2014 №СВЕРД-199 «О внесении изменений в приказ от 29 апреля 2013 г. №СВЕРД-116»
8. Приказ Свердловской железной дороги от 3.06.2016 №СВЕРД-205 «О внесении изменений в приказ от 29 апреля 2013 г. №СВЕРД-116»
9. Приказ Свердловской железной дороги от 31.07.2015 №СВЕРД-272 «О внесении изменений в приказ от 29 апреля 2013 г. №СВЕРД-116»

По вопросам информационной безопасности

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2. Концепция обеспечения кибербезопасности ОАО «РЖД» от 25.12.2014
3. Стандарт ОАО «РЖД», СТО 1.18.002-2009 Управление информационной безопасностью. Общие положения
4. Политика информационной безопасности Свердловской железной дороги, утвержденная 01.10.2015 № 76 Н-94/пд
5. Положение по управлению инцидентами информационной безопасности в ОАО «РЖД» от 27.11.2014
6. Распоряжение ОАО «РЖД» от 28.11.2011 № 2546р «О порядке предоставления доступа к информационным системам ОАО «РЖД»
7. Приказ Свердловской железной дороги от 09.06.2014 №СВЕРД-165 «О повышении безопасности корпоративной компьютерной сети и порядке предоставления доступа к информационным системам»
8. Распоряжение Свердловской железной дороги от 4.03.2015 № СВЕРД-250р «О временном порядке использования мобильных планшетных компьютеров в границах Свердловской железной дороги»
9. Распоряжение ОАО «РЖД» от 02.08.2004 № 3034р «Об организации работы по предотвращению записи, хранения, распространения информации и программных продуктов непроизводственного характера»
10. Распоряжение ОАО «РЖД» от 06.06.2013 № 1280р «Об обеспечении информационной безопасности при использовании в ОАО «РЖД» средств мобильной связи»

11. Распоряжение ОАО «РЖД» от 01.11.2013 № 2347р «Об утверждении Порядка использования мобильных технических средств в ОАО «РЖД»
12. Распоряжение ОАО «РЖД» от 11.02.2015 № 321р «Об утверждении Регламента взаимодействия ОАО «РЖД» с организациями при их подключении к информационным системам ОАО «РЖД»
13. Приказ административно - организационного аппарата ОАО «РЖД» от 03.10.2016 № ЦА-1 «О повышении качества подготовки документов»

Составители программы и согласующие

Составители программы

Должность	ФИО	Дата	Подпись
Руководитель специализации, заведующая кафедрой «Экономика транспорта» УрГУПС, д.э.н., профессор	Рачек С.В.	29.06.22	

Согласующие

Должность	ФИО	Дата	Подпись
Зам. директора ИДПО АКО	Шумаков К. Г.	30.06.22	
Начальник УМО ИДПО	Лесников Д. В.	30.06.22