Смоленский колледж телекоммуникаций (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования «Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Утверждаю
Директор СКТ(ф)СПбГУТ
_____Казаков А.В.
«___» ____09_____2020 г.

Рабочая программа

курсов повышения квалификации по направлению

«Менеджмент и аудит систем информационной безопасности»

Смоленск 2020 г.

Рассмотрено
на заседании методической комиссии
дисциплин компьютерных сетей и средств
подвижной связи
Председатель _____Е.Н. Кожекина
Протокол № 1 от
«31» 03 2020 г.

Согласовано
Зам. директора по учебной работе
_____И.В. Иванешко
«31» 08 2020г.

Составил:
Грубник Е.М. - преподаватель первой квалификационной категории СКТ (ф) СПбГУТ,
Ломатенков Д.А. – преподаватель высшей категории СКТ (ф) СПбГУТ

Согласовано
Начальник Департамента Смоленской области
по информационным технологиям
_____Рудометкин А.Н.
«01» 09 2020г.

Рабочая программа разработана в рамках реализации регионального проекта «Кадры для цифровой экономики (Смоленская область)» в составе национальной программы «Цифровая экономика Российской Федерации».

Содержание

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ КУРСОВ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Менеджмент и аудит систем информационной безопасности»

1.1. *Область применения программы*

Рабочая программа предназначена для повышения квалификации государственных служащих органов исполнительной власти Смоленской области, муниципальных служащих исполнительно-распорядительных органов местного самоуправления муниципальных районов и городских округов Смоленской области, сотрудников областных и муниципальных учреждений, осуществляющих деятельность в сферах здравоохранения, образования, строительства, социальной защиты, сельского хозяйства, ИКТ и других сферах экономики. Программа предусматривает изучение и освоение следующих вопросов:

- основные понятия цифровой экономики, сущность цифровой экономики и перспективы развития;
- данные в государственном управлении в условиях цифровой трансформации;
- сквозные технологии в государственном управлении;
- обзор успешных практик, в том числе в государственном управлении (реализованные проекты и технологии, на основе которых создаются проекты цифровой трансформации);
- основные положения, понятия и определения теории информационной безопасности, понятие аудита информационной безопасности, анализ и управление рисками информационной безопасности;
- действующая в Российской Федерации система нормативно-правовых документов в области информационной безопасности;
- назначение и цели аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации (ИОГВ и ОМС);
- планирование и организация работ по аудиту информационной безопасности ИОГВ и ОМС;
- процедура аудита информационной безопасности ИОГВ и ОМС в соответствии с требованиями СРТ-К ФСТЭК России.

К освоению данной дополнительной профессиональной программы допускаются лица, имеющие среднее профессиональное и (или) высшее образование.

Для успешного освоения программы повышения квалификации слушатель должен:

знать и понимать:

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации;
- правовые основы организации защиты информации,
- принципы и методы организационной защиты информации;

уметь:

- анализировать и оценивать угрозы информационной безопасности объекта;
- пользоваться нормативными документами по защите информации;
- использовать в практической деятельности правовые знания; анализировать основные правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности.

владеть:

- навыками работы с нормативными правовыми актами в сфере экономической и

информационной безопасности;

- навыками компьютерной обработки служебной документации, статистической информации и деловой графики; работы с информационно- поисковыми и информационно-справочными системами и базами данных, используемыми профессиональной деятельности;

- навыками организации и обеспечения режима секретности;

- навыками обоснования, выбора, реализации и контроля результатов управленческого решения.

По окончании курсов повышения квалификации предусматривается итоговая аттестация дифференцированного зачёта.

По итогам тестирования слушателю выдается документ установленного образца - удостоверение о повышении квалификации.

1.2. Цели и задачи программы – требования к результатам освоения программы:

В результате освоения программы слушатель должен приобрести и (или) усовершенствовать следующие компетенции:

ПК 1.1 реализация процессного управления в условиях цифровой трансформации;

ПК 1.2 выполнение комплекса мер по информационной безопасности, управление процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты.

1.3.Количество часов на освоение программы:

Всего 16 часов, в том числе:

- теоретических и практических занятий - 14 часов

- итоговая аттестация – 2 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ

Результатом освоения программы повышения квалификации является овладение слушателями следующими компетенциями:

ПК 1.1 реализация процессного управления в условиях цифровой трансформации;

ПК 1.2 выполнение комплекса мер по информационной безопасности, управление процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты.

3. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

3.1. Тематический план рабочей программы

Наименование тем	Количество часов
Тема 1. Основные понятия цифровой экономики; сущность цифровой экономики и перспективы развития. Цифровая трансформация.	2
Тема 2. Данные в государственном управлении в условиях цифровой трансформации. Сквозные технологии в государственном управлении; процессное управление в условиях цифровой трансформации.	2
Тема 3. Обзор успешных практик, реализованных проектов и технологий на уровне государственного управления в регионах России.	2

Тема 4. Организация комплексной системы мер по защите информации в муниципальных (государственных) информационных системах.	2
Тема 5. Нормативная база аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов РФ	1
Тема 6. Методика проведения аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов РФ	1
Тема 7. Планирование и организация работ по аудиту информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов РФ	2
Тема 8 Процедура проведения аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов РФ	2
Итоговая аттестация	2
Итого	16

Тема 1 проводится очно.

Темы 2 – 8 проводятся с применением электронного обучения и дистанционных образовательных технологий.

4. Условия реализации рабочей программы

4.1.Требования к материально-техническому обеспечению

Технические средства обучения (персональные компьютеры, оргтехника):

- автоматизированные рабочие места студентов – 10 шт. (Компьютер в составе: системный блок Ci3-3100/Mb Asus IH361/8Gb/DVD+RW/430W+монитор);
- автоматизированное рабочее место преподавателя (Компьютер в составе: системный блок Ci3-3100/Mb Asus IH361/8Gb/DVD+RW/430W+монитор).

Учебный сервер в колледже (аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 4 Гб; жесткий диск объемом не менее 1Тб; лицензионное или свободно распространяемое программное обеспечение).

Типовое активное оборудование: сетевые маршрутизаторы, сетевые коммутаторы, сетевые хранилища, шлюзы VPN, сетевые адаптеры и карты, сетевые контроллеры.

Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения безопасности.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

1. Городнова, А. А. Развитие информационного общества: учебник и практикум для академического бакалавриата / А. А. Городнова. — М. : Издательство Юрайт, 2017. — 243 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-9916-9437-7. https://www.biblio-online.ru/viewer/CA2A2AC6-0C7D-4DE1-80B6-6F014E1C1C8D#page/1.

2. Трофимов, В. В. Информационные технологии в 2 т. Том 1 : учебник для академического бакалавриата / В. В. Трофимов ; отв. ред. В. В. Трофимов. — М. : Издательство

Юрайт, 2017. — 238 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-01935-3. https://www.biblio-online.ru/viewer/39752ABD-6BE0-42E2-A8A2-96C8CB534225#page/1.

3. Трофимов, В. В. Информационные технологии в 2 т. Том 2 : учебник для академического бакалавриата / В. В. Трофимов ; отв. ред. В. В. Трофимов. — М. : Издательство Юрайт, 2017. — 390 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-01937-7. https://www.biblio-online.ru/viewer/4FC4AE65-453C-4F6A-89AA-CE808FA83664#page/1.

4. Нетёсова, О. Ю. Информационные системы и технологии в экономике: учебное пособие для вузов / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 146 с. — (Серия : Университеты России). — ISBN 978-5-9916-9733-0. https://www.biblio-online.ru/viewer/252563FB-FE6B-4038-9FE7-AB5FEC2B6711#page/1.

5. Ищейнов В.Я. Основные положения информационной безопасности / В.Я. Ищейнов, М.В. Мецатунян. - Москва : Форум, 2018. - 208 с. - ISBN 978-5-00091-489-2. - URL: https://ibooks.ru/bookshelf/361467/reading - Текст: электронный.

6. Кузнецова, И. В. Ведение конфиденциального делопроизводства : учебник для СПО / И. В. Кузнецова, Г. А. Хачатрян. — Саратов : Профобразование, 2020. — 145 с. — ISBN 978-5-4488-0837-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97082.html — Режим доступа: для авторизир. пользователей.

7. Васильков А.В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - Москва : Форум, 2019. - 368 с. - ISBN 978-5-91134-360-6. - URL: https://ibooks.ru/bookshelf/361192/reading - Текст: электронный.

8. Баранова Е. К. Моделирование системы защиты информации: Практикум / Е.К. Баранова, А.В. Бабаш. - Москва : ИЦ РИОР, 2018. - 224 с. - ISBN 978-5-369-01559-9. - URL: https://ibooks.ru/bookshelf/361422/reading - Текст: электронный.

9. Зверева В.П. Организация и технология работы с конфиденциальными документами / В.П. Зверева, А.В. Назаров. - Москва : КУРС, 2018. - 320 с. - ISBN 978-5-906818-96-6. - URL: https://ibooks.ru/bookshelf/360624/reading - Текст: электронный.

10. Зверева В.П. Участие в планировании и организации работ по обеспечению защиты объекта. / В.П. Зверева, А.В. Назаров. - Москва : КУРС, 2017. - 320 с. - ISBN 978-5-906818-92-8. - URL: https://ibooks.ru/bookshelf/360623/reading - Текст: электронный.

11. Информационная безопасность России [Электронный ресурс]. Аналитический сборник: выпуск №1, январь 2016. -128 с. Режим доступа: http://znanium.com/bookread.php?book=402702.

12. Основы цифровой экономики [Электронный ресурс]: учебное пособие / ред.: М.И. Столбов, ред.: Е.А. Бренделева, Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации .— М. : Научная библиотека, 2018 . - 238 с. https://vk.com/doc107248915_545218865?hash=f0b1ff16b4071276d8.

13. Медведовский, И.Д. Практическое применение международного стандарта безопасности информационных систем ISO 17799 [Электронный ресурс] / И.Д. Медведовский. – Электрон. текст. дан. – Режим доступа: www.dsec.ru/cd-courses/iso 17799 cd.php/.

Интернет-ресурсы:

1. Сайт Федеральной службы безопасности России (ФСБ России) [Электронный ресурс]. - Режим доступа: http://www.fsb.ru, свободный.

2. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [Электронный ресурс]. - Режим доступа: http://www.fstec.ru/, свободный.

3. Сайт проекта Общие критерии оценки безопасности информационных технологий [Электронный ресурс]. - Режим доступа: http://www.commoncriteriaportal.org/, свободный.

4. www.cyberpol.ru Компьютерная преступность и способы борьбы.

5. www.iso27000.ru Информационный портал, посвященный вопросам управления информационной безопасностью.

6. www.itsec.ru Интернет-журнал «Информационная безопасность».

7. www.inside-zi.ru Информационно-методический журнал «Защита информации. Инсайд».

4.3. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по рабочей программе: наличие высшего образования.

Инженерно-педагогический состав: дипломированные специалисты-преподаватели.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Результаты (освоенных ПК, обобщенной трудовой функции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Реализация процессного управления в условиях цифровой трансформации	ОПОР 1. Грамотная организация и контроль работы на основе современных цифровых технологий. ОПОР 2 - Качество анализа и рациональность решения прикладных задач в рамках управленческих полномочий конкретной функциональной подсистемы с помощью каждой из технологий Индустрии 4.0.	Текущий контроль в форме: - электронного тестирования; - наблюдения преподавателя за выполнением конкретного задания.
ПК 1.2. Выполнение комплекса мер по информационной безопасности, управление процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты	ОПОР 3 - Четкое понимание проблем информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов РФ. ОПОР 4 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления. ОПОР 5 – Владение правилами проведения возможных проверок; определения конфиденциальности документов объекта защиты; структуры подсистем информационной безопасности в корпоративных сетях исполнительных органов государственной власти и органов местного самоуправления субъектов РФ	Текущий контроль в форме: - электронного тестирования; - наблюдения преподавателя за выполнением конкретного задания.