МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО «СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Директор НОЦ «Институт
непрерывного образования»
_____ Е.В. Мошкина
«__» апреля 2024 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Информационные технологии информационной безопасности»

Красноярск 2024

СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы повышения квалификации «Информационные технологии информационной безопасности»

№ п/п	Наименование модулей (дисциплин)	Общая трудоем-кость, ч	Всего контактн., ч		Контактные часы		СРС, ч	Формы контроля
			синхрон-ных	асинхрон-ных	Лекции	Практические и семинарские занятия		
1	Технические аспекты информационной безопасности	80	36	4	10	30	40	Зачет
2	Правовые аспекты информационной безопасности	62	24	8	10	22	30	Зачет
3	Итоговая аттестация	2					2	Зачет в форме тестирования
	Итого	**144**	**60**	**12**	**16**	**56**	**72**	

СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
дополнительной профессиональной программы повышения квалификации
«Информационные технологии информационной безопасности»

Категория слушателей: лица, имеющие высшее образование — бакалавриат в области информационной безопасности.
Срок обучения: 144 часа.
Форма обучения: очно-заочная, с применением исключительно электронного обучения и дистанционных образовательных технологий.

№ п/п	Наименование модулей (курсов)	Общая трудоем-кость, ч	Всего контактн., ч		Контактные часы		СРС, ч	Формы контроля
			синхрон-ных	асинхрон-ных	Лекции	Практ. и семинарские занятия		
1	**Технические аспекты информационной безопасности**	**80**	**36**	**4**	**10**	**30**	**40**	**Зачет**
1.1	Построение и администрирование телекоммуникационных сетей и систем	40	18	2	4	16	20	
1.2	Технические основы информационной безопасности	40	18	2	6	14	20	
2	**Правовые аспекты информационной безопасности**	**62**	**24**	**8**	**10**	**22**	**30**	**Зачет**
2.1	Система нормативно-правовых актов по вопросам информационной безопасности	32	12	4	6	10	16	
2.2	Информационная открытость органов государственной власти и местного самоуправления	30	12	4	4	12	14	
3	**Итоговая аттестация**	**2**					**2**	**Зачет в форме тестирования**
	Итого	**144**	**60**	**12**	**16**	**56**	**72**	

СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

Календарный учебный график*
дополнительной профессиональной программы повышения квалификации
«Информационные технологии информационной безопасности»

Наименование модулей (курсов)	Неделя	Объем учебной нагрузки, ч.	Виды занятий (количество часов)						Итоговый контроль
			Лекция	Практ. и семинарские занятия	СРС	Консуль-тация	Контр. работа	Тест	
Технические аспекты информационной безопасности	1–5	80	10	30	40				Зачет
Правовые аспекты информационной безопасности	5–7	62	10	22	30				Зачет
Итоговая аттестация	7	2						2	Зачет в форме тестирования
Итого		**144**	**16**	**56**	**72**				

Календарный учебный график составляется для программ профессиональной переподготовки и представляет собой график учебного процесса, устанавливающий последовательность и продолжительность теоретического обучения, экзаменационных сессий, практик, стажировок, итоговой аттестации

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Аннотация программы

Программа повышения квалификации разрабатывалась с учетом квалификационных требований к лицу, ответственному за обеспечение информационной безопасности в органе исполнительной власти, высшем исполнительном органе субъекта Российской Федерации, государственном фонде, государственной корпорации (компании) и иной организации, созданной на основании федерального закона, стратегического предприятия, стратегического акционерного общества и системообразующей организации российской экономики, юридического лица, являющегося субъектом критической информационной инфраструктуры Российской Федерации.

Выпускники программы смогут организовывать работу по обеспечению информационной безопасности органа государственной власти, местного самоуправления, организаций государственного сектора и иных организаций.

1.2. Цель программы

Цель программы повышения квалификации — получение новых компетенций, необходимых для обеспечения информационной безопасности в органах государственной власти, местного самоуправления, организаций государственного сектора, иных организаций, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты.

1.3. Компетенции (трудовые функции) в соответствии с Профессиональным стандартом (формирование новых или совершенствование имеющихся)

Дополнительная образовательная программа повышения квалификации «Информационные технологии информационной безопасности» обеспечивает достижение *шестого* уровня квалификации в соответствии с требованиями профессионального стандарта 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации № 536н от 14 сентября 2022 г.

Программа направлена на формирование и совершенствование следующих трудовых функций:

– B/02.6 Управление функционированием СССЭ, защищенностью от НД и компьютерных атак сооружений и СССЭ.

– C/02.6 Обеспечение бесперебойной работы средств связи сетей связи специального назначения, включая СКЗИ, средства для поиска признаков компьютерных атак в сетях электросвязи.

1.4. Планируемые результаты обучения

В результате освоения программы слушатель будет:

Знать:

– модели угроз несанкционированного доступа к сетям электросвязи;

– программно-аппаратные средства обеспечения защиты сетей;

– сетевые протоколы и их параметры настройки;

– средства анализа и контроля защищенности в конвергентных информационных системах;

– нормативные правовые акты в области связи, информатизации и защиты информации, защиты персональных данных;

– руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;

– методы комплексного обеспечения защиты сетей электросвязи;

– требования по обеспечению доступа к открытой информации о деятельности органов (организаций).

Уметь:

– выявлять и оценивать угрозы несанкционированного доступа к сетям связи, организует работу по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак;

– устанавливать и настраивать параметры сетевых протоколов;

– проводить мониторинг и анализ нормативных правовых актов, руководящих и методических документов уполномоченных федеральных органов исполнительной власти в сфере защиты информации;

– разрабатывать предложения по совершенствованию и повышению эффективности принимаемых технических мер и проводимых организационных мероприятий по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак;

– организовывать работы по выполнению требований режима защиты информации ограниченного доступа в сети электросвязи.

Владеть:

– методами оценки уязвимостей сетей электросвязи с точки зрения возможности несанкционированного доступа к ним;

– навыками разработки и организации выполнения мероприятий в соответствии с положениями политики информационной безопасности в органе (организации), согласование иных документов органа (организации) в части обеспечения информационной безопасности;

– методикой проведения мониторинга нормативных правовых актов, руководящих и методических документов уполномоченных федеральных органов исполнительной власти в сфере защиты и обеспечения безопасности информации;

– навыками контроля выполнения требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного

порядка выполнения работ при решении вопросов, касающихся защиты информации, соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации.

1.5. Категория слушателей

Руководители (заместители руководителя), должностные лица (работники) структурных подразделений ответственные за обеспечение информационной безопасности в органе исполнительной власти, высшем исполнительном органе субъекта Российской Федерации, государственном фонде, государственной корпорации (компании) и иной организации, специалисты по информационным системам, специалисты по защите информации, специалисты по информационным системам и программированию.

1.6. Требования к уровню подготовки поступающего на обучение

В соответствии с требованиями к образованию и обучению, предъявляемыми к 6 уровню квалификации профессионального стандарта 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации № 536н от 14 сентября 2022 г., необходимо иметь высшее образование - бакалавриат в области информационной безопасности.

1.7. Продолжительность обучения

Продолжительность программы – 144 часа, из них 72 часа контактной работы.

1.8. Форма обучения

Очно-заочная, с применением исключительно электронного обучения и дистанционных образовательных технологий.

1.9. Требования к материально-техническому обеспечению, необходимому для реализации дополнительной профессиональной программы повышения квалификации (требования к аудитории, компьютерному классу, программному обеспечению)

Программа реализуется дистанционно с использованием системы дистанционного обучения. Для доступа к учебным материалам слушателям необходимо стандартное программное обеспечение (операционная система, офисные программы) и выход в Интернет.

Программа реализуется с использованием системы дистанционного обучения LMS Odin. Для доступа к учебным материалам в LMS Odin слушателям необходимо стандартное программное обеспечение (операционная система, офисные программы) и выход в Интернет.

1.10. Особенности (принципы) построения дополнительной профессиональной программы повышения квалификации

Учебный план программы повышения квалификации сочетает в себе образовательные компоненты и практическую направленность, наличие ключевых дисциплин и тем занятий.

К преподаванию приглашенные штатные преподаватели университета, имеющие значительные практический, научный и преподавательский опыт в ведении соответствующих дисциплин на дополнительных образовательных программах по направлению.

Разработка и обновления учебно-методических материалов осуществляется преподавателями Сибирского федерального университета в соответствии с изменениями нормативно-правовой базы.

1.11. Документ об образовании: удостоверение о повышении квалификации установленного образца.

II. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Обучение по программе реализуется в дистанционном формате с применением технологий дистанционного обучения в электронной среде. Лекционный материал представляется в виде записей занятий, текстовых материалов, презентаций. Данные материалы сопровождаются практическими заданиями, заданиями для самостоятельной работы, тестами.

Материально-технические условия реализации программы

В ФГАОУ ВО «Сибирский федеральный университет» созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств, которые обеспечивают освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся.

Учебно-методическое и информационное обеспечение программы модуля

Программа реализуется заочно с применением электронного обучения и дистанционных образовательных технологий. Она включает занятия лекционного типа, интерактивные формы обучения, семинарские занятия.

По данному курсу имеются материалы для размещения в электронном курсе в системе электронного обучения LMS Odin. Обучающиеся могут дополнить представленные материалы, подключая к учебной работе иные источники информации, освещающие рассматриваемые вопросы.

Содержание комплекта учебно-методических материалов

По программе разработан электронный курс в системе электронного обучения LMS Odin. Материалы курса содержат: систему навигации по программе (учебно-тематический план, график работы по программе, сведения о результатах обучения, о преподавателях программы, чат для объявлений и вопросов преподавателям), набор видеолекций, презентации к лекциям, набор ссылок на внешние образовательные ресурсы и инструменты, систему заданий с подробными инструкциями, списки основной и дополнительной литературы. В электронном курсе реализована система обратной связи.

Виды и содержание самостоятельной работы

Самостоятельная работа слушателей проходит в дистанционном режиме, включает освоение предоставленного преподавателем материала, поиск в учебной литературе ответов на проблемные вопросы, касающихся предмета учебного занятия, выполнение практических работ, решение и разбор кейсов, выполнение расчетных заданий, прохождение пробного тестирования, подготовку к итоговой аттестации.

Видами заданий для самостоятельной работы могут быть: чтение текста (учебника, первоисточника, дополнительной литературы); изучение нормативных материалов; ответы на контрольные вопросы; аналитическая

обработка текста (аннотирование, рецензирование, реферирование и др.); подготовка сообщений к выступлению на семинаре; подготовка рефератов, докладов; тестирование и др.

Критериями оценки результатов самостоятельной работы могут являться:

– уровень освоения слушателем теоретических знаний при выполнении практических задач;

– обоснованность и четкость изложения ответа: оформление материала в соответствии с требованиями.

Выполнение данных работ осуществляется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

III. КАДРОВЫЕ УСЛОВИЯ

Руководитель программы:

Почекутова Елена Николаевна, кандидат экономических наук, доцент, почетный работник сферы образования Российской Федерации, директор центра дополнительного профессионального образования государственных и муниципальных служащих Сибирского федерального университета, руководитель программы, разработчик программы.

Преподаватели:

Черников Дмитрий Юрьевич, кандидат технических наук, доцент, заведующий базовой кафедрой инфокоммуникаций Института инженерной физики и радиоэлектроники Сибирского федерального университета, преподаватель, разработчик программы.

Гутник Сергей Иосифович, кандидат юридических наук, доцент кафедры деликтологии и криминологии Юридического института Сибирского федерального университета, преподаватель программы.

Красноусов Сергей Дмитриевич, кандидат юридических наук, доцент, доцент базовой кафедры антимонопольного и тарифного регулирования ФАС Института экономики, государственного управления и финансов Сибирского федерального университета, преподаватель программы.

Булавчук Александр Михайлович, старший преподаватель кафедры социально-экономического планирования Института экономики, государственного управления и финансов Сибирского федерального университета, преподаватель программы.

Феденко Анастасия Петровна, заместитель директора центра дополнительного профессионального образования государственных и муниципальных служащих Сибирского федерального университета, куратор программы, разработчик программы.

IV. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

4.1. Учебно-методическое обеспечение

1. Указ Президента РФ «О стратегии национальной безопасности Российской Федерации» от 31.12.2015 №683.
2. Указ Президента РФ от 12.08.2002 № 885 «Об утверждении общих принципов служебного поведения государственных служащих».
3. Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
6. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (с изм. и доп., вступ. в силу с 01.10.2022).
7. Постановление Правительства РФ от 24.10.2011 № 861 (ред. от 17.08.2022) «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)» (вместе с «Положением о федеральной государственной информационной системе «Федеральный реестр государственных и муниципальных услуг (функций)», «Правилами ведения федеральной государственной информационной системы «Федеральный реестр государственных и муниципальных услуг (функций)», «Положением о федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)», «Требованиями к региональным порталам государственных и муниципальных услуг (функций)», «Положением о федеральной государственной информационной системе «Единая система предоставления государственных и муниципальных услуг (сервисов)») (с изм. и доп., вступ. в силу с 24.08.2022).
8. Распоряжение Правительства РФ от 11.04.2022 № 837-р (ред. от 24.10.2022) «О Концепции перехода к предоставлению 24 часа в сутки 7 дней в неделю абсолютного большинства государственных и муниципальных услуг без необходимости личного присутствия граждан».

Основная (учебная) литература

1. Галуев Г.А. Принципы построения и основы функционирования систем и сетей связи: Учебно-методическое пособие. – Таганрог: Изд-во ТРТУ.2000. – 100 с.
2. Государственное и муниципальное управление: учебник / под ред. проф. Н.И. Захарова. –М.: ИНФРА-М, 2022. – 289 с. [Электронный ресурс]. – (Высшее образование: Бакалавриат). – URL: https://znanium.com/catalog/product/1859958(дата обращения: 12.12.2022). – Режим доступа: по подписке.

3. Заленская М.К., Тарбазанов К.В., Черников Д.Ю. Практика конфигурирования коммутаторов L2 компании Huawei для обработки нетегированного трафика // Успехи современной радиоэлектроники. – 2019. – № 12. – С. 220–225.

4. Заленская М.К., Черников Д.Ю. Формирование компетенций в области телекоммуникации при изучении технологий Huawei // Инновационные, информационные и коммуникационные технологии. – 2019. – № 1. – С. 167–172.

5. Иванов А.А. Цифровая этика и право // Закон. – 2021. – № 4. – С. 67–73.

6. Иванов, В.В. Государственное и муниципальное управление с использованием информационных технологий / В.В. Иванов, А.Н. Коробова. – М.: ИНФРА-М, 2021. – 383 с. – (Национальные проекты). – URL: https://znanium.com/catalog/product/1141773(дата обращения: 12.12.2022). – Режим доступа: по подписке.

7. Ковалева Н.Н. Информационное право России: учебное пособие / Н.Н. Ковалева. – М.: Дашков и К, Ай Пи Эр Медиа, 2016. – 352 с.

8. Копылова Н.Г., Черников Д.Ю. Виртуальный лабораторный практикум на основе эмулятора eNSP. / В сб.: Информатизация образования и методика электронного обучения: цифровые технологии в образовании // Материалы IV Междунар. научн. конф. в 2-ух ч. – Красноярск, 2020. – С. 186–190.

9. Копылова Н.Г., Черников Д.Ю. Изучение сетевого оборудования компании Huawei с использованием симулятора eNSP / В сб.: Информатизация образования и методика электронного обучения // Материалы III Междунар. научн. конф.; Сибирский федер. ун-т, Институт космических и информационных технологий. – Красноярск, 2019. – С. 166–171.

10. Липковская В.В., Лупачева М.А. Компоновка и настройка системных параметров eNSP-моделей оборудования Huawei / В сб.: Современные проблемы радиоэлектроники // Материалы XXII Всерос. научн.-техн. конф. С междунар. участием, Красноярск, 14–15 мая 2020 г./ отв. ред. Ф.В. Зандер. – Красноярск: Сиб. федер. ун-т, 2020. – 314 с.

11. Терещенко Л.К. Правовой режим персональных данных и безопасность личности // Закон. – 2013. – № 6. – С. 38.

12. Черников Д.Ю., Тарбазанов К.В., Заленская М.К. Использование эмулятора eNSP для отладки конфигураций телекоммуникационного оборудования компании Huawei // Вестник Восточно-Сибирской Открытой Академии. 2019. – № 34. – С. 11.

13. Этика государственной и муниципальной службы: учебник и практикум для вузов / Е.Д. Богатырев, А.М. Беляев, С.Г. Еремин; под ред. С.Е. Прокофьева. – 2-е изд., перераб. и доп. –М.: Издательство Юрайт, 2023. – 326 с. – (Высшее образование)// Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/512370(дата обращения: 11.12.2022).

14. Этика и «цифра»: от проблем к решениям/ под ред. Е.Г. Потаповой, М.С. Шклярук. – М.: РАНХиГС, 2021. – 184 с.

Дополнительная литература

1. Амелин, Р.В. Правовой режим государственных информационных систем: монография / под ред. С.Е. Чаннова. – М.: ГроссМедиа, 2016. – 338 с.

2. Грипич, С.А. Правовые аспекты внедрения цифровых технологий в государственное управление // Государственная власть и местное самоуправление. – 2021. – № 2. – С. 47–50.

3. Гриценко, Е.В. Право на хорошее управление в условиях цифровой трансформации // Сравнительное конституционное обозрение. – 2022. № 4. – С. 15–36.

4. Караваева, Е.Д. Управление организацией в условиях цифровизации: учебное пособие. – СПб.: Наукоемкие технологии, 2020. – 68 с.

5. Систематизация и электронное кодирование функций и полномочий в системе публичного управления: монография / Г.А. Бученков, Ю.А. Головин, Д.В. Карпухин и др.; под ред. И.Л. Бачило, М.А. Лапиной. – М.: Юстиция, 2016. – 210 с.

6. Швабауэр, А.В. Кардинальное изменение правил оказания госуслуг и конституционные права граждан // Государственная власть и местное самоуправление. – 2021. – № 10. – С. 3–7.

4.2.Информационное обеспечение

Программа реализуется с применением электронного обучения и дистанционных образовательных технологий. Она включает занятия лекционного типа, интерактивные формы обучения, семинарские занятия.

По данному курсу имеются материалы для размещения в электронном курсе в системе электронного обучения LMS Odin. Обучающиеся могут дополнить представленные материалы, подключая к учебной работе иные источники информации, освещающие рассматриваемые вопросы.

IV. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4.1. Формы аттестации, оценочные материалы, методические материалы

Оценка качества освоения программы включает текущую и итоговую аттестацию обучающихся.

Текущий и промежуточный контроль осуществляется в форме проведения контрольных работ, лабораторных работ, тестов.

Методические материалы, необходимые для выполнения текущих заданий, представлены в соответствующих элементах электронного обучающего курса и включают описание задания, методические рекомендации по его выполнению, критерии оценивания.

4.2. Требования и содержание итоговой аттестации

Итоговая аттестация слушателя дополнительной образовательной программы повышения квалификации «Информационные технологии информационной безопасности» представляет собой тестирование по дисциплинам учебного плана с использованием сервисов электронной образовательной среды.

К итоговому тестированию по программе повышения квалификации допускаются слушатели, успешно выполнившие задания текущей аттестации.

Шкала оценивания итогового тестирования:

– 75 % верных ответов и более – оценка «зачтено»;

– менее 75 % верных ответов – оценка «не зачтено».

Тест содержит 65 вопросов, продолжительность тестирования 60 минут.

Примеры тестовых заданий для итогового тестирования

1. Шифрование информации — это:

а) процесс преобразования, при котором информация удаляется;

б) процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов;

в) процесс ее преобразования, при котором содержание информации изменяется на ложную;

г) процесс преобразования информации в машинный код.

2. Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?

а) защита от сбоев в электропитании;

б) защита от сбоев серверов, рабочих станций и локальных компьютеров;

в) защита от сбоев устройств для хранения информации;

г) защита от утечек информации электромагнитных излучений.

3. Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе, может быть осуществлен только тем лицам, которые на это имеют право:

а) управление доступом;

б) конфиденциальность;
в) аутентичность;
г) целостность;
д) доступность.

4. Представитель нанимателя вправе освободить гражданского служащего от замещаемой должности и уволить его с гражданской службы при:

а) отказе гражданского служащего от получения дополнительного профессионального образования;

б) отказе перевода на другую должность гражданской службы;

в) наличии отрицательного мотивированного отзыва непосредственного руководителя служащего;

г) наличии отрицательного мотивированного отзыва коллег служащего.

5. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем:

а) защита от сбоев в электропитании;
б) защита от сбоев серверов, рабочих станций и локальных компьютеров;
в) защита от сбоев устройств для хранения информации;
г) защита от утечек информации электромагнитных излучений.

Слушатель, прошедший итоговую аттестацию с оценкой «зачтено» считается успешно выполнившим программу повышения квалификации.

РАБОЧАЯ ПРОГРАММА
модуля
«Информационные технологии информационной безопасности»

1. Аннотация

Программа призвана решать задачи формирования основ для понимания принципов построения телекоммуникационных топологий информационной безопасности опираясь на информацию о принципах работы устройств в составе различных телекоммуникационных топологий, принципов функционирования сетевых топологий различного назначения и устройств коммутации в их составе, также формирования теоретических основ для разработки новых схемотехнических решений с использованием коммутаторов.

Также курс включает в себя рассмотрение вопросов, связанных с системой информационных прав, источниками нормативно-правового регулирования информационной открытости деятельности органов власти. Рассматриваются принципы обеспечения информационной открытости, а также ситуации, при которых информация о деятельности государственных органов сохраняется в тайне.

В результате изучения дисциплины слушатель будет

Знать:

– модели угроз несанкционированного доступа к сетям электросвязи;

– программно-аппаратные средства обеспечения защиты сетей;

– сетевые протоколы и их параметры настройки;

– средства анализа и контроля защищенности в конвергентных информационных системах;

– нормативные правовые акты в области связи, информатизации и защиты информации, защиты персональных данных;

– руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;

– методы комплексного обеспечения защиты сетей электросвязи;

– требования по обеспечению доступа к открытой информации о деятельности органов (организаций).

Уметь:

– выявлять и оценивать угрозы несанкционированного доступа к сетям связи, организует работу по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак;

– устанавливать и настраивать параметры сетевых протоколов;

– проводить мониторинг и анализ нормативных правовых актов, руководящих и методических документов уполномоченных федеральных органов исполнительной власти в сфере защиты информации;

– разрабатывать предложения по совершенствованию и повышению эффективности принимаемых технических мер и проводимых организационных мероприятий по обеспечению информационной безопасности органа

(организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак;

– организовывать работы по выполнению требований режима защиты информации ограниченного доступа в сети электросвязи.

Владеть:

– методами оценки уязвимостей сетей электросвязи с точки зрения возможности несанкционированного доступа к ним;

– навыками разработки и организации выполнения мероприятий в соответствии с положениями политики информационной безопасности в органе (организации), согласование иных документов органа (организации) в части обеспечения информационной безопасности;

– методикой проведения мониторинга нормативных правовых актов, руководящих и методических документов уполномоченных федеральных органов исполнительной власти в сфере защиты и обеспечения безопасности информации;

– навыками контроля выполнения требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного порядка выполнения работ при решении вопросов, касающихся защиты информации, соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации.

2. Содержание

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Технические аспекты информационной безопасности (80 часов)			
Построение и администрирование телекоммуникационных сетей и систем (40 ч.)	Концепция построения мультисервисных пакетных сетей (4 ч.)	Концепция построения мультисервисных пакетных сетей (4 ч.). Программно определяемые (SD) средства информационной безопасности (10 ч.). Комплексное задание (2 ч.)	Изучение материалов, подготовка вопросов к семинарскому занятию, выполнение практических заданий (10 ч.). Подготовка комплексного задания (10 ч.)
Технические основы информационной безопасности (40 ч.)	Угрозы безопасности информации в конвергентных информационных системах (4 ч.). Организация технической защиты конфиденциальной информации (2 ч.)	Угрозы безопасности информации в конвергентных информационных системах (6 ч.). Организация технической защиты конфиденциальной информации (8 ч.)	Изучение материалов, подготовка вопросов к семинарскому занятию, выполнение практических заданий (16 ч.). Тестирование (4 ч.)

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Правовые аспекты информационной безопасности (62 ч.)			
Система нормативно-правовых актов по вопросам информационной безопасности (32 ч.)	Общая характеристика законодательства РФ об информационной безопасности (4 ч.). Обеспечение доступа к информации о деятельности органов власти (2 ч.)	Правовые основы регулирования деятельности по обеспечению информационной безопасности (6 ч.). Обеспечение доступа к информации о деятельности органов власти (4 ч.)	Изучение материалов, подготовка вопросов к семинарскому занятию, выполнение практических заданий (10 ч.). Тестирование (6 ч.)
Информационная открытость органов государственной власти и местного самоуправления (30 ч.)	Информационная открытость органов государственного управления (2 ч.). Предоставление публичных услуг в электронной форме (2 ч.)	Способы обеспечения информационной открытости деятельности органов публичной власти (4 ч.). Цифровая этика и право (6 ч.). Предоставление публичных услуг в электронной форме (2 ч.)	Изучение материалов, подготовка вопросов к семинарскому занятию, выполнение практических заданий (10 ч.). Тестирование (4 ч.)

3. Оценка качества освоения программы модуля (формы аттестации, оценочные и методические материалы)

Форма итоговой аттестации — зачет в форме теста.

Шкала оценки:

– 70% верных ответов и более – оценка «зачтено».

Текущая аттестация проходит в форме обсуждений на семинарах, самостоятельного анализа заданий преподавателя.

Промежуточная аттестация проводится в виде выполнения практических заданий в ходе семинарских занятий и тестирования.

Примеры практических заданий

1. Привести и обосновать максимальное количество виртуальных сетей — VLAN, которые могут быть организованы на управляемых коммутаторах.

2. Привести и пояснить возможные варианты для команд визуализации отнесения портов коммутаторов к организованным на нем VLAN, а также возвращения любого из портов к VLAN по умолчанию.

3. Орган местного самоуправления начал взимать плату за предоставление информации о своей деятельности. В частности, деньги взимались за предоставление справок в отношении обращающихся, сведений о количественных показателях органов, текстов проектов нормативных правовых актов, порядка обжалования муниципальных нормативных правовых актов.

1. Оцените, законно ли это?

2. В каком объёме государственные органов и органы местного самоуправления обязаны предоставлять информацию гражданам бесплатно?

3. Чем урегулирован порядок предоставления информации о деятельности органа государственной власти или органа местного самоуправления?

Пример комплексного задания

Задание 1. В эмуляторе телекоммуникационных топологий eNSP считать с жесткого диска произвольную топологию с использованием коммутирующего активного оборудования. Получить перечень всех VLAN, которые были организованы на каждом из коммутаторов, которые использованы в данной телекоммуникационной топологии.

Цель задания: получить опыт работы с командной строкой операционной системы VRP, необходимых для использования технологий виртуальных сетей – VLAN, при работе коммутаторов под управлением данной операционной системы.

Инструкция:

Шаг 1. Основываясь на изученном материале считать произвольную телекоммуникационную топологию на рабочее поле эмулятора eNSP.

Шаг 2. Используя функционал эмулятора eNSP, проверить наличие соединений между моделями маршрутизирующего активного телекоммуникационного оборудования, использованного в подготовленной топологии.

Шаг 3. Проверить текущее состояние интерфейсов, которые использованы для организации взаимодействия между моделями маршрутизирующего телекоммуникационного оборудования.

Шаг 4. Вывести на экран терминала, подключенного к консольному порту одного из маршрутизаторов, перечень всех возможных вариантов VRP команд, которые могут быть использованы для этого устройства

Обратную связь по выполненной работе слушатель получит напрямую. Ряд работ будут рассмотрены и резюмированы на практическом занятии.

Критерии оценивания заданий и лабораторных работ

Баллы	1 балл	2 балла	3 балла
Критерий	Задание выполнено частично, требуется серьезная доработка	Задание выполнено, но требуется некоторая доработка	Задание выполнено полностью, никакой доработки не требуется

Задание для самостоятельной работы

В самостоятельную работу входит изучение материалов курса и закрепление полученных знаний за счет воспроизведения телекоммуникационных топологий средствами эмулятора eNSP с требованиями

обязательного использования коммутирующего и маршрутизирующего оборудования.

Примеры тестовых заданий для итогового тестирования

1. Что можно отнести к техническим мерам ИБ?
   а) разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства;
   б) охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.;
   в) защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое;
   г) простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов;
   д) в административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.
2. Потенциальные угрозы, против которых направлены технические меры защиты информации:
   а) потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей;
   б) потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения;
   в) потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками;
   г) потери информации из-за не достаточной установки сигнализации в помещении;
   д) процессы преобразования, при котором информация удаляется.
3. Наибольшую угрозу для безопасности сети представляют:
   а) несанкционированный доступ, электронное подслушивание и преднамеренное или неумышленное повреждение;
   б) вскрытие стандартной учётной записи пользователя;
   в) вскрытие стандартной учётной группы администратора;
   г) копирование файлов, которые были изменены в течение дня, без отметки о резервном копировании.
4. Примером защиты через права доступа является:
   а) присвоение каждому пользователю определенного набора прав;
   б) размещение серверов в специальном запертом помещении с ограниченным доступом;

в) присвоение пароль каждому общедоступному ресурсу;

г) наличие преобразователя микрофона.

5. Режим конфиденциальной информации не устанавливается в отношении одного из следующих видов информации:

а) о личной жизни человека;

б) о государственной тайне;

в) персональных данных;

г) о деятельности государственных органов.

6. Открытость информации в архивных фондах обеспечивается:

а) различными режимами доступа к информации;

б) переходом информации из одной категории доступа в другую;

в) различными режимами доступа к информации и переходом информации из одной категории доступа в другую;

г) правовым статусом архивного фонда;

7. Взимается ли плата за предоставление информации о деятельности государственного органа или органа местного самоуправления:

а) взимание такой платы во всех случаях запрещено;

б) плата взимается за предоставление любой информации о деятельности государственного органа или органа местного самоуправления;

в) плата взимается по усмотрению государственного органа или органа местного самоуправления;

г) плата взимается только в случае её предоставления по запросу, если объём запрашиваемой и получаемой информации превышает объём, установленный Правительством РФ для бесплатного предоставления.

Программу составили:

Канд. эконом. наук, доцент, директор центра дополнительного профессионального образования государственных и муниципальных служащих СФУ — Е.Н. Почекутова

Канд. техн. наук, заведующий кафедрой инфокоммуникаций Института инженерной физики и радиоэлектроники СФУ — Д.Ю. Черников

Зам. директора центра дополнительного профессионального образования государственных и муниципальных служащих СФУ — А.П. Феденко

Руководитель программы:

Канд. эконом. наук, доцент, директор центра дополнительного профессионального образования государственных и муниципальных служащих СФУ — Е.Н. Почекутова