Для служебного пользования
Экз. № 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

СОГЛАСОВАНО	УТВЕРЖДАЮ
Начальник 1 Управления ФСТЭК России	Первый проректор по учебной работе
_____ Н.М. Мартинец	_____ Е.Е. Шваков
«__» _____ 2018 г.	«24» января 2019 г.
М.П.	М.П.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ

Барнаул 2018

1. Общие положения

Настоящая программа повышения квалификации «Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» (далее - программа повышения квалификации) разработана с учетом положений:

Федерального закона от 29 декабря 2012 г. №273-ФЗ «Об образовании в Российской Федерации»;

постановления Правительства Российской Федерации от 6 мая 2008 г. № 362 «Об утверждении государственных требований к профессиональной переподготовке, повышению квалификации государственных гражданских служащих Российской Федерации»;

приказа Министерства образования и науки Российской Федерации от 1 июля 2013 г. №499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

приказа Министерства образования и науки Российской Федерации от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»;

профессионального стандарта «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н;

профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н.

Программа повышения квалификации разработана в соответствии с Методическими рекомендациями по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической зашиты информации, утвержденными ФСТЭК России 16 апреля 2018 г., и примерной программой повышения квалификации «Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну», утвержденной ФСТЭК России 30 марта 2016 г.

Программа повышения квалификации реализуется на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Алтайский государственный университет» (ФГБОУ ВО «Алтайский государственный университет») (АлтГУ), г. Барнаул.

Разработчики:

Поляков В.В., д.ф-м.н., профессор, декан физико-технического факультета АлтГУ, заведующий кафедрой прикладной физики, информатики и информационной безопасности

Мансуров А.В., к.т.н., доцент кафедры прикладной физики, информатики и информационной безопасности

Программа повышения квалификации разработана в инициативном порядке.

Программа повышения квалификации обсуждена на заседании кафедры прикладной физики, электроники и информационной безопасности 29 марта 2018 г., протокол № 8-2017/18, рассмотрена на заседании учебно-методической комиссии физико-технического факультета, протокол № 7-2017/18 от 11 апреля 2018 г.

2. Цель реализации программы повышения квалификации Целью реализации программы повышения квалификации является совершенствование компетенций, необходимых для осуществления профессиональной деятельности, повышение профессионального уровня в рамках имеющейся квалификации руководителей (включая государственных гражданских служащих), работающих в области технической защиты информации (ТЗИ) (далее - обучающихся), в части организации защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее - информация ограниченного доступа).

Обучающиеся по программе повышения квалификации готовятся к осуществлению следующих видов профессиональной деятельности: организационно-управленческая и проектная.

Объектами профессиональной деятельности обучающихся являются:

объекты информатизации, включающие автоматизированные (информационные) системы различного уровня и назначения, средства и системы обработки информации и средства их обеспечения, а также помещения, предназначенные для ведения конфиденциальных переговоров (защищаемые помещения);

технические каналы утечки информации (ТКУИ) на объектах информатизации и угрозы безопасности информации в автоматизированных (информационных) системах;

система нормативных правовых актов, методических документов, национальных и международных стандартов в области ТЗИ ограниченного доступа, не содержащей сведения, составляющие государственную тайну (конфиденциальной информации, далее - ТЗКИ);

способы и средства, используемые для обеспечения ТЗКИ.

Задачами профессиональной деятельности обучающихся являются:

а) в организационно-управленческой деятельности:

– планирование деятельности по обеспечению ТЗКИ (разработка документов, регламентирующих в организации политики (правила, процедуры) по обеспечению ТЗКИ);

– организация внедрения и применения политик (правил, процедур) по обеспечению ТЗКИ в организации;

– проведение контроля (мониторинга) и анализа применения политик (правил, процедур) по обеспечению ТЗКИ в организации;

– поддержка и совершенствование деятельности по обеспечению ТЗКИ в организации;

б) в проектной деятельности:

– определение ТКУИ на объектах информатизации и угроз безопасности информации в автоматизированных (информационных) системах;

– формирование требований к обеспечению ТЗКИ на объектах информатизации (формирование требований к системе защиты информации объекта информатизации);

– выбор способов и средств для обеспечения ТЗКИ на объектах информатизации (разработка системы защиты информации);

– внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации (внедрение системы защиты информации объекта информатизации).

3. Требования к квалификации поступающего на обучение

К освоению программы допускаются лица, имеющие высшее образование по направлению подготовки (специальности) в области информационной безопасности, или прошедшие профессиональную переподготовку для выполнения нового вида профессиональной деятельности в области ТЗИ, подтвержденное документом об образовании.

4. Планируемые результаты обучения

Процесс освоения обучающимися программы повышения квалификации направлен на совершенствование следующих компетенций:

а) общепрофессиональных:

– способность использовать нормативные правовые акты, методические документы, национальные и международные стандарты в области ТЗКИ в своей профессиональной деятельности;

– способность определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;

– способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области ТЗИ;

б) профессиональных:

в организационно-управленческой деятельности:

– способность планировать деятельность по обеспечению ТЗКИ (разрабатывать документы, регламентирующие в организации политики (правила, процедуры) по обеспечению ТЗКИ);

– способность организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ в организации;

– способность проводить контроль (мониторинг) и анализ применения политик (правил, процедур) по обеспечению ТЗКИ в организации;

– способность поддерживать и совершенствовать деятельность по обеспечению ТЗКИ в организации;

в проектной деятельности:

– способность определять ТКУИ на объектах информатизации и угрозы безопасности информации в автоматизированных (информационных) системах;

– способность формировать требования к обеспечению ТЗКИ на объектах информатизации (формировать требования к системе защиты информации объекта информатизации);

– способность организовывать выбор способов и средств для обеспечения ТЗКИ на объектах информатизации (разрабатывать системы защиты информации);

– способность организовывать внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации (внедрять системы защиты информации объекта информатизации).

В результате освоения программы повышения квалификации обучающиеся должны получить знания, умения и навыки, обеспечивающие совершенствование соответствующих компетенций.

Освоившие программу должны:

а) знать:

– нормативные правовые акты Российской Федерации, нормативные и методические документы в области ТЗИ (в том числе по защите информации от ее утечки по техническим каналам, защите информации от несанкционированного доступа (НСД));

– основы построения информационных систем и формирования информационных ресурсов ограниченного доступа;

– виды конфиденциальной информации;

– перечни сведений конфиденциального характера, основные требования и рекомендации по их защите;

– действующую систему сертификации средств защиты информации по требованиям безопасности информации;

– основы лицензирования деятельности по ТЗКИ и (или) деятельности по разработке и производству средств защиты информации;

– возможные ТКУИ на объектах информатизации и угрозы безопасности информации в автоматизированных (информационных) системах;

– организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов (в том числе по защите информации от утечки по техническим каналам, защите информации от НСД и по защите информации от специальных воздействий);

– организационные и технические мероприятия по ТЗКИ и контролю защищенности информации;

– общие требования по ТЗКИ (в том числе по защите информации от ее утечки по техническим каналам, защите информации от НСД), нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля их выполнения;

– требования к средствам ТЗКИ и контроля защищенности информации;

– средства ТЗКИ и контроля защищенности информации;

– показатели оценки защищенности информации, методы их расчета и анализа, методы и средства контроля защищенности информации;

– порядок организации взаимодействия структурных подразделений по ТЗИ при решении вопросов ТЗКИ, организационного и технического контроля в организации или в органах государственной власти;

– структуру, назначение, задачи, полномочия, техническую оснащенность и возможности структурных подразделений по ТЗИ в организации или в органах государственной власти;

– сертифицированные по требованиям безопасности информации основные технические средства и системы (ОТСС) и вспомогательные технические средства и системы (ВТСС), порядок оснащения ими подразделений по ТЗИ;

– порядок проведения аттестации объектов информатизации по требованиям безопасности информации;

– основы проведения научных исследований и разработок в области ТЗКИ;

– достижения науки и техники в стране и за рубежом в области ТЗИ;

б) уметь:

– применять на практике требования нормативных правовых актов, нормативных и методических документов в области ТЗКИ;

– организовывать работы по ТЗКИ на объектах информатизации и автоматизированных (информационных) системах;

– разрабатывать нормативные, методические и плановые документы по ТЗКИ;

– руководить деятельностью подразделений по ТЗИ при решении задач ТЗКИ;

– планировать и организовывать мероприятия по контролю защищенности информации;

– определять возможные ТКУИ на объектах информатизации и угрозы безопасности информации в автоматизированных (информационных) системах;

– формировать требования по ТЗКИ (в том числе по защите информации от ее утечки по техническим каналам, защите информации от НСД);

– формировать требования к средствам ТЗКИ и контроля защищенности информации;

– применять средства ТЗКИ и контроля защищенности информации;

в) владеть навыками:

– работы с действующими нормативными правовыми актами, нормативными и методическими документами в области ТЗКИ;

– организации разработки необходимой документации по вопросам ТЗКИ;

– руководства работами по выявлению ТКУИ и определению угроз безопасности информации применительно к объектам защиты, определению требований по ТЗКИ объектов защиты, контролю защищенности информации на объектах защиты;

– организации и проведения научных исследований и разработок в области ТЗКИ;

– руководства деятельностью подразделений по ТЗКИ в организации или в органе государственной власти при решении задач ТЗКИ;

– организации проведения контроля защищенности конфиденциальной информации в организации или в органе государственной власти при решении задач ТЗКИ;

– организации аттестации объектов информатизации, проведения специальных исследований, лицензирования и сертификации в области ТЗКИ.

5. Условия реализации программы

Лабораторная база АлтГУ оснащена современным оборудованием, стендами, приборами, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой повышения квалификации.

Компьютерные классы оборудованы автоматизированными рабочими местами для занятий по учебным дисциплинам из расчета одно рабочее место на одного обучающегося при проведении занятий в данных классах.

АлтГУ имеет необходимый комплект лицензионного программного обеспечения и сертифицированные программные и аппаратные средства защиты информации.

Формирование профессиональных компетенций обеспечивается широким использованием в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Реализация программы повышения квалификации обеспечивается руководящими и научно-педагогическими работниками АлтГУ, а также специалистами, привлекаемыми к реализации программы на условиях гражданско-правового договора.

В рамках программы повышения квалификации предусматривается проведение практических занятий с привлечением специалистов высшего уровня квалификации в области ТЗИ, представителей российских компаний, государственных и общественных организаций.

Программа повышения квалификации предусматривает проведение занятий в соответствии с целевыми установками программы, которые обеспечивают требуемый уровень усвоения учебного материала. Знания приобретаются в основном проведением ряда взаимосвязанных семинаров и практических занятий, компьютерного моделирования последствий принимаемых решений, деловых и ролевых игр, разбором конкретных ситуаций, тренингов и др.

Занятия проводятся на базе лабораторий и специализированных классов кафедры прикладной физики, электроники и информационной безопасности (ПФЭБ) физико-технического факультета (ФТФ) ФГБОУ ВО «Алтайский государственный университет». Место проведения занятий - г. Барнаул, пр. Красноармейский, д.90, ФГБОУ ВО «Алтайский государственный университет», физико-технический факультет.

Каждому обучающемуся обеспечивается доступ к библиотечному фонду, укомплектованному печатными и электронными изданиями основной учебной литературы, изданными за последние 10 лет, из расчета не менее одного экземпляра на четыре-пять обучающихся.

В фонд дополнительной литературы, помимо учебной, включены официальные, справочно-библиографические и специализированные периодические издания, в том числе правовые нормативные акты и нормативные методические документы в области информационной безопасности, из расчета один-два экземпляра на каждые 20 обучающихся.

Для обучающихся обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам по тематике информационной безопасности.

Передача программы повышения квалификации другой образовательной организации допускается при создании условий и соблюдении требований законодательства Российской Федерации о порядке обращения со служебной информацией ограниченного распространения и наличии разрешения федеральных государственных органов, в ведении которых находятся организации, осуществляющие образовательную деятельность.

Внесение изменений в программы повышения квалификации осуществляется в соответствии с требованиями, установленными законодательными и иными

нормативными правовыми актами Российской Федерации в области образования и порядком обращения со служебной информацией ограниченного распространения.

Сведения, составляющие государственную тайну, в данной программе повышения квалификации не используются.

6. Формы аттестации

По результатам каждого модуля обучающийся в соответствии с учебным планом проходит тестирование. Итоговой аттестацией является экзамен в форме тестирования и защита итоговой работы по основным вопросам программы повышения квалификации.

Перечень тестов, используемых для проведения экзамена, целесообразно формировать на основе перечней тестов, выносимых для контроля знаний обучающихся при проведении промежуточных аттестаций по учебным модулям, представленным в рабочей программе курса повышения квалификации.

Для проведения итоговой аттестации. создается аттестационная комиссия, состав которой утверждается приказом ректора АлтГУ.

В целях обеспечения объективного определения теоретической и практической подготовленности обучающихся к выполнению профессиональных задач по результатам обучения в состав аттестационной комиссии могут включаться (по согласованию) представители Управления ФСТЭК России по Сибирскому федеральному округу.

Обучающемуся, успешно освоившему программу повышения квалификации и прошедшему итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

7. Учебный план программы повышения квалификации

7.1. Категория обучающихся: руководители структурных подразделений (включая государственных служащих), работающие в области ТЗИ в части организации работ по защите информации ограниченного доступа.

7.2. Форма обучения: очная.

7.3. Продолжительность обучения: 108 часов.

7.4. Режим занятий: не более 8 академических часов с преподавателем в день, с перерывом на обед (не менее 45 минут).

Для всех аудиторных занятий продолжительность академического часа равна 45 минут.

Учебная нагрузка не превышает 54 часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы обучающегося.

7.5. План учебного процесса

№, п/п	Наименование учебных модулей, тем	Всего учебных часов	Часов занятий с преподавателем	Распределение времени, час				Формы аттестации и контроля знаний
				Лекции	Семинары	Практические	Самостоятельная работа	
1	2	3	4	5	6	7	8	9
1	Учебный модуль №1. Планирование и организация работ по защите информации	46	32	10	8	14	14	Текущий контроль. Тестирование
1.1	Тема № 1. Защищаемые информация и информационные ресурсы. Цели и задачи ТЗИ	4	2	2	-	-	2	-
1.2	Тема № 2. Определение угроз безопасности информации ограниченного доступа	14	10	2	-	8	4	-
1.3	Тема № 3. Нормативно-правовые основы ТЗКИ	8	6	2	4	-	2	-
1.4	Тема № 4. Планирование работ по ТЗКИ	12	8	2	2	4	4	-
1.5	Тема № 5. Требования по защите информации и создание системы защиты информации	8	6	2	2	2	2	-
2	Учебный модуль №2. Выполнение мероприятий по защите информации и применение технических средств в интересах ТЗКИ	26	18	4	4	10	8	Текущий контроль. Тестирование
2.1	Тема № 1. Организационные основы выполнения мероприятий по защите информации	10	6	2	2	2	4	-
2.2	Тема № 2. Меры и средства ТЗКИ	16	12	2	2	8	4	-
3	Учебный модуль №3. Контроль состояния защиты информации и ТЗКИ.	24	18	8	10	-	6	Текущий контроль. Тестирование
3.1	Тема № 1. Основы организации контроля состояния ТЗКИ	6	4	2	2	-	2	-
3.2	Тема № 2. Методы и средства контроля защищенности информации	10	8	2	6	-	2	-
3.3	Тема № 3. Аттестация объектов информатизации по требованиям к безопасности информации	6	4	2	2	-	2	-

1	2	3	4	5	6	7	8	9
3.4	Тема № 4. Сертификация средств защиты информации	2	2	2	-	-	-	-
4.	Итоговая аттестация	12	4	-	-	-	8	-
4.1.	Итоговое тестирование	-	2	-	-	-	4	Экзамен в форме тестиро-вания
4.2.	Защита итоговой работы	-	2	-	-	-	4	Защита итоговой работы
	ИТОГО:	108	72	22	22	24	36	-

7.6 Сводные данные по бюджету времени

Общий объем времени, отводимого на освоение программы (календарных дней/часов)			Распределение учебного времени (количество часов)					
Всего	Из них		Всего часов учебных занятий	В том числе		Время на самостоятельную работу	Итоговая аттестация	Резерв учебного времени
	Выходные праздничные дни	Учебное время		Учебные занятия по расписанию	Практики			
14	2	108	108	72	-	36	экзамен	-

8. Календарный учебный график

Срок обучения по программе повышения квалификации, недели	1	2	
Виды занятий, предусмотренные программой повышения квалификации	А	А	И

А – аудиторная и самостоятельная работа;
И – итоговая аттестация

9. Рабочая программа учебного курса

9.1 Содержание учебных модулей, тем

Учебный модуль № 1. Планирование и организация работ по ТЗКИ.

Тема № 1. Защищаемые информация и информационные ресурсы. Цели и задачи ТЗИ.

Информация как объект защиты. Информация ограниченного доступа (конфиденциальная информация).

Объекты информатизации: классификация и характеристика.

Защищаемые информация и информационные ресурсы.

Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций.

Основные термины и определения в области ТЗИ.

Цели и задачи ТЗИ.

Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации.

Организация научных исследований и разработок в области ТЗИ.

Тема № 2. Определение угроз безопасности конфиденциальной информации.

Угрозы безопасности конфиденциальной информации.

Классификация ТКУИ.

Классификация и характеристики угроз безопасности информации, связанных с НСД.

Модель угроз безопасности информации.

Методы выявления и анализа угроз безопасности информации. Методы выявления и анализа уязвимостей программного обеспечения, используемого в информационных системах.

Банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемого в информационных системах.

Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в информационных системах.

Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE. Общая система оценки уязвимостей (стандарт CVSS).

Тема № 3. Правовые основы ТЗКИ.

Правовые основы защиты информации. Система документов в области ТЗИ, а также ТЗКИ. Нормативные правовые акты Российской Федерации. Нормативные правовые акты ФСТЭК России. Методические документы. Технические документы (документация). Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Организационно-правовые основы лицензирования деятельности в области защиты информации, аттестации объектов информатизации по требованиям безопасности информации. Система сертификации средств защиты информации. Ответственность за правонарушения в области защиты информации.

Тема № 4. Планирование работ по ТЗКИ.

Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения планов проведения мероприятий по ТЗКИ.

Тема № 5. Требования по защите информации и создание системы защиты информации.

Организация работ по ТЗКИ.

Требования по защите информации, содержащейся в информационной системе (на объекте информатизации).

Требования по защите информации, обрабатываемой техническими средствами, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН).

Требования по защите акустической речевой информации.

Требования по защите информации от НСД.

Требования национальных и международных стандартов по защите информации.

Создание и функционирование системы защиты информации ограниченного доступа как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий.

Стадии и этапы создания системы защиты информации ограниченного доступа.

Порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении.

Комплекс работ по созданию системы защиты информации (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации по требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации).

Разработка эксплуатационной документации на систему защиты информации.

Особенности организации защиты персональных данных.

Учебный модуль № 2. Выполнение мероприятий по ТЗКИ и применение технических средств в интересах ТЗКИ.

Тема № 1. Организационные основы выполнения мероприятий по ТЗКИ.

Комплекс мероприятий по ТЗКИ от утечки по техническим каналам и от НСД к ней.

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.

Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Особенности реализации мероприятий по защите персональных данных.

Тема № 2. Меры и средства ТЗКИ.

Основные меры защиты информации от утечки по техническим каналам. Организационные меры защиты: временные ограничения, территориальные ограничения.

Способы и средства ТЗКИ от утечки по техническим каналам. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам при ее обработке с использованием технических средств. Способы и средства защиты акустической речевой информации от утечки по техническим каналам.

Общая характеристика и классификация мер и средств защиты информации от НСД.

Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ.

Защита информации в локальных вычислительных сетях.

Защита информации при межсетевом взаимодействии.

Защита информации при работе с системами управления базами данных.

Особенности реализации требований по защите информации при взаимодействии абонентов с информационными сетями общего пользования.

Учебный модуль № 3. Контроль состояния ТЗКИ.

Тема № 1. Основы организации контроля состояния ТЗКИ.

Основные задачи контроля состояния ТЗКИ.

Классификация видов контроля состояния ТЗКИ.

Система документов по контролю состояния ТЗКИ.

Вопросы, подлежащие проверке при контроле состояния ТЗКИ в организации.

Организационный и технический контроль состояния ТЗКИ.

Тема № 2. Методы и средства контроля защищенности информации.

Методы и средства контроля защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

Методы и средства контроля защищенности акустической речевой информации от утечки по техническим каналам.

Методы и средства контроля защищенности информации от НСД.

Документирование результатов контроля.

Требования к средствам контроля защищенности информации.

Тема № 3. Аттестация объектов информатизации по требованиям безопасности информации.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Программы и методики аттестационных испытаний. Заключение по результатам аттестации объекта информатизации. Аттестат соответствия объекта информатизации.

Тема № 4. Сертификация средств защиты информации.

Порядок сертификации продукции, используемой в целях защиты конфиденциальной информации: технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля защищенности информации, программных, программно-технических

средств защиты информации, программных средств контроля защищенности информации.

9.2. Лабораторный практикум

В процессе изучения рабочей программы учебного курса лабораторный практикум не предусмотрен.

9.3. Практические занятия (семинары)

9.3.1. Семинары

№ п/п	Номер (наименование) учебного модуля, темы	Тематика семинара	Количество времени, отводимого на проведение семинара (час.)
1	Модуль № 1, Тема № 3	Нормативно-правовые акты и методические документы ФСТЭК России в области ТЗКИ	2
2	Модуль № 1, Тема № 3	Международные и национальные стандарты в области ТЗКИ	1
3	Модуль № 1, Тема № 3	Лицензирование деятельности в области ТЗКИ	1
4	Модуль № 1, Тема № 4	Организация работ по созданию системы защиты информации	2
5	Модуль № 1, Тема № 5	Формирование требований по ТЗКИ	2
6	Модуль № 2, Тема № 1	Защита персональных данных	2
7	Модуль № 2, Тема № 2	Современные технологии защиты информации от НСД	2
8	Модуль № 3, Тема № 1	Организация и порядок проведения контроля состояния ТЗКИ	2
9	Модуль № 3, Тема № 2	Методы и средства контроля защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН	2
10.	Модуль № 3, Тема № 2	Методы и средства контроля защищенности акустической речевой информации	2
11.	Модуль № 3, Тема № 2	Средства контроля защищенности информации от НСД	2
12.	Модуль № 3, Тема № 3	Аттестация объектов информатизации на соответствие требованиям безопасности информации	2

9.3.2. Практические занятия

№ п/п	Номер (наименование) учебного модуля, темы	Тематика практических занятий	Количество времени, отводимого на проведение семинара (час.)
1.	Модуль № 1, Тема № 2	Технические каналы утечки информации, обрабатываемой вычислительной техники	2
2.	Модуль № 1, Тема № 2	Технические каналы утечки акустической речевой информации.	2
3.	Модуль № 1, Тема № 2	Угрозы безопасности информации. Методы выявления и оценки возможности реализации угроз безопасности информации	2
4.	Модуль № 1, Тема № 2	Угрозы безопасности информации, связанные с НСД при ее обработке в автоматизированных системах	2
5.	Модуль № 1, Тема № 4	Разработка руководства по ТЗКИ в организации (на предприятии)	2
6.	Модуль № 1, Тема № 4	Разработка технического задания на создание системы защиты информации	2
7.	Модуль № 1, Тема № 5	Аналитическое обоснование необходимости создания системы защиты информации	2
8.	Модуль № 2, Тема № 1	Разработка организационно-распорядительных документов по ТЗКИ	2
9.	Модуль № 2, Тема № 2	Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН	2
10.	Модуль № 2, Тема № 2	Способы и средства защиты информации от утечек по техническим каналам	2
11.	Модуль № 2, Тема № 2	Меры и средства защиты информации от НСД	4

9.4. Учебно-методическое и информационное обеспечение учебного курса

9.1. основная литература:

1. Основы информационной безопасности: Учебное пособие/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - М.: Горячая линия - Телеком, 2005.

2. Хорев А.А. Техническая защита информации: Учебное пособие для студентов. В 3 т. Т. 1. Технические каналы утечки информации. - М.: Аналитика, 2008.

3. Хорев А.А. Защита информации от утечки по техническим каналам: Учебное пособие. - М.: Министерство обороны Российской Федерации, 2006.

4. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: Форум; Инфра-М, 2012.

5. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации: Учебное пособие / В.С. Горбатов, С.В. Дворянкин, А.П. Дураковский, Р.С. Енгалычев [и др.], под общ. ред. Ю.Н. Лаврухина. - М: НИЯУ МИФИ, 2014. - 560 с.

6. Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации: Учебное пособие / А.А. Голяков, В.С. Горбатов, А.П. Дураковский, А.Е. Панин, М.С. Чистяков; под общ. ред. Ю.Н. Лаврухина. - М: НИЯУ МИФИ, 2014. - 208 с.: ил.

7. Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации: Учебное пособие / В.С. Горбатов, А.П. Дураковский, И.В. Куницын, А.Е. Панин, под общ. ред. Ю.Н. Лаврухина. - М: НИЯУ МИФИ, 2014.-248 с.: ил.

8. Технические средства и методы защиты информации: Учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков; под ред. А.П. Зайцева и А.А. Шелупанова. - 7-е изд. испр. - М.: Горячая линия- Телеком, 2012.

9. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / Ю.Ю. Коваленко. - М.: Горячая линия - Телеком, 2012.

10. Концептуальные основы создания и применения системы защиты объектов / В.А. Воронов, В.А. Тихонов.-М.: Горячая линия - Телеком, 2013.

11. П.Грибунин В.Г. Комплексная система защиты информации на предприятии: Учебное пособие. - М.: Академия, 2009.

12. Гришина Н.В. Комплексная система защиты информации на предприятии: Учебное пособие. - М.: Форум, 2013.

13. Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.

14. Безопасность глобальных сетевых технологий. - 2-е изд./ В.М. Зима, А.А. Молдовян, Н.А. Молдовян. - СПб.: БХВ-Петербург, 2014. - 368 с.;

б) дополнительная литература:

1. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4 Федеральный закон от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации».

5. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспеченно информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. Утверждено постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

8. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

9. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации 5 декабря 2016 г. № 646.

10. ГОСТ 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

11 ГОСТ 34.602-89 Информационная технология. Комплекс стандартов автоматизированные системы. Техническое задание на создание автоматизированной системы. Госстандарт СССР, 1990.

12. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. Госстандарт СССР, 1990.

13. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения, Ростехрегулирование, 2008.

14. ГОСТ Р 51241-2008 средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Ростехрегулирование, 2008.

15. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

16. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Росстандарт, 2013.

17. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. Росстандарт, 2013.

18. ГОСТ 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

19. ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимости. Росстандарт, 2015.

20. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимости информационных систем. Росстандарт, 2015.

21. Руководящий документ, защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Гостехкомиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114.

22. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15 февраля 2008 г.

23. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

24. Требования к обеспечению зашиты информации в автоматизированных системах управления производственными технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31.

25. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

26. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

27. 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 2011 г. № 21.

28. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119

29. Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом Гостехкомиссии России от 27 октября 1995 г. № 199.

30. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

31. Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55.

32. Положение о банке угроз безопасности информации. Утверждено приказом ФСТЭК России от 16 февраля 2015 г. № 9дсп;

в) базы данных, информационно-справочные и поисковые системы: www.pravo.gov.ru,www.fstec.ru, www.gost.ru/wps/portal/tk362/, www.bdu.fstec.ru; правовые справочно-поисковые системы («Гарант», «Консультант Плюс»).

9.5. Материально-техническое обеспечение

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Специализированный учебный класс	Лекции	Автоматизированное рабочее место (АРМ) преподавателя: ПЭВМ, принтер, LCD-панель (или проектор и экран). Операционная система ОС Windows 7 или выше, Офисные программы, Антивирусные программы.
Специализированный учебный класс	Семинары и практические занятия	Лаборатория безопасности информационных сетей Аппаратно-программный комплекс обнаружения компьютерных атак "Аргус"v1.5; Аппаратно-программный комплекс шифрования (абонентские точки доступа) ПО СКЗИ; Аппаратно-программный комплекс шифрования АПКШ «Континент» 3.5. ЦУС. Платформа I; Беспроводная IP-камера D-Link DCS-2130; Компьютер КламаС Офис; Концентратор доступа по VPN D-Link DSA-3110; Маршрутизатор уровня малого офиса/филиала Cisco 2911R ; Межсетевой экран с поддержкой VPN D-Link DSR-500; Межсетевой экран уровня малого офиса ALTELL NEO 100; Открытая телекоммуникационная стойка для монтажа аппаратуры ЦМО 2242/СТК-42.2; Сетевой коммутатор уровня малого офиса/филиала Cisco WS-C2960G-24TC-L; Коммутатор D-LINK DES-3018 16-port 10/100 BASE-TX Ethernet ports+2 Open Slots L2 Управляемый коммутатор Ethernet 2 уровня D-Link DES-3200-28/C1 Лаборатория технических средств и методов защиты информации Аппаратно-программный комплекс телевизионного наблюдения и регистрации PHOBOS-8; Бинокль ночного видения БНВ-3 "Селена"; Видеокамера ACV-2134DCN/PC день/ночь; Видеокамера ACV-282 CWHA, 6mm; Видеокамера ТСС-3242 P/B3. 7 цв 1/3" SONY SH, 470ТВЛ; Генератор 03020; Генератор шума "Гром ЗИ-4"; Гром ЗИ 4А (состав: шумогенератор и дисконусная антенна SI-5002.1); Диктофон цифровой Sony ICD-UX300B; Имитатор многофункциональный "ИМФ-2"; Индикатор радиоизлучения АПП-7М; КВАДРАТ многоканальный комплекс радиоконтроля; Комплекс средств контроля защищенности от утечки речевой информации по акустическому каналу VNK-90; Металлодетектор Кондор модель 7252; Мультиметр APPA; Осциллограф АСК-2034; Профессиональный нелинейный радиолокатор "NR 900EM"; Пульт микшерный Behringer Xeyx 1202; Система виброакустической защиты "Соната АВ" 1М; Тепловизор Testo 881-1; Сканер HP. Сканер TP2761.

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
		Лаборатория программно-аппаратных средств обеспечения информационной безопасности Средство защиты информации от несанкционированного доступа Secret Net 6.5, сетевой вариант; Межсетевой экран для защиты локальной вычислительной сети от несанкционированного доступа «VipNet Office Firewall»; Средство защиты информации ПО Vip Net Customs (Administrator, Coordinator, Client); Средство защиты информации от несанкционированного доступа Аура 1.2.4; Коммутатор D-LINK DES-3018 16-port 10/100 BASE-TX Ethernet ports+2 Open Slots L2; Электронные ключи для защиты программного обеспечения от незаконного копирования, тиражирования и использования Guardant»; Электронный замок «Соболь» в комплекте с идентификаторами DS-1995; Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа. «АККОРД-NT/2000»; Средство криптографической защиты информации VIP NET Cjjrdinator HB100B; Компьютеры CTR Office Celeron 2533 MHz/18,5" LCD Acer X 193HQGB

9.6. Методические рекомендации по организации учебного курса

Теоретическая часть материала учебного модуля (темы) отрабатывается на лекциях. На лекционных занятиях излагаются наиболее важные и сложные темы, являющиеся фундаментальной основой нормативной базы и практических рекомендаций по аттестации объектов информатизации на соответствие требованиям по безопасности информации. Часть лекций должна излагаться проблемным методом с привлечением обучающихся для решения сформулированной преподавателем задачи.

С целью текущего контроля знаний в ходе занятий необходимо использовать различные приемы тестирования и контроля успеваемости обучающихся.

Семинары проводятся с целью углубления и закрепления знаний на конкретных примерах из практики, обсуждения частных случаев, важных для освоения вопросов учебного модуля (темы), а также привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам ТЗКИ.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия, с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы.

Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала, подготовка к групповым занятиям и семинарам.

Практическая часть учебного модуля (темы) отрабатывается на практических занятиях. На практических занятиях развиваются умения и навыки применения

средств измерений и испытаний для подтверждения соответствия параметров и характеристик средств защиты информации установленным требованиям, разработки программ и методик проведения этих работ.

9.7. Вопросы для контроля знаний слушателей

1. Цели и задачи защиты информации.
2. Объекты информатизации: классификация и характеристика.
3. Основы лицензирования деятельности по ТЗКИ н (или) деятельности по разработке и производству средств защиты информации,
4. Система сертификации средств защиты информации.
5. Порядок разработки, согласования и утверждения планов проведения мероприятий по ТЗКИ.
6. Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций.
7. Классификация ТКУИ.
8. Классификация и характеристики угроз безопасности информации, связанных с НСД.
9. Требования по защите информации, обрабатываемой техническими средствами, от утечки по каналам ПЭМИН.
10. Требования по защите акустической речевой информации.
11. Требования по защите информации от НСД.
12. Стадии и этапы создания системы зашиты информации ограниченного доступа.
13. Способы и средства ТЗКИ от утечки по техническим каналам.
14. Общая характеристика и классификация мер и средств защиты информации от НСД.
15. Основные задачи контроля состояния ТЗКИ.
16. Методы и средства контроля защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.
17. Методы и средства контроля защищенности акустической речевой информации.
18. Методы и средства контроля защищенности информации от НСД.
19. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.
20. Принципы организации защиты персональных данных.
21. Особенности применения технических, программно-аппаратных средств для защиты персональных данных.

Управление ФСТЭК России
по Сибирскому федеральному округу
к Вх.№ 6дсп 2019 г.
Количество листов: 22

Управление ФСТЭК России
по Сибирскому федеральному округу
к Вх.№ 1587дсп 2018 г.
Количество листов: 22

К вх. № 885дсп 18г
ГНИИИ ПТЗИ