ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «АКАДЕМИЯ ЛИДЕРСТВА И АДМИНИСТРИРОВАНИЯ БИЗНЕС-ПРОЦЕССОВ ФНС РОССИИ – ВОЛГА»

Утверждаю

Документ подписан электронной подписью
Беляков Николай Федорович
Ректор
47C188C83B47230A108583F977487307
Срок действия с 15.01.2024 до 09.04.2025
УЦ: Казначейство России
Подписано: 02.04.2024 11:40 (UTC+3)

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
«Комплексная настройка безопасности систем телекоммуникаций»

по повышению квалификации федеральных государственных гражданских служащих

(объем 72 часа)

Рассмотрена
на заседании кафедры ИБ

Протокол № 1 от 29.01.2024

Нижний Новгород – 2024

Оглавление

ВВЕДЕНИЕ

Настоящая программа повышения квалификации «Комплексная настройка безопасности систем телекоммуникаций» разработана с учетом требований:

- Федерального закона от 29 декабря 2012года № 273-ФЗ «Об образовании в Российской Федерации»;
- Постановления Правительства Российской Федерации от 6 мая 2012 года № 399 «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса»;
- Постановления Правительства РФ от 3 ноября 1994 г. № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности" [в ред. постановлений Правительства Российской Федерации от 20.07.2012 № 740, от 20.02.2016 № 123, от 18.03.2016 № 214];
- приказа Министерства науки и высшего образования Российской Федерации от 19 октября 2020 г. № 1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности;
- приказа Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Порядок организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Выбор тем программы и его основного содержания произведен с учетом обеспечения преемственности к государственному образовательному стандарту высшего профессионального образования направлений подготовки «Информационная безопасность» (уровень бакалавриат) - Приказ Минобрнауки России от 17.11.2020 №1427.

Цель реализации программы повышения квалификации

Целью реализации программы повышения квалификации является совершенствование компетенций, необходимых для повышения профессионального уровня в рамках имеющейся квалификации специалистов (включая государственных гражданских служащих), работающих в области защиты информации в информационных системах (ИС) и телекоммуникационных системах (ТКС) (далее – обучающиеся), в части использования способов и средств защиты информации.

Обучающиеся по программе повышения квалификации готовятся к осуществлению следующего вида профессиональной деятельности: эксплуатационная.

Объектами профессиональной деятельности обучающихся являются:

объекты информатизации, включающие автоматизированные (информационные) системы различного уровня и назначения, средства и системы обработки информации и средств их обеспечения;

угрозы безопасности информации в автоматизированных (информационных) системах;

способы и средства защиты информации (ЗИ) в ИС;

система нормативных правовых актов, методических документов и национальных стандартов в области ЗИ.

Задачами профессиональной деятельности обучающихся являются:

а) в эксплуатационной деятельности:

обеспечение ЗИ в ИС и ТКС с использованием отечественного ПО в ходе эксплуатации объектов информатизации;

обеспечение ЗИ в ИС и ТКС с использованием отечественного ПО при выводе из эксплуатации объектов информатизации.

Требования к квалификации поступающего на обучение

Уровень образования лица, поступающего на обучение – высшее образование по направлению подготовки (специальности) в области информационной безопасности, профессиональная переподготовка для выполнения нового вида профессиональной деятельности «Техническая защита информации», или иное высшее образование и стаж работы в области технической защиты информации не менее 1 года.

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 ЗИ и обеспечения безопасности информационных технологий в своей профессиональной деятельности;

способность определять виды и формы информации, подверженной угрозам, возможные методы и пути 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 ЗИ, пользоваться реферативными и справочно-информационными изданиями в области ЗИ;

б) профессиональных:

в эксплуатационной деятельности:

способность обеспечивать ЗИ в ИС и ТКС в ходе эксплуатации объектов информатизации;

способность обеспечивать ЗИ в ИС и ТКС при выводе из эксплуатации объектов информатизации.

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

Перечень знаний, умений и навыков формируется на основе нижеприведенного списка.

Обучающиеся должны:

а) знать:

нормативные правовые акты Российской Федерации, нормативные и методические документы в области защиты информации в ИС;

основы функционирования вычислительных сетей и ТКС;

основные понятия в области ЗИ;

систему организации защиты информации, действующей в органе государственной власти, организации;

основы методологии и методики проведения ТЗИ от НСД в органе государственной власти, организации;

процедуры выявления угроз безопасности информации на объектах информатизации, организации;

общие требования по защите информации в АС (ИС), требования и рекомендации по защите объектов информатизации;

меры и средства защиты информации в АС (ИС);

требования к средствам защиты информации в АС (ИС);

правила разработки, утверждения, обоснования и отмены документов в области ЗИ;

цели, задачи, основные принципы организации, методы и средства ведения контроля состояния защищенности информации в органе государственной власти, организации;

порядок оформления технической документации по защите информации;

б) уметь:

анализировать угрозы безопасности информации;

проводить обоснование выбора современных способов и средств защиты информации, применяемых в АС (ИС);

проводить мероприятия по защите информации в АС (ИС);

устанавливать, применять и настраивать средства защиты информации, применяемые в АС (ИС);

осуществлять проверку выполнения требований нормативных документов по защите информации в АС (ИС);

осуществлять контроль защищённости информации от НСД;

проводить работы по классификации защищенности автоматизированных (информационных) систем от НСД к информации;

применять на практике положения нормативных документов в части ТЗИ от НСД;

в) владеть навыками:

работы с нормативными правовыми актами, методическими документами, национальными и международными стандартами в области ЗИ;

разработки необходимых документов в интересах организации работ по защите информации от НСД;

проведения работ, связанных с защитой информации в АС (ИС);

установки, первичной настройки компонентов средств защиты информации (СЗИ) доверенной загрузки и разграничения доступа;

установки, настройки и администрирования СЗИ в компьютерных сетях;

выявления угроз безопасности информации в автоматизированных (информационных) системах;

участия в разработке организационных и технических мероприятий по защите объектов информатизации от НСД к информации, контроля их выполнения;

проведения работ по контролю защищенности информации от НСД.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
«Комплексная настройка безопасности систем телекоммуникаций»

по повышению квалификации федеральных государственных гражданских служащих Федеральной налоговой службы

Цель:	*Совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, с учетом изменений в законодательстве, нормативных актах и программном обеспечении, используемом в ФНС России, и (или) повышение профессионального уровня в рамках имеющейся квалификации по вопросам защиты информации в системах телекоммуникаций*
Категория, группа должностей:	*старшая, младшая группы должностей, категории: специалисты, обеспечивающие специалисты*
Форма обучения:	*очная путем непосредственного взаимодействия педагогического работника с обучающимся с отрывом от исполнения должностных обязанностей по замещаемой должности государственной гражданской службы*

Продолжительность обучения: *72 часа*

Режим занятий: *6-8 часов в день*

№ п/п	Наименование разделов и дисциплин	Количество часов				Форма промежуточной аттестации
		Всего	по видам занятий			
			лекции	практические занятия		
				аудиторные	самостоятельная работа	
1	Организация работ по технической защите информации в телекоммуникационных системах	20	12	8	0	зачет
2	Защита информации в вычислительных сетях	32	4	28	0	зачет
3	Контроль состояния защиты информации в телекоммуникационных системах	18	2	16	0	зачет
	Итоговая аттестация	2			2	экзамен в форме тестирования
	ИТОГО	**72**	**18**	**52**	**2**	

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Срок обучения по программе повышения квалификации, недели	1							2				
Срок обучения по программе повышения квалификации, дни	1	2	3	4	5	6	7	8	9	10	11	12
Виды занятий, предусмотренные программой повышения квалификации	А	А	А	А	А	К	К	А	А	А	А	АИ

А- аудиторная и самостоятельная работа
И – итоговая аттестация
К – каникулы.

РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН (МОДУЛЕЙ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организация работ по технической защите информации в телекоммуникационных системах

Введение

Рабочая программа дисциплины разработана для программы повышения квалификации «Комплексная настройка безопасности телекоммуникационных систем».

В результате освоения данной дисциплины государственные гражданские служащие инспекций и управлений ФНС России совершенствуют свои знания правовых основ законодательства РФ, позволяющие специалисту по защите информации организовать мероприятия по обеспечению безопасности информации и применять в своей деятельности

по должностным обязанностям отечественное программное обеспечение для защиты информации.

Цели, задачи и место учебной дисциплины в процессе повышения квалификации

Цель учебной дисциплины – совершенствование и (или) получение новых знаний, умений и навыков специалистами по вопросам организационно-правовых основ в области ТЗКИ.

Задачи учебной дисциплины:

Актуализация знаний о целях, задачах технической защиты информации, её основных направлениях, составе и структуре Государственной системы защиты информации.

Совершенствование знаний о видах информации ограниченного доступа по Российскому законодательству. Какими нормативными актами это закреплено?

Совершенствование знаний о функциях и полномочиях государственных регуляторов в сфере защиты информации, о системе противодействия иностранным техническим разведкам.

Закрепление знаний об ответственности за нарушение требований законодательства о защите информации.

Учебная дисциплина является вводной в данную программу повышения квалификации. Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин: «Защита информации в вычислительных сетях», «Контроль состояния защиты информации в телекоммуникационных системах».

Требования к результатам освоения учебной дисциплины.

В результате освоения дисциплины обучающийся должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Обучающийся должен:

знать:

- нормативные правовые акты, методические документы, международные и национальные стандарты в области ЗИ;
- основы функционирования государственной системы ПД ИТР и ТЗИ, цели и задачи ТЗКИ;
- виды конфиденциальной информации, перечни сведений конфиденциального характера;
- правовую ответственность за нарушение требований законодательства о защите информации
- типовую структуру, задачи и полномочия подразделения по ТЗИ;

уметь:

- применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ЗИ;
- владеть навыками:
- работы с действующей нормативной правовой и методической базой в области ЗИ

№ п/п	Наименование тем	Вид занятия
1.	Цели и задачи ТЗКИ. Защищаемые информация и информационные ресурсы. Объекты защиты	лекция
2.	Требования по защите информации и созданию системы защиты информации	лекция
3.	Требования к поведению государственных гражданских служащих	лекция
4.	Организационные и технические меры защиты информации	лекция
5.	Психология профессиональной деятельности при организации защиты информации (тренинг)	практика

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 20 часов (27,8% от всего объема программы).

Реферативное описание тем

Тема №1. Цели и задачи защиты информации. Защищаемые информация и информационные ресурсы. Объекты защиты.

Основные термины и определения в области ТЗИ. Государственная система ПД ИТР и ТЗИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации. Цели и задачи ТЗИ.

Объекты защиты информации. Защищаемые информация и информационные ресурсы. Объекты информатизации, их классификация и характеристика.

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

Понятия, классификация и технологии построения информационных систем. Информационные системы как объекты защиты от НСД. Стандартная модель взаимодействия открытых систем и протоколы межсетевого взаимодействия.

Тема №2. Требования по защите информации и созданию системы защиты информации

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

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

Требования по защите акустической речевой информации. Требования по защите информации от НСД.

Создание и функционирование системы защиты информации ограниченного доступа, как составные части работ по созданию и эксплуатации объектов информатизации. Стадии и этапы создания системы защиты информации ограниченного доступа.

Порядок выполнения работ по защите информации в создаваемой автоматизированной системе в защищённом исполнении (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.

Тема №3. Требования к поведению государственных гражданских служащих

В соответствии со ст.15 Федерального закона от 27.07.2004г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» на государственного гражданского служащего возложена обязанность поддерживать уровень квалификации, необходимый для надлежащего исполнения должностных обязанностей.

В соответствии с Приказом Министерства финансов Российской Федерации от 15 июня 2012г. № 81н Приказом Федеральной налоговой службы от 16 июля 2012г. № ММВ-7-4/500@

утверждены квалификационные требования к профессиональным знаниям и навыкам, необходимым для исполнения должностных обязанностей федеральными государственными гражданскими служащими территориальных органов Федеральной налоговой службы.

Для всех групп должностей государственной гражданской службы установлены в том числе квалификационные требования к профессиональным знаниям правовых основ прохождения федеральной государственной гражданской службы,

На основании указанных нормативных положений в курсы повышения квалификации включены занятия, проводимые с целью обновления и актуализации знаний по вопросам прохождения государственной гражданской службы. Важной составляющей данной части обучения является тема «Требования к поведению государственных гражданских служащих».

Основной задачей, которая решается при изучении указанной темы являться ознакомление слушателей с наиболее важными положениями законодательства о государственной службе по вопросам соблюдения требований к служебному поведению, дисциплинарной ответственности, современными правовыми позициями судебных органов по вопросам обжалования решений государственных органов о привлечении гражданских служащих к дисциплинарной ответственности и мнениями ведущих ученых, экономистов, юристов по актуальным вопросам теории и практики института ответственности в служебных отношениях в органах публичной власти.

Тема №4. Организационные и технические меры защиты информации

Комплекс мероприятий по технической защите информации от утечки по техническим каналам и от несанкционированного доступа к ней. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы.

Особенности реализации мероприятий по защите персональных данных.

Тема №5. Психология профессиональной деятельности при организации защиты информации (тренинг)

В связи с повышением требований к уровню квалификации государственных гражданских служащих и необходимостью освоения современных методов решения профессиональных задач тема «Психология профессиональной деятельности при организации защиты информации (тренинг)» является весьма актуальной и занимает важное место в процессе обновления и закрепления профессиональных знаний государственных гражданских служащих.

По долгу служебной деятельности государственный гражданский служащий налоговых органов тесно и постоянно общается с коллегами, т.е. его деятельность носит коммуникативный характер. От того, насколько эффективным будет это взаимодействие, часто зависит и эффективность выполняемой работы. Умение выстроить взаимоотношения с коллегами является важным профессиональным навыком государственного гражданского служащего. Он должен уметь устанавливать контакт, формировать аттракцию, организовывать взаимодействие, управлять конфликтами.

Целью изучения темы является развитие коммуникативных знаний, умений и навыков, повышение профессиональной компетентности работников налоговой службы.

В рамках заявленной темы должны быть решены следующие задачи:

– рассмотреть закономерности делового общения;
– изучить приемы разрешения конфликтов;
– овладеть технологиями установления контакта и эффективного взаимодействия в коллективе.

Методические рекомендации

Занятия по дисциплине проводятся в форме лекций и практических занятий. При проведении лекций обязательно наличие презентации и использование мультимедийной техники.

При реализации дисциплины в рамках программы повышения квалификации приоритет отдается практической направленности обучения: практические аспекты применения законодательства и нормативных документов РФ; реализация требований нормативных документов при организации защиты информации от НСД на объекте защиты, особенности подготовки локальных актов, регламентирующих использование средств защиты информации, а также, практические аспекты защиты информации с использованием отечественного программного обучения.

Для проведения всех занятий по дисциплине рекомендуется применять современные формы и методы обучения, включая активные и интерактивные.

Для проведения лекционных занятий используются активные методы обучения, стимулирующие познавательную деятельность слушателей, опираясь на методические основы педагогической технологии «Развитие критического мышления».

Технологическую основу составляет базовая модель трех стадий «вызов – реализация смысла (осмысление) – рефлексия (размышление)», которая позволяет помочь слушателям самим определять цели обучения, осуществлять активный поиск информации и размышлять о том, что они узнали. На стадии вызова (evocation) в сознании слушателей происходит процесс актуализации имеющихся знаний и представлений о предмете изучения. Поскольку при этом сочетаются индивидуальная и групповая формы работы, участие слушателей в образовательном процессе активизируется, формируется познавательный интерес. Результатом данных процессов является самостоятельное определение ими цели дальнейшей учебной деятельности.

На стадии осмысления (realization) слушатель вступает в непосредственный контакт с новой информацией – носителем новых идей. Происходит ее систематизация. Стадия рефлексии (reflection) характеризуется тем, что слушатели закрепляют новые знания и активно перестраивают собственные представления с тем, чтобы включить в них новые понятия. Таким образом, происходит “присвоение” нового знания и формирование на его основе своего аргументированного представления об изучаемом объекте.

В ходе работы по такой модели обучающиеся овладевают различными способами интегрирования информации, учатся вырабатывать собственное мнение на основе осмысления различного опыта, идей и представлений, строить умозаключения и логические цепи доказательств, выражать свои мысли четко, понятно для других, уверенно и корректно по отношению к окружающим.

С целью определения качества усвоения материала проводится проверка знаний слушателей с использованием совокупности контрольных заданий и вопросов в виде текущего и итогового контроля.

Текущий контроль осуществляется на лекциях в самых разнообразных формах – опроса слушателей по изученным вопросам, диалога с преподавателем во время лекций, промежуточного тестирования, выполнения слушателями индивидуальных заданий по темам изучаемой дисциплины.

Практические задания

1. Перечислите виды информации ограниченного доступа с указанием НПА, которыми они установлены.
2. Назовите НПА, регламентирующие защиту информации в государственных информационных системах
3. Перечислите подзаконные акты, регулирующие защиту информации в государственных информационных системах
4. Перечислите состав и содержание мер по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах
5. Назовите требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

6. Каковы меры по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах класса К1?

7. Укажите мероприятия обеспечения защиты информации, не составляющей государственную тайну, содержащейся в государственной информационной системе класса К3.

8. Разработайте Перечень конфиденциальной информации, обрабатываемой в ИС при условии наличия служебной тайны и персональных данных 3 уровня защищённости.

9. Правовое регулирование защиты информации в информационных системах ФНС России: перечислите нормативные документы

10. Государственные информационные системы ФНС России: какой класс им присвоен?

11. Назовите информационные ресурсы ФНС России

Список литературы

а) основная литература:

1. Информационная безопасность в таблицах и схемах: учебно-методическое пособие. 7-е изд. Н.Г. Лабутин, О.И. Климченков. – Н. Новгород: «Академия ФНС ЛАБ-Волга», 2024. – 106 с.

2. Карпычев, В. Ю. Техническая защита информации: организационные основы: Учебное пособие / В.Ю. Карпычев. – Н. Новгород: Приволжский ин-т повышения квалификации ФНС, 2021. – 44 с. : ил.

3. Келдыш, Н.В. Системная защита информации компьютерных сетей. Учебное пособие – М.: Мир науки, 2022. – Сетевое издание. Режим доступа: https://izd-mn.com/PDF/43MNNPU22.pdf

4. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. – М.: ФОРУМ, 2016. – 592 с. – (Высшее образование).

б) дополнительная литература, нормативные и методические документы:

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: учеб. Пособие / под ред. Ю.Ф. Каторина – СПб: НИУИТМО, 2012. – 416 с.

1. Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников. – М.: Финансы и статистика, 2003.

2. Нормативно-правовые аспекты защиты информации: Учебное пособие / А.А. Парошин. – Владивосток: Изд-во Дальневост. федер. ун-та, 2010. – 116 с.

3. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ) // Российская газета. –2009. – 21 января. –№ 7.

4. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 9 сентября 2000 г. Пр-1895) – Российская газета. –2000. – 28 сентября. – № 187.

5. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 27.07.2010) «Об информации, информационных технологиях и о защите информации». // Российская газета. –2006. – 29 июля. – № 165.

6. Федеральный закон от 10.04.2011 N 63-ФЗ (ред. от 01.07.2011) «Об электронной подписи». // Собрание законодательства РФ, 11.04.2011, N 15, ст. 2036.

7. Федеральный закон от 27.07.2006 N 152-ФЗ (в ред. 261-ФЗ 261 от 04.06.2011) «О персональных данных». // Российская газета. –2006. – 29 июля. – № 165.

8. Закон от 21.07.1993 N 5485-1 (ред. от 15.11.2010) «О государственной тайне». // Российская газета. –2006. – 29 июля. – № 165.

9. Концепция информационной безопасности Федеральной налоговой службы (утверждена приказом Федеральной налоговой службы от 13 января 2012 г. № ММВ-7-4/6@)

10.Концепция системы управления информационной безопасностью ФНС России (утверждена приказом Федеральной налоговой службы от 25 февраля 2014 г. № ММВ-7-6/66@)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации в вычислительных сетях

Введение

Рабочая программа дисциплины разработана для программы повышения квалификации «Комплексная настройка безопасности телекоммуникационных систем».

В результате освоения данной дисциплины государственные гражданские служащие инспекций и управлений ФНС России совершенствуют свои знания и приобретают практические навыки использования средств защиты информации в ИС и ТКС, позволяющие специалисту по защите информации выполнять мероприятия по обеспечению безопасности информации с использованием средств защиты информации.

Цели, задачи и место учебной дисциплины в процессе повышения квалификации

Цель учебной дисциплины – совершенствование и (или) получение новых знаний, умений и навыков специалистами по вопросам использования программного обеспечения для защиты информации в автоматизированных (информационных) системах (АС (ИС)) и телекоммуникационных системах.

Задачи учебной дисциплины:

Изучение угроз безопасности информации, связанных с НСД, для приобретения (совершенствования) навыков построения модели угроз безопасности информации.

Совершенствование умений и навыков формирования требований по защите информации и создание системы защиты информации от НСД.

Получение практических навыков использования программного обеспечения для защиты информации.

Учебная дисциплина является основной и максимальной по объёму в данной программе повышения квалификации. Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются слушателями при изучении последующей учебной дисциплины «Контроль состояния защиты информации в телекоммуникационных системах» и в своей дальнейшей профессиональной деятельности.

Требования к результатам освоения учебной дисциплины.

В результате изучения данной дисциплины обучающиеся должны:

а) *знать*:

процедуры выявления угроз безопасности информации на объектах информатизации, организации;

общие требования по ТЗИ (по защите информации от НСД), требования и рекомендации по защите объектов информатизации;

меры и средства защиты информации в телекоммуникационных системах;

требования к средствам защиты информации в АС (ИС);

порядок оформления технической документации по защите информации;

б) *уметь*:

анализировать угрозы безопасности информации;

определять требования к средствам защиты информации от НСД;

устанавливать, применять и настраивать средства защиты информации, применяемые в АС (ИС);

применять на практике положения нормативных документов в части защиты информации;

в) владеть навыками:

проведения работ, связанных с защитой информации в телекоммуникационных системах;

установки, первичной настройки компонентов средств защиты информации (СЗИ) доверенной загрузки и разграничения доступа;

установки, настройки и администрирования СЗИ в компьютерных сетях.

области ЗИ.

№п/п	Наименование тем	Вид занятия
1.	Принципы построения вычислительных сетей	лекция
2.	Риск-ориентированный подход при выявлении угроз безопасности информации	практика
3.	Меры и средства защиты информации в вычислительных сетях	практика
4.	Установка, настройка и администрирование средств защиты информации в локальных вычислительных сетях и при межсетевом взаимодействии	практика
5.	Использование средств защиты информации от НСД. Администрирование клиентов СЗИ	практика
6.	Установка, настройка и использование средств криптографической защиты информации и электронной подписи	практика
7.	Использование средств управления защищёнными сетями	практика
8.	Управление инцидентами информационной безопасности в ТНО	практика

Объем занятий по дисциплине – 32 часа (44,4% от всего объема программы).

Реферативное описание тем

Тема № 1. Принципы построения вычислительных сетей

Вычислительные системы и системы передачи информации.

Локальные, глобальные вычислительные сети и системы передачи информации. Модель взаимодействия открытых систем (OSI). Программное обеспечение, поддерживающее работу сети. Оборудование, предназначенное для объединения локальных вычислительных сетей. Технология управления взаимодействием в сети. Обобщенная структура и функции глобальных компьютерных сетей. Технология Ethernet, основные услуги и сервисы сети. Организация и сервис виртуальных частных сетей (VPN).

Классификация вычислительных (компьютерных) сетей. Типы компьютерных сетей по способу управления: одноранговые сети и сети с выделенным сервером, рабочая группа и доменная сеть.

Стек протоколов TCP/IP: состав и назначение протоколов передачи данных. Принципы IP-адресации и маршрутизации в сетях.

Тема №2. Риск-ориентированный подход при выявлении угроз безопасности информации

Понятие и общая классификация угроз безопасности информации. Источники угроз безопасности информации. Модели угроз безопасности информации в информационных и телекоммуникационных системах.

Методы оценки угроз безопасности информации, выявления уязвимостей в автоматизированных (информационных) и телекоммуникационных системах.

Банк данных угроз безопасности информации, содержащий сведения об уязвимостях программного обеспечения, используемого в автоматизированных (информационных) и телекоммуникационных системах.

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

Международный подход к выявлению и анализу уязвимостей информационных систем, базы данных, содержащие описание уязвимостей информационных систем, в том числе CVE. Общая система оценки уязвимостей информационных систем (стандарты CVSS)

Цели и задачи мероприятий по оценке рисков угроз безопасности информации. Основные этапы мероприятий по оценке рисков. Структура сценариев нанесения возможного ущерба.

Методика оценки угроз безопасности информации согласно методического документа ФСТЭК России.

Тема №3. Меры и средства защиты информации в вычислительных сетях

Комплекс мероприятий по ТЗИ от НСД. Общая характеристика и классификация мер и средств защиты информации в телекоммуникационных системах.

Требования к мерам защиты информации, реализуемым в автоматизированной (информационной) и телекоммуникационной системе. Меры защиты информации в телекоммуникационных системах. Особенности создания системы защиты информации как обеспечивающей подсистемы автоматизированной (информационной) системы. Системные и документационные части системы защиты информации.

Тема №4. Установка, настройка и администрирование средств защиты информации в локальных вычислительных сетях и при межсетевом взаимодействии

Установка, настройка, эксплуатация и техническое обслуживание средств защиты информации в локальных вычислительных сетях и при межсетевом взаимодействии. Межсетевые экраны, требования к ним и способы применения.

Системы обнаружения вторжений, требования к ним и способы применения. Средства антивирусной защиты, требования к ним и способы применения.

Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа. Средства регистрации и учета. Средства (механизмы) обеспечения целостности информации.

Тема №5. Использование средств защиты информации от НСД. Администрирование клиентов СЗИ

Средства защиты информации, встроенные в операционные системы (ОС). Система разграничения доступа пользователей к объектам. Назначение разрешений пользователям на доступ к файлам, папкам, дискам, устройствам. Контроль запуска пользователями приложений и процессов.

Программные средства доверенной загрузки и разграничения контроля доступа. Средства регистрации и учета ОС. Средства (механизмы) обеспечения целостности информации ОС. Их настройка и использование.

Тема №6. Установка, настройка и использование средств криптографической защиты информации и электронной подписи

Средства криптографической защиты информации (СКЗИ): понятие, разновидности, назначение и функции по защите информации. Установка, настройка и использование СКЗИ КриптоПро CSP, КриптоАРМ.

Формирование ключевой информации пользователя. Получение и установка личного сертификата, доверенного корневого сертификата и списка отозванных сертификатов. Зашифрование и расшифрование передаваемых по сети документов. Постановка электронной подписи на документ и её проверка.

Использование криптографически защищённой электронной почты.

Тема №7. Использование средств управления защищёнными сетями

Понятие и назначение защищённой сети (виртуальной частной сети, VPN). Структура

защищённой сети и технологии, применяемые в ней.

Проектирование и создание защищённой сети с помощью специализированного программного обеспечения. Задание защищённых сетевых узлов, ролей узлов, связей между ними. Создание пользователей защищённых узлов, связей между ними. Формирование справочной информации защищённой сети. Формирование ключевой информации сетевого узла и пользователя.

Установка, настройка и использование программного обеспечения VipNet.

Тема №8. Управление инцидентами информационной безопасности в ТНО

Управление инцидентами информационной безопасности как важная составляющая системы ИБ.

Основные цели управления инцидентами: локализация и ликвидация последствий инцидентов ИБ; установление виновных лиц и их мотивации, обеспечение возможности привлечения их к ответственности; анализ инцидентов и принятие мер по предотвращению подобных в будущем.

Сбор свидетельств инцидента ИБ — важнейшая часть процесса независимо от того, в каких целях проводится расследование. Все свидетельства собраны, проведен их анализ. На основании результатов анализа нужно, во-первых, установить глубинные причины инцидента для принятия превентивных мер, а во-вторых, попытаться установить лиц, виновных в возникновении инцидента. Выявление нарушителя — задача не всегда выполнимая, особенно при выявлении сложных и удаленных атак, но в случае внутренних нарушений это почти всегда удается. Работа по идентификации виновника проводится в совокупности с обучением приемам установления психологического контакта с сотрудниками.

Развитие навыков эффективного приема, обработки и передачи информации в процессе коммуникации. Развитие навыков аргументации и контраргументации. Овладение эффективными стратегиями клиентоориентированного поведения при взаимодействии.

Методические рекомендации

Занятия по дисциплине проводятся в форме лекций и практических занятий. При проведении лекций обязательно наличие презентации и использование мультимедийной техники.

При реализации дисциплины в рамках программы повышения квалификации приоритет отдается практической направленности обучения: практические аспекты применения законодательства и нормативных документов РФ; реализация требований нормативных документов при организации защиты информации от НСД на объекте защиты, особенности подготовки локальных актов, регламентирующих использование средств защиты информации, а также, практические аспекты защиты информации с использованием отечественного программного обучения.

Для проведения всех занятий по дисциплине рекомендуется применять современные формы и методы обучения, включая активные и интерактивные.

Для проведения лекционных занятий используются активные методы обучения, стимулирующие познавательную деятельность слушателей, опираясь на методические основы педагогической технологии «Развитие критического мышления».

Технологическую основу составляет базовая модель трех стадий «вызов – реализация смысла (осмысление) – рефлексия (размышление)», которая позволяет помочь слушателям самим определять цели обучения, осуществлять активный поиск информации и размышлять о том, что они узнали. На стадии вызова (evocation) в сознании слушателей происходит процесс актуализации имеющихся знаний и представлений о предмете изучения. Поскольку при этом сочетаются индивидуальная и групповая формы работы, участие слушателей в образовательном процессе активизируется, формируется познавательный интерес. Результатом данных процессов является самостоятельное определение ими цели дальнейшей учебной деятельности.

На стадии осмысления (realization) слушатель вступает в непосредственный контакт с новой информацией – носителем новых идей. Происходит ее систематизация. Стадия рефлексии (reflection) характеризуется тем, что слушатели закрепляют новые знания и активно перестраивают собственные представления с тем, чтобы включить в них новые понятия. Таким образом, происходит “присвоение” нового знания и формирование на его основе своего аргументированного представления об изучаемом объекте.

В ходе работы по такой модели обучающиеся овладевают различными способами интегрирования информации, учатся вырабатывать собственное мнение на основе осмысления различного опыта, идей и представлений, строить умозаключения и логические цепи доказательств, выражать свои мысли четко, понятно для других, уверенно и корректно по отношению к окружающим.

При проведении занятий обязательно учитывается распределение времени на лекционный материал и выполнение практических занятий в соответствии с утвержденным учебно-тематическим планом.

Продолжительность аудиторных занятий – 2-4 аудиторных часа.

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий. Часть лекций может излагаться проблемным методом с привлечением слушателей для решения сформулированных преподавателем проблем.

Каждая лекция должна:

– иметь четкую структуру и логику раскрытия последовательно излагаемых вопросов (понятийная линия лекции);

– иметь твердый теоретический и методический стержень, важную проблему;

– иметь законченный характер освещения определенной темы (проблемы), тесную связь с предыдущим материалом;

– быть доказательной и аргументированной, содержать достаточное количество ярких и убедительных примеров, фактов, обоснований, иметь четко выраженную связь с практикой;

– быть проблемной, раскрывать противоречия и указывать пути их решения, ставить перед обучающимися вопросы для размышления;

– обладать силой логической аргументации и вызывать у слушателей необходимый интерес, давать направление для самостоятельной работы;

– находиться на современном уровне развития науки и техники, содержать прогноз их развития на ближайшие годы;

– отражать методическую обработку материала (выделение главных мыслей и положений, подчеркивание выводов, повторение их в различных формулировках);

– быть наглядной, сочетаться по возможности с демонстрацией аудиовизуальных материалов, макетов, моделей и образцов;

– излагаться четким и ясным языком, содержать разъяснение всех вновь вводимых терминов и понятий;

– быть доступной для восприятия данной аудиторией.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. При проведении практических занятий необходимо отрабатывать задания, учитывающие специфику выполняемых функциональных обязанностей слушателями курсов по своему профессиональному предназначению, в том числе предусматривать задания с проведением деловых игр (эпизодов) и созданием моделей типовых ситуаций.

Для проведения практических занятий должны использоваться методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями информационных систем, и набором конкретных действий, существенных для определённых категорий обучаемых, объединённых в соответствующую подгруппу.

Важнейшим элементом практического занятия является учебная задача (проблема), предлагаемая для решения. Преподаватель подбирает примеры (задачи и логические задания)

для практического занятия, представляет дидактическую цель: привитие каких навыков и умений применительно к каждой задаче установить, каких усилий от обучающихся она потребует, в чем должно проявиться творчество слушателей при решении данной задачи.

При планировании практического занятия и разработке индивидуальных заданий преподавателю важно учитывать подготовку и интересы каждого слушателя.

Рекомендуется сначала давать легкие задачи (логические задания), которые рассчитаны на репродуктивную деятельность, требующую простого воспроизведения способов действия, данных на лекции для осмысления и закрепления в памяти. Такие задачи помогают контролировать правильность понимания обучающимися отдельных вопросов изученного материала небольшого объема (как правило, в пределах одной лекции). В этом случае преобладает решение задач по образцу, предложенному на лекции.

Затем содержание учебных задач усложняется. Предлагаются задачи, рассчитанные на репродуктивно-преобразовательную деятельность, при которой обучающемуся нужно не только воспроизвести известный ему способ действий, но и дать анализ его целесообразности, высказать свои соображения, относящиеся к анализу условий задачи, выдвигаемых гипотез, полученных результатов. Этот тип задач по отдельным вопросам темы должен развивать умения и навыки применения изученных методов и контролировать их наличие у обучающихся.

В дальнейшем содержание задач (логических заданий) снова усложняется с таким расчетом, чтобы их решение требовало в начале отдельных элементов продуктивной деятельности, а затем – полностью продуктивной (творческой). Как правило, такие задачи в целом носят комплексный характер и предназначены для контроля глубины изучения материала темы или курса.

Выстраивая систему задач постепенно возрастающей сложности, преподаватель добивается усвоения слушателями наиболее важных методов и приемов, характерных для данной учебной дисциплины.

С целью определения качества усвоения материала проводится проверка знаний слушателей с использованием совокупности контрольных заданий и вопросов в виде текущего и итогового контроля.

Текущий контроль осуществляется на занятиях в самых разнообразных формах – опроса слушателей по изученным вопросам, диалога с преподавателем во время лекций, промежуточного тестирования, выполнения слушателями индивидуальных заданий по темам изучаемой дисциплины.

Практические задания

1. Выполните рекомендуемые правила безопасного использования учётных записей: сначала переименуйте встроенную учётную запись Администратор в Sysadmin, затем добавьте учётную запись Админ, введите её в группу Администраторы. Отключите учётную запись Sysadmin для безопасной работы с системой.
2. Назначьте и проверьте права пользователей системы для доступа к папке на сервере.
3. Назначьте и проверьте права для удалённого доступа пользователей к папке на сетевом ресурсе.
4. Разграничить полномочия пользователей на запуск разных сетевых приложений.
5. Настройте первоначальные параметры безопасности: отключение потенциально опасных служб, использование локальных параметров безопасности.
6. С помощью вкладки «Доступ» в свойствах папки на сервере настройте Общий доступ для учётных записей с рабочей станции.
7. Настройте сетевые подключения в виртуальной машине SRV: 1-е соединение – 10.0.1.100, 2-е соединение – 10.0.2.100.
8. Настройте Службу маршрутизации и удалённого доступа, используя входящие и исходящие фильтры на запрет пропуска пакетов по протоколам ftp, http, smtp, pop3.Проверьте действие фильтров.

9. Настройте в Службе маршрутизации и удалённого доступа преобразователь сетевых адресов (NAT).

10. Запретите пользователю user1 на рабочей станции выполнение некоторых приложений, например, программ IE и Paint.

11. Установите и настройте межсетевой экран и криптошлюз VipNetCoordinator.

12. Настройте транзитные фильтры VipNetCoordinator на запрет пакетов по протоколам ftp, http. Проверьте действие фильтров.

13. Настройте локальные фильтры VipNetCoordinator на запрет пакетов по протоколам ftp, http. Проверьте действие фильтров.

14. Установите СКЗИ КриптоПроCSP и КриптоАРМ на виртуальную машину с ОС AstraLinux.

15. С помощью КриптоАРМ сформируйте запрос на сертификат к удостоверяющему центру КриптоПро, развёрнутому в виртуальной сети по адресу 10.0.1.250. Получите от него сертификат своего открытого ключа, сертификат корневого удостоверяющего центра, список отозванных сертификатов (CRL); установите их в КриптопроCSP на своей рабочей станции.

16. Создайте документ произвольного содержания. С помощью программы КриптоАРМ подпишите этот документ своим сертификатом (закрытым ключом), сохраните его в виде файла.

17. Скопируйте из папки Ключи подписанный соседом документ, проверьте с помощью КриптоАРМ подпись на полученном документе и извлеките из полученного от соседа подписанного файла исходный документ.

18. Обменяйтесь с соседом сертификатами открытого ключа. Для этого сначала скопируйте свой сертификат ключа в папку Ключи, находящуюся в папке Общая на 10.0.1.253, затем скопируйте оттуда и установите сертификат соседа на свой компьютер.

19. Создайте документ произвольного содержания. С помощью программы КриптоАРМ зашифруйте его сертификатом Вашего соседа. Зашифрованный файл отправьте в сетевую папку Ключи в папке Общая на 10.0.1.253.

Список литературы

а) основная литература:

1. Информационная безопасность в таблицах и схемах: учебно-методическое пособие. 7-е изд. Н.Г. Лабутин, О.И. Климченков. – Н. Новгород: Приволжский ин-т повышения квалификации ФНС, 2024. – 106 с.

2. Безопасность операционной системы Astra Linux Special Edition. Учеб. пособие для вузов. – Екатеринбург: QPSoft, 2019.

3. Безопасность операционной системы специального назначения Astra Linux Special Edition. Буренин П. В., Девянин П. Н., Лебеденко Е. В., Проскурин В. Г., Цибуля А. Н. – М.: Горячая Линия – Телеком, 2019.

4. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. - 3-е изд., перераб. и доп. — М.: Издательство Юрайт, 2024. - 161 с.

5. Келдыш, Н.В. Системная защита информации компьютерных сетей. Учебное пособие – М.: Мир науки, 2022. – Сетевое издание. Режим доступа: https://izd-mn.com/PDF/43MNNPU22.pdf

б) дополнительная литература, нормативные и методические документы:

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: учеб. Пособие / под ред. Ю.Ф. Каторина – СПб: НИУИТМО, 2012. – 416 с.

2. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях: учебное пособие / В. Ф. Шаньгин. - Москва: ДМК Пресс, 2012. – 592 с.

3. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. Курс лекций. Учебное пособие. – М.: Интернет-университет информационных технологий, 2005.

4. Малюк А.А., Пазизин СВ., Погожий Н.С. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов.М.: Горячая линия Телеком, 2004.

5. Мещеряков Р.В., Шелупанов А.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Монография. – Томск: Изд-во В-Спектр, 2007.

6. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений: Учебное пособие. М: ЮНИТИДАНА, 2001.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Контроль состояния ТЗИ от НСД

Введение

Рабочая программа дисциплины разработана для программы повышения квалификации «Комплексная настройка безопасности телекоммуникационных систем».

В результате освоения данной дисциплины государственные гражданские служащие инспекций и управлений ФНС России совершенствуют свои знания и приобретают практические навыки проведения мероприятий по контролю и мониторингу состояния защищённости информации на объектах информатизации, позволяющие специалисту по защите информации выполнять свои должностные обязанности по обеспечению безопасности информации.

Цель, задачи и место учебной дисциплины в процессе повышения квалификации

Рабочая программа дисциплины разработана для программы повышения квалификации «Комплексная настройка безопасности телекоммуникационных систем».

Цель учебной дисциплины - совершенствование и (или) получение новых знаний, умений и навыков специалистами по вопросам контроля состояния технической защиты информации в телекоммуникационных системах.

Задачи:

Изучение методов контроля состояния защиты информации, связанных с ними способов контроля и мониторинга.

Совершенствование умений и навыков формирования организационно-распорядительных документов локального уровня, необходимых для обеспечения систематизированной защиты информации.

Получение практических навыков использования средств и методик контроля и мониторинга защиты информации в телекоммуникационных системах.

Место учебной дисциплины в структуре программы повышения квалификации.

Учебная дисциплина входит в программу повышения квалификации и при ее изучении используются знания, умения и навыки, сформированные в ходе освоения учебных дисциплин: «Правовые и организационные основы защиты информации» и «Способы и средства защиты информации с использованием отечественного программного обеспечения».

Данная учебная дисциплина является итоговой учебной дисциплиной программы повышения квалификации.

Требования к результатам освоения учебной дисциплины

Процесс освоения учебной дисциплины направлен на получение (формирование) обучающимися таких компетенций, как:

а) общепрофессиональных:

способность использовать нормативные правовые акты, методические документы, национальные и международные стандарты в области ЗИ и обеспечения безопасности информационных технологий в своей профессиональной деятельности;

способность определять виды и формы информации, подверженной угрозам, возможные методы и пути 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 ЗИ, пользоваться реферативными и справочно-информационными изданиями в области ЗИ;

б) профессиональных:

в эксплуатационной деятельности:

способность обеспечивать контроль состояния ЗИ в ИС и в телекоммуникационных системах в ходе эксплуатации объектов информатизации;

способность обеспечивать контроль состояния ЗИ в ИС и в телекоммуникационных системах при выводе из эксплуатации объектов информатизации.

В результате освоения программы повышения квалификации обучающиеся должны получить знания, умения и навыки, которые позволят совершенствовать и (или) получить новые компетенции, необходимые им для осуществления своей профессиональной деятельности.

Освоившие программу должны:

а) знать:

нормативные правовые акты Российской Федерации, национальные стандарты, нормативные и методические документы в области технической защиты информации и контроля состояния защиты информации на защищаемом объекте;

правила разработки, утверждения, обоснования и отмены документов в области контроля ТЗИ в телекоммуникационных системах;

цели, задачи, основные принципы организации, методы и средства ведения контроля состояния защищенности информации в органе государственной власти, организации;

порядок оформления технической документации по защите информации.

б) уметь:

осуществлять проверку выполнения требований нормативных документов по защите информации в телекоммуникационных системах;

осуществлять контроль защищённости информации в телекоммуникационных системах;

проводить работы по классификации защищенности автоматизированных (информационных) систем от НСД к информации;

применять на практике положения нормативных документов в части контроля состояния ТЗИ в телекоммуникационных системах;

в) владеть навыками:

проведения работ по контролю защищенности информации от НСД;

проведения работ, связанных с контролем защищённости информации в телекоммуникационных системах;

установки, первичной настройки компонентов средств защиты информации (СЗИ) доверенной загрузки и разграничения доступа;

установки, настройки и администрирования СЗИ в компьютерных сетях.

№п/п	**Наименование тем**	**Вид занятия**
1.	*Интегрированное занятие.* Основные задачи контроля состояния ТЗИ от НСД	практика
2.	Методы и средства контроля защищённости информации от НСД	практика
3.	Аттестация объектов информатизации по требованиям безопасности информации	практика

4.	Сертификация средств защиты информации от НСД	лекция, практика
5.	Внутренний аудит и мониторинг информационной безопасности ТНО	практика
6.	*Интегрированное занятие.* Основные задачи контроля состояния ТЗИ от НСД	практика
7.	Использование средств управления защищёнными сетями	практика
8.	Управление инцидентами информационной безопасности в ТНО	практика

Объем занятий по дисциплине – 18 часов (25% от всего объема программы).

Реферативное описание тем

Тема №1. Основные задачи контроля состояния ТЗИ от НСД

Основные задачи контроля состояния ТЗКИ. Классификация видов контроля состояния ТЗКИ.

Система документов по контролю состояния ТЗКИ. Вопросы, подлежащие проверке при контроле состояния ТЗКИ.

Организационный и технический контроль состояния ТЗКИ

Тема № 2. Методы и средства контроля защищённости информации от НСД

Необходимость проведения контроля защищённости информационных. Органы, имеющие право проведения контроля защищённости информации в информационной системе.

Классификация методов контроля защищенности информации от НСД и их характеристика. Сканеры безопасности и их характеристика. Средства анализа программных кодов и их характеристика. Средства антивирусной защиты и их характеристика.

Установка и настройка сканеров безопасности.

Тема №3. Аттестация объектов информатизации по требованиям безопасности информации

Цели и виды аттестации объектов информатизации на соответствие требованиям безопасности информации.

Участники аттестации и их полномочия (компетенции).

Задачи, функции, права и обязанности органов по аттестации.

Требования к органам по аттестации объектов информатизации.

Деятельность аттестационных комиссий.

Сводный реестр сертифицированной продукции, используемой в целях защиты информации на аттестованных объектах информатизации.

Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации

Тема №4. Сертификация средств защиты информации от НСД

Порядок сертификации продукции, используемой в целях защиты конфиденциальной информации: технических средств защиты информации, защищённых технических средств обработки информации, технических средств контроля защищённости информации, программных, программно-технических средств защиты информации, программных средств контроля защищённости информации.

Система сертификации средств защиты информации.

Тема №5. Внутренний аудит и мониторинг информационной безопасности ТНО

Понятие внутреннего аудита безопасности информации. Порядок организации и проведения аудита безопасности информации в ТНО.

Классификация видов контроля состояния защищённости информации. Система документов по контролю состояния ТЗИ от НСД.

Вопросы, подлежащие проверке при контроле состояния защищённости информации

в организации. Организационный и технический контроль состояния ТЗИ.

Проведение мониторинга защищённости средств и систем телекоммуникаций.

Методические рекомендации

Занятия по дисциплине проводятся в форме лекций и практических занятий. При проведении лекций обязательно наличие презентации и использование мультимедийной техники.

При реализации дисциплины в рамках программы повышения квалификации приоритет отдается практической направленности обучения: практические аспекты применения законодательства и нормативных документов РФ; реализация требований нормативных документов при организации защиты информации от НСД на объекте защиты, особенности подготовки локальных актов, регламентирующих использование средств защиты информации, а также, практические аспекты защиты информации с использованием отечественного программного обучения.

Для проведения всех занятий по дисциплине рекомендуется применять современные формы и методы обучения, включая активные и интерактивные.

Для проведения лекционных занятий используются активные методы обучения, стимулирующие познавательную деятельность слушателей, опираясь на методические основы педагогической технологии «Развитие критического мышления».

Технологическую основу составляет базовая модель трех стадий «вызов – реализация смысла (осмысление) – рефлексия (размышление)», которая позволяет помочь слушателям самим определять цели обучения, осуществлять активный поиск информации и размышлять о том, что они узнали. На стадии вызова (evocation) в сознании слушателей происходит процесс актуализации имеющихся знаний и представлений о предмете изучения. Поскольку при этом сочетаются индивидуальная и групповая формы работы, участие слушателей в образовательном процессе активизируется, формируется познавательный интерес. Результатом данных процессов является самостоятельное определение ими цели дальнейшей учебной деятельности.

На стадии осмысления (realization) слушатель вступает в непосредственный контакт с новой информацией – носителем новых идей. Происходит ее систематизация. Стадия рефлексии (reflection) характеризуется тем, что слушатели закрепляют новые знания и активно перестраивают собственные представления с тем, чтобы включить в них новые понятия. Таким образом, происходит “присвоение” нового знания и формирование на его основе своего аргументированного представления об изучаемом объекте.

В ходе работы по такой модели обучающиеся овладевают различными способами интегрирования информации, учатся вырабатывать собственное мнение на основе осмысления различного опыта, идей и представлений, строить умозаключения и логические цепи доказательств, выражать свои мысли четко, понятно для других, уверенно и корректно по отношению к окружающим.

При проведении занятий обязательно учитывается распределение времени на лекционный материал и выполнение практических занятий в соответствии с утвержденным учебно-тематическим планом.

Продолжительность аудиторных занятий – 2-4 аудиторных часа.

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий. Часть лекций может излагаться проблемным методом с привлечением слушателей для решения сформулированных преподавателем проблем.

Каждая лекция должна:

– иметь четкую структуру и логику раскрытия последовательно излагаемых вопросов (понятийная линия лекции);

– иметь твердый теоретический и методический стержень, важную проблему;

– иметь законченный характер освещения определенной темы (проблемы), тесную связь с предыдущим материалом;

– быть доказательной и аргументированной, содержать достаточное количество ярких и убедительных примеров, фактов, обоснований, иметь четко выраженную связь с практикой;

– быть проблемной, раскрывать противоречия и указывать пути их решения, ставить перед обучающимися вопросы для размышления;

– обладать силой логической аргументации и вызывать у слушателей необходимый интерес, давать направление для самостоятельной работы;

– находиться на современном уровне развития науки и техники, содержать прогноз их развития на ближайшие годы;

– отражать методическую обработку материала (выделение главных мыслей и положений, подчеркивание выводов, повторение их в различных формулировках);

– быть наглядной, сочетаться по возможности с демонстрацией аудиовизуальных материалов, макетов, моделей и образцов;

– излагаться четким и ясным языком, содержать разъяснение всех вновь вводимых терминов и понятий;

– быть доступной для восприятия данной аудиторией.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. При проведении практических занятий необходимо отрабатывать задания, учитывающие специфику выполняемых функциональных обязанностей слушателями курсов по своему профессиональному предназначению, в том числе предусматривать задания с проведением деловых игр (эпизодов) и созданием моделей типовых ситуаций.

Для проведения практических занятий должны использоваться методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями информационных систем, и набором конкретных действий, существенных для определённых категорий обучаемых, объединённых в соответствующую подгруппу.

Важнейшим элементом практического занятия является учебная задача (проблема), предлагаемая для решения. Преподаватель подбирает примеры (задачи и логические задания) для практического занятия, представляет дидактическую цель: привитие каких навыков и умений применительно к каждой задаче установить, каких усилий от обучающихся она потребует, в чем должно проявиться творчество слушателей при решении данной задачи.

При планировании практического занятия и разработке индивидуальных заданий преподавателю важно учитывать подготовку и интересы каждого слушателя.

Рекомендуется сначала давать легкие задачи (логические задания), которые рассчитаны на репродуктивную деятельность, требующую простого воспроизведения способов действия, данных на лекции для осмысления и закрепления в памяти. Такие задачи помогают контролировать правильность понимания обучающимися отдельных вопросов изученного материала небольшого объема (как правило, в пределах одной лекции). В этом случае преобладает решение задач по образцу, предложенному на лекции.

Затем содержание учебных задач усложняется. Предлагаются задачи, рассчитанные на репродуктивно-преобразовательную деятельность, при которой обучающемуся нужно не только воспроизвести известный ему способ действий, но и дать анализ его целесообразности, высказать свои соображения, относящиеся к анализу условий задачи, выдвигаемых гипотез, полученных результатов. Этот тип задач по отдельным вопросам темы должен развивать умения и навыки применения изученных методов и контролировать их наличие у обучающихся.

В дальнейшем содержание задач (логических заданий) снова усложняется с таким расчетом, чтобы их решение требовало в начале отдельных элементов продуктивной деятельности, а затем – полностью продуктивной (творческой). Как правило, такие задачи в целом носят комплексный характер и предназначены для контроля глубины изучения материала темы или курса.

Выстраивая систему задач постепенно возрастающей сложности, преподаватель добивается усвоения слушателями наиболее важных методов и приемов, характерных для данной учебной дисциплины.

С целью определения качества усвоения материала проводится проверка знаний слушателей с использованием совокупности контрольных заданий и вопросов в виде текущего и итогового контроля.

Текущий контроль осуществляется на занятиях в самых разнообразных формах – опроса слушателей по изученным вопросам, диалога с преподавателем во время лекций, промежуточного тестирования, выполнения слушателями индивидуальных заданий по темам изучаемой дисциплины.

Практические задания

1. Сформируйте перечень направлений проверки при контроле состояния ТЗИ от НСД в организациях.
2. Обоснуйте необходимость и правила практического применения антивирусных средств при проведении контроля защищенности информации.
3. Используя методики аттестационных испытаний составьте план аттестационных испытаний для многопользовательской автоматизированной системы и для государственной информационной системы 1 класса защищённости.
4. Подготовьте заключения по результатам аттестации объектов информатизации по требованиям безопасности информации.
5. Составьте перечень работ, выполняемых при осуществлении сертификационных испытаний на соответствие требованиям по безопасности информации продукции, используемой для защиты конфиденциальной информации.
6. Подготовьте все необходимые документы для организации и проведения аттестации объектов информатизации на соответствие требованиям безопасности информации.
7. Настройте средство контроля состояния защищённости информации от НСД на регулярный мониторинг.

Список литературы

а) основная литература:

1. Вострецова, Е. В. Основы информационной безопасности: учебное пособие для студентов вузов / Е. В. Вострецова. — Екатеринбург: Изд-во Урал. ун-та, 2019. — 204 с.
2. Информационная безопасность в таблицах и схемах: учебно-методическое пособие. Изд-е 7-е. Н.Г. Лабутин, О.И. Климченков. - Н. Новгород: Приволжский ин-т повышения квалификации ФНС, 2024. - 100 с.
3. Карпычев, В. Ю. Техническая защита информации: организационные основы: Учебное пособие / В.Ю. Карпычев. - Н. Новгород: Приволжский ин-т повышения квалификации ФНС, 2021. - 44 с. : ил.
4. Келдыш, Н.В. Системная защита информации компьютерных сетей. Учебное пособие – М.: Мир науки, 2022. – Сетевое издание. Режим доступа: https://izd-mn.com/PDF/43MNNPU22.pdf
5. Язов, Ю.К., Соловьёв С.В. Организация защиты информации в информационных системах от несанкционированного доступа. Монография. - Воронеж: Кварта, 2022. - 588 с.

б) дополнительная литература:

1. Курило А.П., Зефиров С.Л., Голованов В.Б. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006.
2. Курило А.П., Милославская Н.Г., Сенатров М.Ю., Толстой А.И. Вопросы управления информационной безопасностью. Книга 15. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2012.

3. Лапонина, О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. Курс лекций. Учебное пособие. – М.: Интернет-университет информационных технологий, 2005.

4. Малюк А.А., Пазизин СВ., Погожий Н.С. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. М.: Горячая линия Телеком, 2004.

5. Мещеряков Р.В., Шелупанов А.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Монография. – Томск: Изд-во В-Спектр, 2007.

6. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. - Ростов-на-Дону: Издательство СКНЦ ВШ, 2006.

в) нормативно-правовые акты, ГОСТы, руководящие и методические документы:

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

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

9. Федеральный закон от 27 июля 2006г. № 152-ФЗ «О персональных данных».

10. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».

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

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

13. Постановление Правительства Российской Федерации от 15 сентября 1993 г. № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам».

14. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

15. Постановление Правительства Российской Федерации от 18 сентября 2012 г. № 940 «Об утверждении правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю».

16. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

17. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии».

18. Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

19. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

20. Постановление Правительства Российской Федерации от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

21. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

22. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

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

24. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

25. ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

26. ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

27. ГОСТ Р 54581-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 1. Обзор и основы.

28. ГОСТ Р 54582-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия.

29. ГОСТ Р 54583-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия.

30. ГОСТ Р ИСО 74981-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.

31. ГОСТ Р ИСО 74982-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

32. ГОСТ Р ИСО/МЭК 133351-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

33. ГОСТ Р ИСО/МЭК 15446-2008 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.

34. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005).

35. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод правил и норм менеджмента информационной безопасности.

36. ГОСТ Р ИСО/МЭК 270331-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.

37. ГОСТ Р ИСО/МЭК 270331-2011 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности.

Безопасность сетей. Часть 1. Обзор и концепции (утвержден и введен в действие Приказом Росстандарта от 01 декабря 2011 г. № 683ст).

38. ГОСТ Р ИСО/МЭК ТО 18044-2008 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

39. ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения.

40. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний.

41. МД Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.).

42. Методика оценки угроз безопасности информации. (утверждена заместителем директора ФСТЭК России 5 февраля 2021 г.).

43. Методический документ. Меры защиты информации в государственных информационных системах (утвержден ФСТЭК России 11 февраля 2014 г.).

44. Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от февраля 2012 г. № 79 (утвержден ФСТЭК России 04апреля 2015 г.).

45. Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения видов работ, установленных Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171 (утвержден ФСТЭК России 09 апреля 2012 г.).

46. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утв. приказом ФСТЭК России от 29 апреля 2021 г. N 77.

47. Приказ Росмкомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

48. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 (ред. от 15.02.2017) «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

49. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

50. Приказ ФСТЭК России от 27 сентября 2013 г. № 119 «Об утверждении требований к средствам доверенной загрузки».

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

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

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Повышение квалификации гражданских служащих осуществляется в очной форме путем непосредственного общения слушателя с преподавателем. В содержании обучения приоритет отдается практической направленности обучения.

При проведении занятий обязательно учитывается распределение времени на лекционный материал и выполнение практических заданий в соответствии с утвержденным учебно-тематическим планом. При этом общее время на лекционный материал не превышает 30%. Практические задания предполагают разбор спорных и проблемных ситуаций из практической работы, подготовку распорядительно-организационных документов, решение практических вопросов из профессиональной деятельности обучающимися.

При выполнении лабораторных работ обучающиеся самостоятельно выполняют практические задания по установке и настройке программных средств защиты информации.

Основными видами самостоятельной работы обучающихся без участия преподавателей являются:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– подготовка к групповым занятиям по определенной теме дисциплины.

Каждый обучающийся на весь период обучения обеспечен индивидуальным неограниченным доступом к электронным учебным материалам, содержащим всю необходимую учебную и учебно-методическую информацию по изучаемым модулям. На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных правовых актов и практических действий. Часть лекций может излагаться проблемным методом с привлечением обучающихся для решения сформулированных преподавателем проблем.

На практические занятия и лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. При проведении практических занятий отрабатываются задания, учитывающие специфику выполняемых функциональных обязанностей обучающихся по своему профессиональному предназначению, в том числе предусмотрены задания с проведением деловых игр (эпизодов) и созданием ситуаций, моделирующих типовые нарушения. В процессе практического обучения особое внимание уделяется формированию и развитию у обучающихся практических умений, навыков и компетенций.

Для проведения практических занятий используются методические разработки, позволяющие индивидуализировать задания обучающимся в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями объектов информатизации, и набором конкретных действий, существенных для определённых категорий обучающихся, объединённых в соответствующую подгруппу.

В ходе самостоятельной работы обучающиеся более детально рассматривают вопросы, изучаемые в ходе лекционных занятий, готовятся к проведению групповых занятий и закрепляют умения и навыки, полученные при отработке на практических занятиях. В целях более эффективной работы обучающиеся, готовятся учебные и контрольно-проверочные материалы.

В ходе самостоятельной работы обучающимся предоставляется возможность пользования интернет ресурсами учебного заведения, на которых размещены электронные учебники, пробные тесты, а также форум для получения консультационных услуг от ведущих преподавателей.

Лабораторная база Академии оснащена современным оборудованием и средствами вычислительной техники, позволяющими реализовать среду виртуализации, в которой может быть выполнено большинство практических занятий и лабораторных работ, для получения умений и навыков установки, настройки и использования программных и программно-

технических средств защиты информации.

Компьютерные классы оборудованы автоматизированными рабочими местами для проведения занятий по учебным дисциплинам из расчёта одно рабочее место на одного обучающегося при проведении занятий в данных классах. Академия имеет необходимый комплект лицензионного программного обеспечения и сертифицированных программных средств по защите информации.

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

Реализация программы обеспечивается как штатными преподавателями специализированных кафедр Академии, так и руководящими и научно-педагогическими работниками организаций и ведущих ВУЗов, а также высококвалифицированными специалистами в области информационной безопасности Управления Федеральной службы по техническому и экспортному контролю по Приволжскому федеральному округу, привлекаемыми к реализации программы на условиях гражданско-правового договора (контракта).

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

На лекционных занятиях излагаются теоретические основы обеспечения безопасности информации. На лекциях, путем постановки проблемных вопросов, совместным их обсуждением и рассмотрением наиболее целесообразных путей решения, у обучающихся углубляются и закрепляются знания, полученные ими в процессе самостоятельной работы над учебным материалом. Лекции и практические занятия проводятся в аудиториях, оснащенных компьютером, мультимедийным проектором, экраном и доской.

На практические занятия и лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. При проведении практических занятий отрабатываются задания, учитывающие специфику выполнения функциональных обязанностей обучающимися по своему профессиональному предназначению, в том числе задания с использованием специализированного программного обеспечения компьютера для защиты информации.

Для проведения практических занятий и лабораторных работ используются аудитории, оснащенные необходимым информационно-техническим оборудованием и программными средствами, позволяющими моделировать изучаемые процессы персонально каждым обучающимся.

В процессе изучения учебной программы используются действующие национальные стандарты, нормативные правовые акты и иные документы в области ТЗИ, нормативные, руководящие и методические документы ФСТЭК России, а также соответствующие учебно-методические пособия и презентации.

Для обеспечения учебной, учебно-методической, научной, справочной литературой, доступа к современным профессиональным базам данных, справочно-правовым системам и к глобальной сети Интернет, имеется библиотека. Каждому обучающемуся обеспечивается доступ к библиотечному фонду, укомплектованному печатными и электронными изданиями основной учебной литературы, изданными за последние 10 лет, из расчёта не менее одного экземпляра на 4-5 обучающихся.

Передача программы повышения квалификации другой образовательной организации допускается при создании условий и соблюдения требований законодательства Российской

Федерации о порядке обращения со служебной информацией ограниченного распространения и наличии разрешения федеральных органов государственной власти, в ведении которых находится организации, осуществляющие образовательную деятельность.

Внесение изменений в программу 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.

Программа может реализовываться в очно-заочной форме, при этом в части применения электронного обучения и дистанционных образовательных технологий исключается изучение вопросов, связанных с изучением документов, содержащих служебную информацию ограниченного распространения.

ФОРМЫ АТТЕСТАЦИИ

Оценка качества освоения программы включает входной, текущий или промежуточный контроли, а также итоговую аттестацию обучающихся.

Входной контроль должен охватывать всех обучающихся и проводится в форме тестирования и последующего собеседования с ведущими преподавателями учебного заведения. Целью является определение уровня знаний обучающихся для корректировки и адаптации учебного процесса под конкретные потребности обучающихся, с учётом уровня освоения учебного материала, изученного ими ранее в рамках получения базового образования или на курсах повышения квалификации.

Текущий контроль или промежуточный контроль предполагается проводить в форме зачётов по отдельным разделам и темам учебной программы. Для проведения промежуточного контроля разрабатываются тестовые задания, включающие вопросы по наиболее актуальным материалам, изучаемым обучающимися. Общее количество вопросов в тестах не должно превышать двадцати.

Конкретные формы и процедуры входного, текущего и промежуточного контроля знаний по каждому разделу и отдельным темам разрабатываются учебным заведением самостоятельно и доводятся до сведения обучающихся.

Итоговая аттестация обучающихся предусматривает проведение экзамена в форме тестирования.

Порядок проведения итоговой аттестации определен Положением об итоговой аттестации, утвержденным ректором Академии.

Перечень вопросов, используемых для проведения экзамена, формируется на основе перечня основных вопросов (тестов), составляемых для контроля знаний обучающихся, при проведении промежуточного контроля знаний по учебным дисциплинам (модулям), представленных в рабочей программе повышения квалификации.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Перечень вопросов, выносимых на экзамен

Перечень основных вопросов, выносимых для контроля знаний, обучающихся по итогам изучения учебного курса:

1. Основные термины и определения в области ТЗИ. Цели и задачи ТЗИ.
2. Понятие защищаемого объекта информатизации. Этапы классификации объектов информатизации. Нормативные документы.
3. Виды объектов информатизации: краткая характеристика. Нормативные документы.
4. Система документов в области ТЗИ.
5. Система стандартов в области ТЗИ.
6. Ответственность за правонарушения в области защиты информации.

7. Основные мероприятия, проводимые для обеспечения защиты информации, содержащейся в государственной информационной системе

8. Требования международных стандартов по защите информации от НСД.

9. Стадии и этапы создания системы защиты информации.

10. Государственные информационные системы.

11. Понятие и общая классификация угроз безопасности информации, связанных с НСД.

12. Методы выявления и анализа угроз безопасности информации.

13. Методы выявления и анализа уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

14. Обеспечение защиты информации от НСД в ходе эксплуатации аттестованной информационной системы.

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

16. Требования к мерам защиты информации от НСД, реализуемым в информационной системе. Меры защиты информации от НСД.

17. Средства защиты информации от НСД.

18. Классификация видов контроля состояния ТЗИ от НСД.

19. Система документов по контролю состояния ТЗИ от НСД.

20. Классификация методов контроля защищенности информации от НСД и их характеристика.

21. Сканеры безопасности и их характеристика.

22. Средства анализа программных кодов и их характеристика. Средства антивирусной защиты и их характеристика.

23. Защита информации в вычислительных сетях: способы и основные средства.

24. Понятие и основные виды вредоносных программ.

25. Компьютерные вирусы: определение, классификация, основные функции (воздействия).

26. Способы и средства защиты от вредоносных программ.

27. Основные способы и средства обеспечения безопасности информации при межсетевом взаимодействии: краткая характеристика.

28. Понятие идентификации, аутентификации, авторизации. Управление доступом к ресурсам сетевой системы.

29. Понятие межсетевого экранирования, типы межсетевых экранов (МЭ). Примеры и основные функции современных МЭ.

30. Назначение и принципы работы систем обнаружения вторжений (IDS).

Примеры тестовых вопросов

1. Что является базовыми свойствами безопасности информации?

Безопасность, актуальность, объективность
Секретность, защищенность, быстродействие
Конфиденциальность, целостность, доступность
Конфиденциальность, неприкосновенность, защищённость

2. Какое свойство безопасности информации означает её неизменность в условиях случайного или преднамеренного искажения?

Конфиденциальность
Целостность
Актуальность

Доступность

3. Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации в соответствии с ГОСТ Р 50922-2006 это_____

Структура защиты информации
Политика безопасности информации
Система защиты информации
Техника защиты информации

4. Какие существуют виды сетей по управлению ресурсами?

проводные и беспроводные
одноранговые и клиент-серверные
локальные и территориальные
одноранговые и беспроводные

5. Модель безопасности "Рабочая группа": какое условие должно быть выполнено для авторизации пользователя рабочей станции на сервере?

наличие учётной записи с одинаковым именем и паролем на рабочей станции и сервере

наличие на сервере и рабочей станции учётных записей с одинаковым именем пользователя, но разными паролями

наличие на сервере и рабочей станции учётных записей с одинаковым паролем, но разными именами пользователей

встроенная учётная запись с административными правами

6. Модель безопасности "Доменная сеть": преимущество в использовании заключается в том, что _____

пользователь домена должен быть указан в учётных записях Windows как локально на узле, так и на сервере

пользователь домена жёстко привязан к сетевому узлу

пользователь домена может зарегистрироваться в сети на любой рабочей станции в этом домене и получить доступ к его ресурсам

контроллер домена используется как файловый сервер

7. Что такое Active Directory (служба каталогов)?

сетевая файловая система

база данных, в которой хранится информация о расположении сетевых каталогов

иерархически организованное хранилище данных об объектах сети, обеспечивающее удобные средства для поиска и использования этих данных

таблица размещения файлов на диске

8. Что является доменом 2-го уровня в представленном примере: www.dev.microsoft.com?

microsoft
dev
com
www

9. Какой из представленных диапазонов IP-адресов зарезервирован под локальные сети?

176.18.1.0 /16
192.168.0.0 /24
162.198.0.0 /24
192.168.0.0 /16

10. Что понимается под сетевым протоколом (протоколом передачи данных)?

набор правил (процедура), позволяющий осуществлять соединение и обмен данными между двумя и более сетевыми абонентами
правила (процедура) обработки данных в компьютерной сети
процедура подключения компьютеров к коммуникационной подсети
регламент работы сетевой службы

11. Какого уровня не существует в Модели взаимодействия открытых систем OSI/ISO?

физического
транспортного
уровня представлений
уровня объединения

12. Для чего предназначен межсетевой экран?

для обнаружения вторжений на узел сети
для запрета запуска приложений на компьютере
для разграничения пропуска трафика по адресам источника/ назначения и открытым приложениями (службами) портам
для обнаружения и устранения вредоносных программ

Лицам, успешно освоившим дополнительную профессиональную программу повышения квалификации и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

Проректор по учебной работе  И.В. Кожанова