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

Утверждаю
Ректор «Академии ФНС ЛАБ»

_____ И.А. Ефремов
«29» января 2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
«Защита информации с использованием отечественного программного обеспечения»

по повышению квалификации федеральных государственных гражданских служащих

(объем 54 часа)

Рассмотрена
на заседании кафедры
информационной безопасности
Протокол № 1 от 29.01.2026

2026

Оглавление

ВВЕДЕНИЕ ... 3
Цель реализации программы повышения квалификации ... 4
Требования к квалификации поступающего на обучение ... 4
ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ... 4
УЧЕБНЫЙ ПЛАН ... 6
КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК ... 7
РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН (МОДУЛЕЙ) ... 8
Правовые и организационные основы защиты информации ... 8
Введение ... 8
Цели, задачи и место учебной дисциплины в процессе повышения квалификации ... 8
Планируемые результаты обучения ... 8
Реферативное описание тем ... 9
Практические задания ... 10
Методические рекомендации ... 10
Список литературы ... 12
Способы и средства защиты информации с использованием отечественного программного обеспечения ... 13
Введение ... 13
Цели, задачи и место учебной дисциплины в процессе повышения квалификации ... 13
Планируемые результаты обучения ... 13
Реферативное описание тем ... 15
Практические задания ... 17
Методические рекомендации ... 18
Список литературы ... 20
Контроль состояния технической защиты информации от несанкционированного доступа ... 20
Введение ... 20
Цели, задачи и место учебной дисциплины в процессе повышения квалификации ... 21
Планируемые результаты обучения ... 21
РЕФЕРАТИВНОЕ ОПИСАНИЕ ТЕМ ... 23
Практические задания ... 23
Методические рекомендации ... 24
Список литературы ... 25
ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ ... 28
ФОРМЫ АТТЕСТАЦИИ ... 30
ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ... 31
Перечень вопросов, выносимых на экзамен ... 31
Примеры тестовых вопросов ... 32

ВВЕДЕНИЕ

Программа повышения квалификации «Защита информации с использованием отечественного программного обеспечения» разработана с учетом требований:

- Федерального закона от 29 декабря 2012 года № 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 науки и высшего образования Российской Федерации от 24.03.2025 N 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Приказа Минтруда России от 14.09.2022 № 536н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 18.10.2022 № 70596);
- Приказа Минтруда России от 14.09.2022 № 533н "Об утверждении профессионального стандарта "Специалист по безопасности компьютерных систем и сетей" (Зарегистрировано в Минюсте России 14.10.2022 № 70515);
- Приказа Минтруда России от 14.09.2022 № 525н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 14.10.2022 № 70543);
- Приказа Минтруда России от 09.08.2022 № 474н "Об утверждении профессионального стандарта "Специалист по технической защите информации" (Зарегистрировано в Минюсте России 09.09.2022 № 70015).

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 информационно-телекоммуникационных сетях (далее – обучающиеся), в части использования способов и средств защиты информации от несанкционированного доступа (НСД).

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 с использованием отечественного ПО в ходе эксплуатации объектов информатизации;

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

способность обеспечивать ЗИ в ИС с использованием отечественного ПО 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;

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 от НСД в АС (ИС), требования и рекомендации по защите объектов информатизации;

меры и средства защиты информации от НСД в АС (ИС);

требования к средствам защиты информации от НСД 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 отечественные 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 отечественных средств защиты информации (СЗИ) доверенной загрузки и разграничения доступа;

настройки и использования основных защитных механизмов, реализованных в отечественных операционных системах;

разграничения прав пользователей в базе данных отечественного производства, настройке ограничений, правил и триггеров;

установки, настройки и администрирования СЗИ отечественного производства 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
«Защита информации с использованием отечественного программного обеспечения»

по повышению квалификации федеральных государственных гражданских служащих

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) повышения профессионального уровня в рамках имеющейся квалификации по вопросам защиты информации от несанкционированного доступа с использованием отечественного программного обеспечения*

Категория, группа должностей: *ведущая, старшая, младшая группы должностей, категории: руководители, 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: *54 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	Правовые и организационные основы защиты информации	8	8	0	0	зачет
2	Способы и средства защиты информации с использованием отечественного программного обеспечения	36	8	28	0	зачет
3	Контроль состояния технической защиты информации от несанкционированного доступа	8	0	8	0	зачет
	Итоговая аттестация	2			2	экзамен в форме тестирования
	ИТОГО	**54**	**16**	**36**	**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
Виды занятий, предусмотренные программой повышения квалификации	А	А	А	А	А	АК	А	АИ

А- аудиторная и самостоятельная работа

И – итоговая аттестация

К – каникулы.

РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН (МОДУЛЕЙ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Правовые и организационные основы защиты информации

Введение

Рабочая программа дисциплины разработана для программы повышения квалификации «Защита информации с использованием отечественного программного обеспечения».

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: «Способы и средства защиты информации с использованием отечественного программного обеспечения», «Контроль состояния технической защиты информации от несанкционированного доступа».

Планируемые результаты обучения

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.	Правовые основы защиты информации	лекция

Объем занятий по дисциплине – 8 часов (15% 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. Правовые основы ЗИ.

Правовые основы защиты информации. Система документов в области

ТЗИ. Нормативные правовые акты. Нормативные правовые акты ФСТЭК России. Методические документы. Технические документы (документация). Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Общие вопросы организации лицензирования деятельности в области ТЗИ, сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Ответственность за правонарушения в области защиты информации.

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

Методические рекомендации

Занятия по дисциплине проводятся в форме лекций; практических занятий и семинаров по данной дисциплине не предусмотрено. 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.

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. 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. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2022. — 325 с.

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

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. Сёмкин С.Н., Сёмкин А.Н. Основы правового обеспечения защиты информации. Учебное пособие для вузов. М.: 2008. - 238 с.: ил.

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

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

5. 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.

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

7. 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.

8. 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.

9. 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.

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

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

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Способы и средства защиты информации с использованием отечественного программного обеспечения

Введение

Рабочая программа дисциплины разработана для программы повышения квалификации «Защита информации с использованием отечественного программного обеспечения».

В результате освоения данной дисциплины государственные гражданские служащие инспекций и управлений ФНС России совершенствуют свои знания и приобретают практические навыки использования отечественного программного обеспечения, 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 отечественного программного обеспечения для защиты информации в автоматизированных (информационных) системах (АС (ИС)).

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 отечественного 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 технической защиты информации от несанкционированного доступа» и в своей дальнейшей профессиональной деятельности.

Планируемые результаты обучения

В результате изучения данной дисциплины обучающиеся должны:

а) *знать*:

процедуры выявления угроз НСД 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 от НСД;

требования к отечественным 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 отечественные средства защиты информации, применяемые в АС (ИС);

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

в) владеть навыками:

проведения работ, связанных с защитой информации от НСД;

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

настройки и использования основных защитных механизмов, реализованных в отечественных операционных системах;

разграничения прав пользователей в базе данных, настройке ограничений, правил и триггеров с использованием отечественных СУБД;

установки, настройки и администрирования отечественных СЗИ в компьютерных сетях.

№п/п	**Наименование тем**	**Вид занятия**
1.	Угрозы безопасности информации, связанные с несанкционированным доступом	лекция
2.	Порядок использования средств защиты информации	практика
3.	Меры и средства защиты информации от несанкционированного доступа с использованием отечественного ПО	лекция
4.	Администрирование и принципы работы с современными операционными системами Linux	практика
5.	Настройка и использование основных защитных механизмов, реализованных в операционных системах Linux	практика
6.	Способы и средства ограничения полномочий и разрешений пользователей баз данных с использованием отечественного ПО	практика
7.	Установка, настройка и администрирование средств защиты информации в локальных вычислительных сетях и при межсетевом взаимодействии с использованием отечественного ПО	практика
8.	Управление ключевой информацией с использованием отечественного ПО. Удостоверяющие центры.	практика
9.	Установка, настройка и использование средств криптографической защиты информации и электронной подписи с использованием отечественного ПО	практика

Объем занятий по дисциплине – 36 часов (67% от всего объема программы).

Реферативное описание тем

Тема № 1. Угрозы безопасности информации, связанные с НСД.

Понятие и классификация угроз безопасности информации, связанных с НСД. Источники угроз безопасности информации от НСД.

Модели угроз безопасности информации от НСД.

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

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

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

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

Угрозы безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн).

Тема №2. Порядок использования средств защиты информации.

Классификация и требования к информационным (автоматизированным) системам по защите информации от НСД.

Классификация и требования к средствам вычислительной техники (СЗИ) по защищённости от НСД. Понятие СВТ, отличие СВТ от средств защиты информации (СЗИ) от НСД.

Классификация СЗИ от НСД по защищённости от НСД. Требования нормативных документов к каждому типу и классу СЗИ от НСД.

Требования нормативных документов РФ по использованию сертифицированных СВТ и СЗИ от НСД.

Порядок использования сертифицированных СЗИ в ТНО: получение СЗИ из вышестоящей организации, регистрация и учёт СЗИ, правила установки СЗИ на АРМ, настройка и использование СЗИ в ходе эксплуатации. Установка, настройка и использование отечественных сертифицированных средств комплексной защиты от НСД.

Тема №3. Меры и средства защиты информации от несанкционированного доступа с использованием отечественного ПО.

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

Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД. Особенности создания системы защиты информации от НСД как обеспечивающей подсистемы автоматизированной (информационной) системы.

Системные и документационные части системы защиты информации от НСД.

Тема №4. Администрирование и принципы работы с современными операционными системами Linux.

Принципы построения и структура операционных систем (ОС) класса Linux. Графические оболочки Fly, GNOME, KDE и другие.

Пользователи с точки зрения системы, понятие терминала. Работа с командной строкой, структура файловой системы Ext2 (Ext3, Ext4) и работа с объектами файловой системы (файлами, папками, дисками, устройствами), права доступа в Linux, возможности командной оболочки, текстовые редакторы. Элементы администрирования ОС Linux: этапы загрузки системы, технологии работы с внешними устройствами, файловыми системами и сетью в Linux, администрирование системы посредством конфигурационных файлов, управление пакетами.

Тема №5. Настройка и использование основных защитных механизмов, реализованных в операционных системах Linux.

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

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

Тема №6. Способы и средства ограничения полномочий и разрешений пользователей баз данных с использованием отечественного ПО.

Понятие базы данных, системы управления базами данных (СУБД). Механизмы разграничения доступа пользователей к объектам баз данных. Установка, настройка и использование механизмов разграничения доступа, встроенных в СУБД My SQL (PostGreSQL).

Основы использования языка Transact SQL для управления механизмами защиты информации от НСД в базах данных.

Тема №7. Установка, настройка и администрирование средств защиты информации в локальных вычислительных сетях и при межсетевом взаимодействии с использованием отечественного ПО.

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.

Настройка встроенных в ОС межсетевых экранов (iptables или ipchains), настройка правил фильтрации, то есть, обработки IP-пакетов, основываясь на IP-адресе источника пакета, IP-адресе назначения пакета, интерфейсе, который принял пакет, протоколе, по которому осуществляется передача пакета, на порту назначения пакета.

Установка, настройка и использование отечественных средств комплексной защиты от НСД.

Тема №8. Управление ключевой информацией с использованием

отечественного ПО. Удостоверяющие центры.

Назначение и порядок использования аппаратных ключей в качестве ключевых носителей. Использование дополнительных служб в инфраструктуре открытых ключей.

Основные понятия и определения PKI. Назначение и взаимодействие элементов PKI. Состав PKI. Системы стандартов в области PKI. Протоколы, используемые в PKI. Основные группы приложений-потребителей услуг PKI.

Назначение, состав и порядок использования программно-аппаратных средств автоматизации деятельности Удостоверяющих центров, работающих под ОС Linux.

Автоматизация управления жизненным циклом сертификатов, изданных с помощью средств Удостоверяющего центра.

Тема №9. Установка, настройка и использование средств криптографической защиты информации и электронной подписи с использованием отечественного ПО.

Криптографические средства защиты информации (СКЗИ): состав, принципы работы, что к ним относится. Установка, настройка и использование СКЗИ КриптоПро CSP и КриптоАРМ. Использование КриптоПро CSP для постановки электронной подписи и её проверки.

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 Astra Linux 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 приложений Astra Linux.
5. Настройте первоначальные параметры безопасности: отключение потенциально опасных служб, использование локальных параметров безопасности.
6. С помощью Диспетчера конфигурации PostGre SQL на сервере настройте доступ к SQL Server’у с рабочей станции.
7. Откройте среду PostGre SQL, войдите с проверкой подлинности SQL server – имя входа sa, пароль sa.
8. Создайте в SQL-сервере для доступа к БД Торговля новые имена входа с разными серверными ролями: Имя1 – роль sysadmin; Имя2 – роль serveradmin. Проверьте их права и полномочия.
9. Создайте пользователя БД Торговля User1, сопоставьте его с именами входа – Пользователи Astra Linux, схемой БД – db_datareader и ролью – db_datareader. Проверьте полномочия пользователя User1 в БД Торговля.

10. В SQL-сервере для этих учётных записей создайте имена входа: reader_товары и reader_покупки с ролью сервера Public, сопоставив их с пользователями базы данных Торговля.

11. Настройте сетевые подключения в виртуальной машине с Astra Linux: 1-е соединение – 10.0.1.100, 2-е соединение – 10.0.2.100.

12. Настройте межсетевой экран Astra Linux, используя входящие и исходящие фильтры на запрет пропуска пакетов по протоколам ftp, http, smtp, pop3. Проверьте действие фильтров.

13. Настройте в межсетевом экране Astra Linux преобразователь сетевых адресов (NAT).

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

15. Установите и настройте под Astra Linux межсетевой экран и криптошлюз VipNet Coordinator.

16. Настройте транзитные фильтры VipNet Coordinator на запрет пакетов по протоколам ftp, http. Проверьте действие фильтров.

17. Настройте локальные фильтры VipNet Coordinator на запрет пакетов по протоколам ftp, http. Проверьте действие фильтров.

18. Установите СКЗИ КриптоПро CSP и КриптоАРМ на виртуальную машину с ОС Astra Linux.

19. 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 Криптопро CSP на своей рабочей станции.

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

21. 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.

22. 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.

23. 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.

Методические рекомендации

Занятия по дисциплине проводятся в форме лекций, практических занятий и лабораторных работ. 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 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.

При проведении практических занятий и лабораторных работ рекомендовано использование лицензионного программного обеспечения.

Список литературы

а) основная литература:

1. Информационная безопасность в таблицах и схемах: учебно-методическое пособие. Н.Г. Лабутин, О.И. Климченков. Часть 1, 6-е изд. – Н. Новгород: Приволжский ин-т повышения квалификации ФНС, 2023. – 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. 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. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях: учебное пособие / В.Ф. Шаньгин. – М.: ДМК Пресс, 2023. – 594 с.

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

Введение

Рабочая программа дисциплины разработана для программы повышения

квалификации «Защита информации с использованием отечественного программного обеспечения».

В результате освоения данной дисциплины государственные гражданские служащие инспекций и управлений ФНС России совершенствуют свои знания и навыки по выполнению мероприятий по контролю состояния защищённости объектов информатизации, позволяющие специалисту по защите информации организовать мероприятия по технической защите информации от несанкционированного доступа и применять в своей деятельности 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 контроля состояния технической защиты информации от несанкционированного доступа.

Задачи:

Приобретение (совершенствование) навыков проведения мероприятий контроля состояния технической защиты информации.

Получение навыков разработки документов локального уровня для организации и проведения мероприятий по контролю состояния защиты информации на объекте.

Получение практических навыков использования отечественного программного обеспечения для мониторинга безопасности информации.

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.

Планируемые результаты обучения

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 с использованием отечественного ПО в ходе эксплуатации объектов информатизации;

способность обеспечивать контроль состояния ЗИ в ИС с использованием отечественного ПО 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;

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 от НСД;

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 контроля состояния ТЗИ от НСД;

в) владеть навыками:

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

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

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.

№п/п	Наименование тем	Вид занятия
1.	Методы и средства контроля защищённости информации от НСД с использованием отечественного ПО	практика
2.	Мониторинг информационной безопасности средств и систем информатизации с использованием отечественного ПО	практика

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 8 часов (15% от всего объёма программы).

РЕФЕРАТИВНОЕ ОПИСАНИЕ ТЕМ

1. Методы и средства контроля защищённости информации от НСД с использованием отечественного ПО

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 под Linux.

2. Мониторинг информационной безопасности средств и систем информатизации с использованием отечественного ПО

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

Вопросы, подлежащие проверке при контроле состояния ТЗИ от НСД в организации. Организационный и технический контроль состояния ТЗИ от НСД.

Проведение мониторинга защищённости средств и систем с использованием отечественного ПО.

Практические задания

1. Формирование перечня направлений проверки при контроле состояния ТЗИ от НСД в организациях.
2. Практическое применение антивирусных средств при проведении контроля защищенности информации.
3. Практическое применение методик аттестационных испытаний.
4. Подготовка заключения по результатам аттестации объекта информатизации по требованиям безопасности информации.
5. Организация проведения работ, выполняемых при осуществлении сертификационных испытаний на соответствие требованиям по безопасности

информации продукции, используемой для защиты конфиденциальной информации.

6. Подготовка документов для организации и проведения аттестации объектов информатизации на соответствие требованиям безопасности информации.

7. Использование средств мониторинга защищённости информации. Анализ отчётов средств мониторинга.

Методические рекомендации

Занятия по дисциплине проводятся в форме практических занятий. В процессе изучения учебной дисциплины лекций не предусмотрено.

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 контроля состояния технической защиты конфиденциальной информации на объекте защиты, особенности подготовки локальных актов, регламентирующих проведения контроля состояния технической защиты конфиденциальной информации.

Все занятия по данной дисциплине - практические, для проведения которых рекомендуется применять современные формы и методы обучения, включая активные и интерактивные.

Для проведения практических 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 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.

При выполнении практических заданий рекомендуется применять лицензионное программное обеспечение.

Список литературы

а) основная литература:

1. Информационная безопасность в таблицах и схемах: учебно-методическое пособие. Часть 1, 6-е изд. Н.Г. Лабутин, О.И. Климченков. - Н. Новгород: Приволжский ин-т повышения квалификации ФНС, 2023. - 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. Защита информации в компьютерных системах и сетях: учебное пособие / В.Ф. Шаньгин. – М.: ДМК Пресс, 2023. – 594 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. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и Техника, 2011. — 384 с.
4. Мещеряков Р.В., Шелупанов А.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Монография. – Томск: Изд-во В-Спектр, 2007.
5. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений: Учебное пособие. М: ЮНИТИДАНА, 2001.

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

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

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

8. 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».

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

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

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

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

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

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

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

16. 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.

17. 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.

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

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

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

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

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

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

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

25. 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).

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

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

28. 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).

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

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

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

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

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

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

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Занятия проводятся в соответствии с методическими материалами, разработанными преподавателями Академии. 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. 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.

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.

ФОРМЫ АТТЕСТАЦИИ

Оценка качества освоения программы включает входной, текущий или промежуточный контроль, 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. Методы защиты информации на уровне управления базами данных в ОС Linux: от случайных угроз и от преднамеренных угроз.

24. Защита информации в базе данных с помощью определения прав и привилегий пользователей в ОС Linux.

25. Понятие и основные виды вредоносных программ.

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

27. Методы и средства выявления в ОС Linux компьютерных вирусов и защиты от них.

28. Способы и средства защиты от вредоносных программ.

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

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

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

32. Назначение и принципы работы систем обнаружения вторжений (IDS) под Linux.

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. Как называется состояние информации, при котором субъекты, имеющие права доступа к ней, могут реализовывать их беспрепятственно?

Доступность
Конфиденциальность
Актуальность
Целостность

5. Какое свойство безопасности информации означает обязательное требование к лицу, получившему доступ к информации, не передавать ее третьим лицам без согласия обладателя этой информации?

Актуальность
Целостность
Конфиденциальность
Доступность

6. Согласно законодательству РФ информация в зависимости от категории доступа к ней подразделяется на:

неконфиденциальную и конфиденциальную информацию
секретную и несекретную информацию
общедоступную и информацию ограниченного доступа
речевую и видовую информацию

7. Какие из представленных средств НЕ являются вредоносными программами

троянские кони
сетевые черви
компьютерные вирусы
трансляторы

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

Проректор по научному и инновационному развитию Е.А. Хицков