Публичное акционерное общество
«Информационные телекоммуникационные технологии»
(ПАО «Интелтех»)

УТВЕРЖДАЮ
Генеральный директор
ПАО «Интелтех»

М.В.Винокур

«08» ноября 2023

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ СВЯЗИ

ПО ДИСЦИПЛИНЕ «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. СПОСОБЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА»

Рассмотрено на заседании
Научно-технического совета
ПАО «Интелтех».
Протокол № 14-23
от «27» апреля 2023 г.

Санкт-Петербург
2023

I. ЦЕЛЕВАЯ УСТАНОВКА И ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Целью учебной дисциплины является повышение уровня профессиональной подготовки военнослужащих по контракту, исполняющих должности (обязанности) по обеспечению защиты информации в АС СН специального назначения (АС СН).

Задачи учебной дисциплины:

1. Изучить основы построения Государственной системы защиты информации в Российской Федерации, ее цели и основные задачи.

2. Изучить принципы обеспечения безопасности использования аппаратно-программных средств защиты информации.

3. Изучить деятельность должностных лиц по обеспечению защиты информации в органах и на объектах военного управления при ее обработке техническими средствами.

В результате изучения дисциплины обучающиеся должны:

иметь представление:

о целях, задачах и структуре государственной системы защиты информации в Российской Федерации, о нормативно-правовой основе ее функционирования;

о характеристиках и возможностях основных систем и технических средств разведки иностранных государств;

об основах организации комплексной защиты информации в АС СН;

о принципах обеспечения защиты объектов управления, связи и автоматизации от несанкционированного доступа техническими средствами;

об основах защиты информации в системах и средствах автоматизации от несанкционированного доступа;

о перспективах развития систем и комплексов средств автоматизации управления войсками и связью;

знать:

требования руководящих и нормативных документов ФСТЭК Российской Федерации по защите информации в АС СН;

требования приказов МО РФ, внутренних распорядительных документов по защите информации в АС СН;

основы защиты информации рабочих станций АС СН от несанкционированного доступа;

основы защиты информации от несанкционированного доступа с помощью штатных средств операционных систем;

основы организации и обеспечения мониторинга безопасности информации в АС СН;

организацию защищенного документооборота и обеспечение защиты информации на объектах военного управления;

администрирование и контроль безопасности информации в АС СН;

основы защиты информации с помощью межсетевых экранов;

основы защиты информации в АС СН с помощью виртуальных защищенных сетей;

уметь:

применять сертифицированные аппаратно-программные и программные средства защиты рабочих станций АС СН;

применять средства антивирусной защиты;

применять средства анализа защищенности АС СН;

проводить мониторинг безопасности информации АС СН.

Объектом учебной дисциплины являются АС СН органов и объектов военного управления.

Предметом учебной дисциплины является комплексная защита информации в АС СН органов и объектов военного управления.

Учебная дисциплина «Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа» состоит из пятнадцати тем.

Дисциплина обеспечивает формирование специальных знаний и практических навыков, необходимых для качественного исполнения должностей специалистами защиты информации в АС СН.

Занятия по теме 1 обеспечивают совершенствование знаний по основам Государственной системы защиты информации. Раскрывают требования основных руководящих документов в области защиты информации в АС СН. Характеризуют основные направления защиты и содержание основных мероприятий.

Занятия по теме 2 раскрывают современные взгляды на принципы и технологии построения АС СН. Обеспечивают овладение знаниями по роли и месту АС СН в организации и обеспечении обмена информацией в органах военного управления. Раскрывают основные аппаратно-технические элементы АС СН, виды и классификацию программного обеспечения.

Содержание темы 3 раскрывает современные угрозы информационной безопасности. Дают представление о современных взглядах на сущность и содержание комплексной защиты информации.

Содержание темы 4 способствует совершенствованию знаний основам организации комплексной защиты информации в АС СН объектов военного управления.

Занятия по теме 5 обеспечивают совершенствование знаний по вопросам организации защиты информации в АС СН объектов военного управления от утечки по техническим каналам. Раскрывают характеристики основных технических каналов утечки информации при функционировании АС СН.

Занятия по теме 6 раскрывают основы защиты информации в АС СН от несанкционированного доступа. Характеризуют структуру подсистемы защиты информации в АС СН от несанкционированного доступа.

Занятия по теме 7 дают основы защиты информации в АС СН от специальных программ - «вирусов».

Занятия по теме 8 обеспечивают овладение знаниями по основам защиты информации с помощью штатных средств операционных систем. Позволяют овладеть основами применения политик информационной безопасности.

Занятия по теме 9 обеспечивают овладение знаниями по вопросам обеспечения мониторинга безопасности информации в АС СН. Раскрывают механизмы и алгоритмы функционирования средств анализа защищенности АС СН.

Занятия по теме 10 раскрывают основы защиты информации в АС с помощью систем обнаружения компьютерных атак.

Занятия по теме 11 позволяют овладеть знаниями по защите абонентских пунктов АС СН техническими средствами охраны.

Занятия по теме 12 обеспечивают овладение знаниями по обеспечению защиты информации при организации защищенного электронного документооборота на объектах военного управления.

Занятия по теме 13 дают основы администрирования и контроля безопасности информации в АС СН. Раскрывают основные должностные обязанности администратора безопасности.

Занятия по теме 14 позволяют овладеть знаниями по основам защиты информации с помощью межсетевых экранов. Дают механизмы и алгоритмы их функционирования.

Занятия по теме 15 раскрывают принципы построения и практического использования протоколов и алгоритмов защиты информации в АС СН с помощью виртуальных защищенных сетей

Материал учебной дисциплины осваивается как на лекциях, семинарских и групповых занятиях, так и в ходе практических занятий. Особенностями содержания занятий является их связь с практикой функционирования органов и объектов военного управления.

Изложение материала основывается на результатах входного контроля знаний обучаемых и исполняемых ими должностных обязанностей. Текущий контроль хода усвоения материала дисциплины осуществляется на всех видах занятий.

Изучение дисциплины заканчивается проведением зачета с оценкой.

Зачет с оценкой является итоговым аттестационным испытанием, завершающим освоение дополнительной образовательной программы повышения квалификации специалистов по обеспечению защиты информации в АС СН. На зачет выносятся два теоретических вопроса. Первый вопрос - по государственной системе защиты информации, второй вопрос - по организации комплексной защиты информации в АС СН органов и объектов военного управления.

II. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ТЕМАМ И ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ

Номера и наименование разделов и тем	Всего учебного времени	Всего часов учебных занятий по расписанию	Из них по основным видам занятий										Зачеты, экзамен	Время, отводимое на самостоятельную работу
			Лекции	Семинары	Лабораторные работы	Практические занятия	Групповые упражнения	Групповые занятия	Тактические и тактико-специальные занятия	КШВИ, КШУ, военные (военно-специальные) игры	Курсовая работа (проекты, задачи)	Самостоятельные занятия под руководством преподавателя		
Тема 1. Государственная система защиты информации. Требования правовых, руководящих и нормативных документов по комплексной защите информации в АС СН.	18	12	10	2										6
Тема 2. Роль и место АС СН в организации и обеспечении обмена информации в органах военного управления.	9	6	4	2										3
Тема 3. Современные угрозы информационной безопасности АС СН.	9	6	4	2										3
Тема 4. Основы организации и обеспечения комплексной защиты информации в АС СН.	9	6	2	2				2						3
Тема 5. Основы защиты информации в АС СН от утечки по техническим каналам.	12	8	4	2		2								4
Тема 6. Основы защиты информации от несанкционированного доступа в АС СН	9	6	2	2		2								3
Тема 7. Основы защиты информации в АС СН от специальных программ-вирусов.	18	12	2	2		6		2						6
Тема 8. Основы защиты информации от НСД с помощью штатных средств операционных систем.	18	12	2	2		6		2						6
Тема 9. Основы организации и обеспечения мониторинга безопасности информации в АС СН.	18	12	2	2		6		2						6
Тема 10. Основы защиты информации в АС СН с помощью систем обнаружения компьютерных атак.	18	12	2	2		6		2						6

Номера и наименование разделов и тем	Всего учебного времени	Всего часов учебных занятий по расписанию	Из них по основным видам занятий										Зачеты, экзамен	Время, отводимое на самостоятельную работу
			Лекции	Семинары	Лабораторные работы	Практические занятия	Групповые упражнения	Групповые занятия	Тактические и тактико-специальные занятия	КШВИ, КШУ, военные (военно-специальные) игры	Курсовая работа (проекты, задачи)	Самостоятельные занятия под руководством преподавателя		
Тема 11. Основы защиты абонентских пунктов АС СН техническими средствами охраны.	9	6	4	2										3
Тема 12. Обеспечение защиты информации при организации защищенного документооборота в АС СН.	12	8	2	2		2		2						4
Тема 13. Администрирование и контроль безопасности информации в АС СН. Основные должностные обязанности администратора безопасности, операторов рабочих станций АС СН.	15	10	2	2		4		2						5
Тема 14. Основы защиты информации в АС СН с помощью межсетевых экранов.	18	12	2	2		6		2						6
Тема 15. Основы защиты информации в АС с помощью виртуальных защищенных сетей.	15	10	2	2		4		2						5
Зачет с оценкой	9	6											6	3
Всего по дисциплине:	216	144	46	30		44		18					6	72

III. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ

Тема 1. Государственная система защиты информации. Требования правовых, руководящих и нормативных документов по комплексной защите информации в АС СН.

Цели, задачи и структура органов защиты информации в штабах и воинских частях. Правовые, руководящие и нормативные документы по комплексной защите информации в АС СН. *Руководящие и нормативные документы ФСТЭК Российской Федерации по защите информации в АС СН. Приказы МО РФ, внутренние распорядительные документы по защите информации в АС СН.*

Тема 2. Роль и место АС СН в организации и обеспечении обмена информации в органах военного управления.

Современные принципы и технологии построения АС СН. Основные аппаратно-технические элементы АС СН. Виды и классификация программного обеспечения АС СН.

Аппаратно-технические элементы АС СН и их программное обеспечение.

Тема 3. Современные угрозы информационной безопасности АС СН.

Модель угроз безопасности информации. Возможные сценарии воздействия нарушителя на систему защиты АС СН. Современные взгляды на сущность и содержание комплексной защиты информации АС СН.

Тема 4. Основы организации и обеспечения комплексной защиты информации АС СН

Основы организации комплексной защиты информации АС. *Основные аппаратно-технические элементы АС СН, виды и классификация программного обеспечения.*

Тема 5. Основы защиты информации в АС СН от утечки по техническим каналам

Характеристика основных ТКУИ при функционировании элементов АС СН, методы и средства защиты информации от утечки по ТКУИ. Модель ТКУИ при функционировании объектов ЭВТ как элементов АС СН.

Тема 6. Основы защиты информации от несанкционированного доступа в АС СН

Структура подсистемы защиты информации в АС СН от несанкционированного доступа. *Основы защиты информации рабочих станций АС СН от НСД.*

Тема 7. Основы защиты информации от специальных программ-вирусов

Основы защиты информации в АС СН с помощью средств антивирусной защиты. Применение средств антивирусной защиты в АС СН.

Тема 8. Основы защиты информации от НСД с помощью штатных средств операционных систем

Основы защиты информации в АС СН с помощью штатных средств операционных систем по обеспечению защиты информации, политик информационной безопасности. *Настройка политик информационной безопасности.*

Тема 9. Основы организации и обеспечения мониторинга безопасности информации в АС СН.

Основы защиты информации в АС СН с помощью средств анализа защищенности. *Основы администрирования и организации и обеспечения мониторинга безопасности информации в АС СН.*

Тема 10. Основы защиты информации в АС СН с помощью систем обнаружения компьютерных атак

Основы защиты информации от удаленного НСД с помощью систем обнаружения компьютерных атак. *Механизмы и алгоритмы функционирования систем обнаружения компьютерных атак.*

Тема 11. Основы защиты абонентских пунктов АС СН техническими средствами охраны.

Абонентские пункты. Структура, характеристика и основы защиты развертываемых абонентских пунктов. *Защита автоматизированных систем объектов информатизации от НСД техническими средствами охраны.*

Тема 12. Обеспечение защиты информации при организации защищенного документооборота в АС СН

Организация защищенного документооборота и обеспечение защиты информации в органах военного управления.

Тема 13. Администрирование и контроль безопасности информации в АС СН. Основные должностные обязанности администратора безопасности, операторов рабочих станций АС СН

Администрирование и контроль безопасности информации в АС СН.

Тема 14. Основы защиты информации в АС СН с помощью межсетевых экранов

Основы защиты информации в АС СН от удаленного НСД с помощью межсетевых экранов. *Основы защиты информации с помощью межсетевых экранов.*

Тема 15. Основы защиты информации в АС СН с помощью виртуальных защищенных сетей

Современные технологии защиты информации на основе виртуальных защищенных сетей. Принципы построения и практического использования протоколов и алгоритмов защиты информации в виртуальных защищенных сетях военного назначения.

IV. КОНТРОЛЬНЫЕ ЗАДАНИЯ

1. Входной контроль исходного уровня подготовки слушателей.
2. Государственная система защиты информации Российской Федерации (доложить).
3. Требования правовых и нормативных документов РФ, ФСТЭК, МО по защите информации в АС СН (доложить).
4. Современные принципы и технологии построения АС СН (доложить).
5. Модель угроз безопасности информации АС СН (доложить).
6. Модель технических каналов утечки информации (ТКУИ) на элементах АС СН (доложить).
7. Современные методы и средства защиты информации в АС СН от утечки по ТКУИ. (доложить).
8. Структура подсистемы защиты информации в АС СН от несанкционированного доступа (доложить).
9. Структура подсистемы защиты информации АС СН от несанкционированного доступа (доложить).
10. Защита информации в АС СН с помощью средств антивирусной защиты (доложить).
11. Штатные средства операционных систем по обеспечению защиты информации (доложить).
12. Защита информации в АС СН с помощью средств анализа защищенности (доложить).
13. Мониторинг безопасности информации в АС СН (доложить).
14. Защита информации в АС СН с помощью систем обнаружения компьютерных атак (доложить).
15. Обеспечение защиты информации в АС СН при организации защищенного документооборота (доложить).
16. Защита информации в АС СН с помощью межсетевых экранов (доложить).
17. Основные должностные обязанности администратора безопасности, операторов рабочих станций (доложить).
18. Протоколы безопасности виртуальных защищенных сетей (доложить).

V. СПИСОК ЛИТЕРАТУРЫ

1. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
2. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
3. Руководящий документ. «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации Классификация по уровню контроля отсутствия недекларированных возможностей». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
4. Руководящий документ. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
5. Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
6. Руководящий документ. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.
7. Руководящий документ. «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий». Введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187.
8. Руководящий документ. «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности». Введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187.
9. Руководящий документ. «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности». Введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187.
10. ИНФОРМАЦИОННОЕ СООБЩЕНИЕ. «Об утверждении Требований безопасности информации к операционным системам» от 18 октября 2016 г. № 240/24/4893.
11. ИНФОРМАЦИОННОЕ СООБЩЕНИЕ. «Об утверждении Требований к средствам антивирусной защиты» от 30 июля 2012 г. № 240/24/3095.
12. МЕТОДИЧЕСКИЙ ДОКУМЕНТ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.
13. МЕТОДИЧЕСКИЙ ДОКУМЕНТ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.
14. ГОСТ 34.003-90. «Автоматизированные системы. Термины и определения»
15. Приказ ФСТЭК № 9-2006. «Требования к МЭ».

16. ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».
17. ГОСТ Р 51188-98. «Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство».
18. ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения».
19. ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».
20. ГОСТ Р 51583-2014. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
21. Компьютерные сети. Принципы, технологии, протоколы. [Текст]: / В.Г. Олифер, Н.А. Олифер // – СПб.: Издательство «Питер», 2021.
22. Малюк А.А., Пазин С.В., Погожин Н.С. Введение в защиту информации в АС СН. – М.: Горячая линия – Телеком, 2001. – 148 с.
23. Стародубцев Ю.И., Коцыняк М.А., Фролов В.Ю. и др. Основы защиты систем связи и автоматизации от технических средств разведки. Учебное пособие. – СПб.: ВУС, 1998. – 416 с.
24. Запечников С.В., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей. М.: Горячая линия – Телеком, 2000.
25. Техническая документация по операционной системе специального назначения «ASTRA-Linux». [Текст]: техническая документация / НПО РусБИТех, Москва, 2013.
26. Техническая документация по системе антивирусной защиты «Dr.Web». [Текст]: техническая документация / ДокторВеб, Москва, 2013.

Заместитель генерального директора ПАО «Интелтех» по научной работе
доктор технически наук, доцент

И.А.Кулешов

Начальник НИО-062 (информационной безопасности)

В.С.Харитонов

Главный специалист отдела 0623
доктор технических наук, доцент

В.Е.Дементьев

«___»_____ 2023 года

Публичное акционерное общество
«Информационные телекоммуникационные технологии»
(ПАО «Интелтех»)

Учебный план
дополнительной образовательной программы
повышения квалификации специалистов по способам и средствам защиты информации от несанкционированного доступа в автоматизированных системах специального назначения
(код Д-3)

Цель обучения: повышение уровня профессиональной подготовки специалистов по обеспечению защиты информации в автоматизированных системах специального назначения.

Категория слушателей: офицеры с высшим военно-специальным образованием, исполняющие должности (обязанности) по обеспечению защиты информации в автоматизированных системах специального назначения, имеющие стаж практической работы не менее 5 лет или вновь назначенные на указанные должности.

Срок обучения: 1 месяц (216 часов).

Режим занятий: 6 учебных часов в день.

А. Сводные данные по бюджету учебного времени

Календарных дней/часов			Распределение учебного времени в часах						
Всего	Из них		Всего часов учебных занятий	В том числе			Итоговый контроль	Итоговая аттестация	Резерв учебного времени
	Выходные, праздничные дни	Учебное время		Учебные занятия по расписанию	Стажировки (практики)	Время на самостоятельную работу			
30/180	5/30	25/144	216	144	-	72	-	12	-

Примечания:

1. Предельная нагрузка слушателей различными видами занятий, проводимых под руководством преподавателей - 36 часов в неделю;
2. Общий объем учебной работы слушателей, включая самостоятельную работу, - 54 часа в неделю.

Б. План учебного процесса

Порядковый номер учетной дисциплины	Наименование учебных дисциплин и циклов (групп) учебных дисциплин	Всего учебного времени	Распределение учебного времени																
			Всего часов учебных занятий	в том числе											Время на стажировки	Время на самостоятельную работу	Итоговый контроль		
				Лекции	Семинары	Лабораторные работы	Практические занятия	Групповые упражнения	Групповые занятия	Тактические (тактико-специальные) занятия и учения	КШУ, военные (военно-специальные) игры	Курсовые работы, (проекты, задачи)	Самостоятельная работа под руководством преподавателя	Другие виды занятий			Экзамены	Зачеты	
																		С оценкой	Без оценки
Д-3	Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа	207	138	46	30		44		18							69			
ИАЗ	Итоговая аттестация-зачет с оценкой по дисциплине Д-3.	9	6													3		6	
	Всего учебных часов	216	144	46	30		44		18							72		6	
Недельная загрузка учебными занятиями 36 часов Количество: дисциплин - 1; зачет с оценкой – 1.																			

Заместитель генерального директора ПАО «Интелтех» по научной работе
Доктор технически наук, доцент

И.А.Кулешов

«___»_____ 2023 года

Публичное акционерное общество
«Информационные телекоммуникационные технологии» (ПАО «Интелтех»)

Учебная программа
дополнительной образовательной программы повышения квалификации специалистов по способам и средствам защиты информации от несанкционированного доступа в автоматизированных системах специального назначения
(код Д-3)