Аннотация дисциплины «Информационная безопасность»

Дисциплина «Информационная безопасность» посвящена изучению теоретических основ и получению практических навыков применения способов и средств технической и криптографической защиты информации, законодательства Российской Федерации, а также нормативных и руководящих документов регуляторов в области защиты информации. При освоении дисциплины «Информационная безопасность» обучающиеся изучают вопросы выявления актуальных угроз безопасности информации, методы и средства противодействия угрозами безопасности, планирование мероприятий, направленных на защиту информации, организация внедрения и применения политик (правил, процедур) по обеспечению технической защиты конфиденциальной информации, организацию мероприятий по контролю (мониторингу) защищенности конфиденциальной информации и внедрение способов и средств защиты информации.

Целью изучения дисциплины «Информационная безопасность» является систематизация и обновление профессиональных знаний в области организации комплексной защиты информации, в том числе персональных данных.

В рамках заявленной темы должны быть решены следующие задачи:

- формирование способности к обобщению, анализу, восприятию информации по обеспечению безопасности информации в органе государственной власти, в организации, на предприятии,
- формирование современных представлений об информационной безопасности и технической защите информации (ТЗИ);
- обучение подготовке организационных документов по ТЗИ;
- формирование представлений о защите информации криптографическими способами;
- обучение использованию современных компьютерных информационных технологий для защиты информации с помощью СКЗИ;
- приобретение умений и навыков использования программных и программно-аппаратных СКЗИ и ТЗИ
- изучение способов и средств защиты от несанкционированного доступа к конфиденциальной информации на объектах информатизации;
- организация информационных систем в соответствии с требованиями по защите конфиденциальной информации, в том числе, персональных данных.

Процесс изучения данной дисциплины направлен на развитие следующих компетенций.

Общекультурные компетенции:

– знать основы законодательства и правил его применения;

–применять современные информационно-коммуникационные технологии в сфере профессиональной деятельности;

– организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;

– осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;

– самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

Профессиональные компетенции:

– способность к аналитическому, системному, стратегическому видению формирования и развития процессов по защите информации;

– способность планирования работы исходя из должностных обязанностей;

– способность и готовность разрабатывать и аргументировать предложения, направленные на повышение эффективности защиты информации;

– способность применять способы и средства защиты информации для обеспечения требований нормативных документов.

Изучив данную программу, слушатель должен:

а) знать:

нормативные правовые акты, методические документы, международные и национальные стандарты в области криптографической и ТЗКИ;

виды конфиденциальной информации, перечни сведений конфиденциального характера;

возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;

действующую систему сертификации средств защиты информации по требованиям безопасности информации;

основы лицензирования деятельности по ТЗКИ;

требования по криптографической и ТЗКИ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения);

организацию и содержание проведения работ по криптографической и ТЗКИ, состав и содержание необходимых документов;

организацию и содержание проведения работ по контролю (мониторингу) защищенности конфиденциальной информации, состав и содержание необходимых документов;

правила разработки, утверждения, обновления и отмены документов в области криптографической и ТЗКИ;

типовую структуру, задачи и полномочия подразделения по ТЗИ;

принципы работы основных узлов современных технических средств информатизации;

технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами;

способы (методы) и требования по ТЗКИ;

методы и методики контроля (мониторинга) защищенности конфиденциальной информации;

порядок проведения контроля (мониторинга) информационной безопасности средств и систем информатизации;

требования к СКЗИ, средствам ТЗКИ и средствам контроля (мониторинга) эффективности мер защиты информации;

средства ТЗКИ, средства контроля (мониторинга) эффективности мер защиты информации, СКЗИ, порядок их применения, перспективы развития;

порядок установки, монтажа, испытаний СКЗИ, средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

б) уметь:

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

– разрабатывать необходимые документы в интересах проведения работ по криптографической и ТЗКИ;

– определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;

– формировать требования по криптографической и ТЗКИ;

– определять требования к средствам ТЗКИ и СКЗИ на объектах информатизации;

– организовывать и проводить работы по криптографической и ТЗКИ;

– организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля;

– применять на практике штатные СКЗИ, средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;

– проводить аттестационные испытания и аттестацию объектов информатизации на соответствие требованиям по защите информации, оформлять материалы аттестационных испытаний;

– проводить установку, монтаж, испытания и техническое обслуживание СКЗИ, средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

– разрабатывать документы для получения лицензии на проведение работ и оказания услуг по ТЗКИ для их представления в лицензирующий орган;

в) владеть навыками:

– работы с действующей нормативной правовой и методической базой в области криптографической и ТЗИ;

– выявления ТКУИ и определения угроз безопасности информации;

– определения задач, проведения организационных и технических мероприятий по криптографической и ТЗКИ;

– определения задач, проведения организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации, подготовки материалов по результатам контроля;

– применения СКЗИ, средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

– проведения аттестационных испытаний и аттестаций объектов информатизации на соответствие требованиям по защите информации, оформления материалов аттестационных испытаний;

– организации деятельности подразделений и специалистов в области криптографической и ТЗКИ;

– проведения установки, монтажа, испытания средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

В зависимости от категории слушателей дисциплина «Информационная безопасность» представлена в учебно-тематическом плане следующими темами:

1. Вычислительные сети, сети и системы передачи информации
2. Защищаемые информация и информационные ресурсы. Объекты защиты
3. Интегрированное занятие: расследование инцидентов информационной
4. безопасности
5. Криптографические методы и средства защиты информации
6. Меры и средства защиты информации от НСД
7. Методы и средства контроля защищённости информации
8. Мониторинг информационной безопасности средств и систем
9. информатизации
10. Настройка и использование основных защитных механизмов
11. Определение угроз безопасности информации ограниченного доступа
12. Организационно-технические основы выполнения мероприятий по ТЗИ
13. Организационные и технические меры защиты персональных данных в ИС
14. Организация защиты конфиденциальной информации на объектах информатизации
15. Основы организации и ведения работ по обеспечению безопасности персональных данных
16. Основы организации контроля состояния ТЗКИ
17. Планирование работ по защите информации
18. Реализация требований по ТЗКИ
19. Способы и средства защиты информации, обрабатываемой техническими средствами
20. Способы и средства защиты персональных данных, обрабатываемых в ИС
21. Способы и средства ограничения полномочий и разрешений пользователей баз данных
22. Технические и программные средства защиты информации от НСД
23. Технические каналы утечки информации
24. Технические средства обработки информации
25. Требования по защите информации и созданию системы защиты
26. информации
27. Управление ключевой информацией. Удостоверяющий центр
28. Установка, настройка и использование средств криптографической защиты

29. Формирование требований по защите информации и созданию системы защиты
30. Цели и задачи технической защиты информации