АННОТАЦИЯ

дисциплины

«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – специалист по защите информации

Специализация – «Информационная безопасность автоматизированных систем на транспорте»

**1. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «Информационная безопасность» (Б1.Б.16) относится к вариативной части Блока 1 и является обязательной.

**2. Цель и задачи дисциплины**

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других базовых дисциплин вариативной части первого блока в соответствии с требованиями, установленными федеральным государственным образовательным стандартом (приказ Минобрнауки России от 1.12.2016 № 1509 для формирования у выпускника профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности: научно-исследовательская, проектная, контрольно-аналитическая, организационно-управленческая, эксплуатационная и специализацией «Информационная безопасность автоматизированных систем на транспорте»

Для достижения поставленной цели решаются следующие задачи:

* подготовка обучающегося по разработанной в университете основной профессиональной образовательной программе к успешной аттестации планируемых конечных результатов освоения дисциплины;
* подготовка обучающегося к освоению дисциплины " Комплексное обеспечение информационной безопасности автоматизированных систем";

развитие социально-воспитательного компонента учебного процесса.

**3. Перечень планируемых результатов обучения по дисциплине**

Изучение дисциплины направлено на формирование следующих компетенций: ОПК-6, ПК-1, 4, 16, 21, 23.

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

* основы российской правовой системы и законодательства;
* основы правового статуса личности;
* характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ;
* основные меры по защите информации в АС (организационные, правовые);
* методы аттестации уровня защищенности АС;
* нормативно-правовую базу обеспечения ИБ;
* основные отечественные и зарубежные стандарты в области ИБ;
* принципы формирования политики ИБ;
* основные понятия и содержание организационного обеспечения ИБ АС;
* основы комплексного обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте;
* акты в области обеспечения информационной безопасности и нормативные, методические документы ФСБ России и ФСТЭК России в области защиты информации;
* правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
* организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
* основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
* основные методы управления информационной безопасностью;
* принципы формирования политики информационной безопасности в автоматизированных системах.

УМЕТЬ:

* использовать в практической деятельности правовые знания;
* анализировать правовые акты и осуществлять правовую оценку информации;
* предпринимать необходимые меры по восстановлению нарушенных прав;
* определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
* разрабатывать модели угроз и нарушителей ИБ АС;
* разрабатывать предложения по совершенствованию системы управления ИБ АС;
* разрабатывать проекты нормативных и методических документов, регламентирующих работы по обеспечению ИБ АС;
* используя современные методы и средства, разрабатывать и оценивать модели и политики безопасности автоматизированных и информационно-управляющих систем на железнодорожном транспорте;
* проводить мониторинг угроз безопасности компьютерных сетей;
* реализовывать политику безопасности баз данных;
* применять средства обеспечения безопасности данных;
* классифицировать защищаемую информацию по видам и грифам секретности (конфиденциальности);
* анализировать и оценивать угрозы информационной безопасности объекта;
* определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
* разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;
* выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем;
* оценивать информационные риски в автоматизированных системах;
* определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
* составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;
* разрабатывать частные политики информационной безопасности автоматизированных систем;
* контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;
* разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.

ВЛАДЕТЬ:

* навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
* методами оценки информационных рисков;
* навыками анализа угроз и уязвимостей информационной безопасности в автоматизированных и информационно-управляющих системах на железнодорожном транспорте;
* навыками анализа угроз и навыками построения политик безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем железнодорожного транспорта;
* профессиональной терминологией в области информационной безопасности;
* навыками безопасного использования технических средств в профессиональной деятельности;
* навыками работы с нормативными правовыми актами;
* навыками организации и обеспечения режима секретности;
* методами организации и управления деятельностью служб защиты информации на предприятии;
* методами формирования требований по защите информации.

**4. Содержание и структура дисциплины**

|  |
| --- |
| Российское законодательство в области информационной безопасности |
| Защита информации с ограниченным доступом |
| Правовые режимы защиты информаци |
| Защита интеллектуальной собственности |
| Организационные системы обеспечения безопасности информации |
| Корпоративное нормативное регулирование |
| Организация объектовых режимов безопасности |
| Система подготовки кадров в области информационной безопасности в Российской Федерации |
| Российское законодательство в области информационной безопасности |
| Защита информации с ограниченным доступом |
| Правовые режимы защиты информаци |

.

**5. Объем дисциплины и виды учебной работы**

Для очной формы обучения:

Объем дисциплины – 4 зачетные единицы (144 час.), в том числе:

лекции – 16 час.

практические занятия – 32 час.

самостоятельная работа – 60 час.

контроль – 36 час.

Форма контроля знаний – экзамен.