





1. Цели и задачи дисциплины

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным «1» декабря 2016г. №1509 по направлению 10.00.00 «Информационная безопасность», по дисциплине «Основы информационной безопасности».

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других базовых дисциплин первого блока в соответствии с требованиями, установленными федеральным государственным образовательным стандартом (приказ Минобрнауки России от 1.12.2016 № 1509) для формирования у выпускника общекультурных и 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 сетей и 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.
1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Планируемыми результатами обучения по дисциплине являются: приобретение знаний, умений, навыков и/или опыта деятельности.

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

* основы обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта;
* 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;
* основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
* основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);
* основные методы управления информационной безопасностью;
* принципы формирования политики информационной безопасности в телекоммуникационных системах.

УМЕТЬ:

* классифицировать защищаемую информацию по видам информации ограниченного доступа;
* классифицировать и оценивать информационные угрозы для объекта информатизации;
* пользоваться нормативными документами по противодействию технической разведке;
* анализировать и оценивать информационные угрозы объекта информатизации;
* 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 автоматизированных систем;
* составлять аналитические обзоры по вопросам обеспечения 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 анализа угроз и уязвимостей информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте;
* 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.

Приобретенные знания, умения, навыки и/или опыт деятельности, характеризующие формирование компетенций, осваиваемые в данной дисциплине, позволяют решать профессиональные задачи, приведенные в соответствующем перечне по видам профессиональной деятельности в п. 2.4 основной профессиональной образовательной программы (ОПОП).

Изучение дисциплины направлено на формирование следующих общекультурных компетенций (ОК):

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5).

Изучение дисциплины направлено на формирование следующих профессиональных компетенций (ПК), соответствующих видам

профессиональной деятельности, на которые ориентирована программа специалитета:

* научно-исследовательская деятельность:

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4).

* проектно-конструкторская деятельность:

способностью участвовать в разработке защищенных

автоматизированных систем в сфере профессиональной деятельности (ПК-9);

способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11).

* контрольно-аналитическая деятельность:

способностью участвовать в проведении экспериментально­исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16).

- организационно-управленческая деятельность:

Способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22).

* эксплуатационная деятельность:
* способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);
* способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);
* способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27).

Сформированность компетенций у обучающихся проверяется на различных этапах их формирования в соответствии с Фондами оценочных средств по дисциплинам и практикам учебного плана. Государственная итоговая аттестация направлена на проверку сформированности у обучающегося следующих компетенций: ОК-5, ПК-4, ПК-9, ПК-11, ПК-16, ПК-22, ПК-24, ПК-25, ПК-27.

Область профессиональной деятельности обучающихся, освоивших данную дисциплину, приведена в п. 2.1 ОПОП.

Объекты профессиональной деятельности обучающихся, освоивших данную дисциплину, приведены в п. 2.2 ОПОП.

1. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Основы информационной безопасности» (Б1.Б.11) относится к базовой части Блока 1 и является обязательной дисциплиной обучающегося.

1. Объем дисциплины и виды учебной работы

|  |  |  |
| --- | --- | --- |
| Вид учебной работы | Всего часов | Семестр |
| IV |
| Контактная работа (по видам учебных занятий) | 68 | 68 |
| В том числе:- лекции (Л) | 34 | 34 |
| - практические занятия (ПЗ) | 34 | 34 |
| - лабораторные работы (ЛР) | - | - |
| Самостоятельная работа (СРС) (всего) | 40 | 40 |
| Контроль | - | - |
| Форма контроля знаний | 3 | 3 |
| Общая трудоемкость: час / з.е. | 108/3 | 108/3 |

1. Содержание и структура дисциплины

**5.1 Содержание дисциплины**

|  |  |  |
| --- | --- | --- |
| №п/п | Наименование раздела дисциплины | Содержание раздела |
| 1. | Понятие национальной безопасности | Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание. |
| 2. | Информационная безопасность в системе национальной безопасностиРоссийской Федерации | Основные понятия, общеметодологические. Принципы обеспечения информационной безопасности. Национальные интересы в информационной сфере. Источники и содержание угроз в информационной сфере |
| 3. | Государственная информационная политика | Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности. |
| 4. | Информация – наиболее ценный ресурс современного общества | Понятие «информационный ресурс». Классы информационных ресурсов |
| 5. | Угрозы информации | Классы каналов несанкционированного получения информации Причины нарушения целостности информации Виды угроз информационным системам Виды потерь. Информационные инфекции Убытки, связанные с информационным обменом Модель нарушителя информационных систем |
| 6. | Проблемы информационной войны | Информационное оружие и его классификация. [Информационная война](#bookmark7) |
| 7. | Проблемы информационной безопасности в сфере государственного и муниципального управления | Информационные процессы в сфере государственного и муниципального управления. Виды информации и информационных ресурсов в сфере ГМУ.Состояние и перспективы информатизации сферы ГМУ |
| 8. | Система подготовки кадров в области информационной безопасности в Российской Федерации | Структура системы подготовки кадров в области информационной безопасности Состав учебно-методического обеспечения системы и ее подсистема управления Основные направления учебной деятельности |
| 9. | Анализ существующих методик определения требований к защите информации | Требования к безопасности информационных систем в США. Требования к безопасности информационных систем в России. Классы защищенности средств вычислительной техники от несанкционированного доступа. Оценка состояния безопасности ИС Франции. Факторы, влияющие на требуемый уровень защиты информации. Критерии оценки безопасности информационных технологий. |
| 10. | Способы и средства защиты информации | Правовые, организационные, технические, программно-аппаратные. |
| 11. | Методы и модели оценки уязвимости информации | Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита» |

**5.2 Разделы дисциплины и виды занятий**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №п/п | Наименование раздела дисциплины | Л | ПЗ | ЛР | СРС |
| 1. | Понятие национальной безопасности | 2 | 2 | - | 2 |
| 2. | Информационная безопасность в системе национальной безопасности Российской Федерации | 2 | 2 | - | 2 |
| 3. | Государственная информационная политика | 4 | 4 | - | 4 |
| 4. | Информация - наиболее ценный | 2 | 2 | - | 2 |
|  | ресурс современного общества |  |  |  |  |
| 5. | Угрозы информации | 6 | 6 | - | 4 |
| 6. | Проблемы информационной войны | 2 | 2 | - | 2 |
| 7. | Проблемы информационной безопасности в сфере государственного и муниципального управления | 2 | 2 | - | 2 |
| 8. | Система подготовки кадров в области информационной безопасности в Российской Федерации | 2 | 2 | - | - |
| 9. | Анализ существующих методик определения требований к защите информации | 4 | 4 | - | 8 |
| 10. | Способы и средства защиты информации | 4 | 4 | - | 8 |
| 11. | Методы и модели оценки уязвимости информации | 4 | 4 | - | 6 |
| Итого | 34 | 34 | - | 40 |

1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

|  |  |  |
| --- | --- | --- |
| №п/п | Наименование раздела дисциплины | Перечень учебно-методического обеспечения |
| 1. | Понятие национальной безопасности | Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", ГОСТ Р 50922-2006 С истема ГАРАНТ: http://base.garant.rU/12148555 /#ixzz3Q6X8uNT J |

|  |  |  |
| --- | --- | --- |
| 2. | Информационная безопасность в системе национальной безопасности Российской Федерации | Доктрина информационной безопасности; Стратегия национальной безопасности; Закон РФ от 21.07.1993 N 5485-1 (ред. от 21.12.2013) "О государственной тайне" (21 июля 1993 г.) Система Консультант Плюс http://www.consultant.ru/ document/cons doc LAW 156018/ |
| 3. | Государственная информационная политика | 1. А. Тихонов, В.В. Райх Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. М.: Гелиос АРВ, 2012. 528с., ил.
2. Н. Семкин, А.Н. Семкин Основы правового обеспечения защиты информации: Учебное пособие для ВУЗов. - М.: Горячая линия-Телеком, 2010. М.: «Гелиос- АРВ», 2010. -239 с.: ил.

А.А. Малюк, В.С. М.: Научно-техническое издательство «Горячая линия Горбатов, В.И. Королев и др. Введение в информационную безопасность: Учебное пособие для вузов. - Телеком», 2014. 288 с. |
| 4. | Информация - наиболее ценный ресурс современного общества | Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Основы информационной безопасности. Учебное пособие для вузов / - М.: Горячая линия - Телеком, 2006. - 544 с.: ил.httD://www.1variant.ru/2011-10-27-22-57-07/175-2014-02-10- 10-02-40/1870--4-4-2014-43.html |
| 5. | Угрозы информации | ГОСТ Р 51275-2006 |
| 6. | Проблемы информационной войны | Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" Система ГАРАНТ: http://base.garant.ru/12148555/#ixzz3Q6X8uNT J |
| 7. | Проблемы информационной безопасности в сфере государственного и муниципального управления | Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" Система ГАРАНТ: http://base.garant.ru/12148555/#ixzz3Q6X8uNT J |
| 8. | Анализ существующих методик определения требований к защите информации | Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Основы информационной безопасности. Учебное пособие для вузов / - М.: Горячая линия - Телеком, 2006. - 544 с.: ил.http://www.1variant.ru/2011-10-27-22-57-07/175-2014-02- 10- 10-02-40/1870--4-4-2014-43.htm |

|  |  |  |
| --- | --- | --- |
| 9. | Способы и средства защиты информации | Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Основы информационной безопасности. Учебное пособие для вузов / - М.: Горячая линия - Телеком, 2006. - 544 с.: ил. |
| 10 | Методы и модели оценки уязвимости информации | Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Основы информационной безопасности. Учебное пособие для вузов / - М.: Горячая линия - Телеком, 2006. - 544 с.: ил. |

1. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств по дисциплине является неотъемлемой частью рабочей программы и представлен отдельным документом, рассмотренным на заседании кафедры и утвержденным заведующим кафедрой.

1. Перечень основной и дополнительной учебной литературы, нормативно-правовой документации и других изданий, необходимых для освоения дисциплины
	1. **Перечень основной учебной литературы, необходимой для освоения дисциплины**
2. Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Основы информационной безопасности. Учебное пособие для вузов / - М.: Горячая линия - Телеком, 2006. – 544 с.: ил. Режим доступа: http://www.1variant.ru/ 2011-10-27-22-57-07/175-2014-02-10-10-02-40/1870--4- 4-2014-43.html
3. С.П. Расторгуев. Основы информационной безопасности. Учебное пособие для вузов / - М.: Издательский Центр - «Академия», 2008. – 192 с.: Режим доступа: http://www.telecomlaw.ru/studyguides/orgprav straa.pdf
4. В.А. Тихонов, В.В. Райх Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. М.: Гелиос АРВ, 2012. 528с.
5. С.Н. Семкин, А.Н. Семкин Основы правового обеспечения защиты информации: Учебное пособие для ВУЗов. - М.: Горячая линия- Телеком, 2008. М.: «Гелиос-АРВ», 2010. -239 с.: ил.
6. А.А. [Малюк,](http://www.techbook.ru/book_list.php?str_author=%d0%a0%d1%9a%d0%a0%c2%b0%d0%a0%c2%bb%d0%a1%d0%8b%d0%a0%d1%94%20%d0%a0%d1%92.%20%d0%a0%d1%92.) В.С. Горбатов, В.И. [Королев и](http://www.techbook.ru/book_list.php?str_author=%d0%a0%d1%99%d0%a0%d1%95%d0%a1%d0%82%d0%a0%d1%95%d0%a0%c2%bb%d0%a0%c2%b5%d0%a0%d0%86%20%d0%a0%e2%80%99.%20%d0%a0%c2%98.) др. Введение в информационную безопасность: Учебное пособие для вузов. М.: Научно­техническое издательство «Горячая линия - Телеком», 2014. 288 с.
	1. **Перечень дополнительной учебной литературы, необходимой для освоения дисциплины**
7. Конституция Российской Федерации. // Российская газета № 7 от 22.12.2008г.
8. Закон Российской Федерации № 2446-1 от 5.03.1992г. «О безопасности». // Российская газета от 22.02.1995г.
9. Концепция национальной безопасности Российской Федерации. // Российская газета от 26.12.1997г.
10. Доктрина информационной безопасности Российской Федерации. // Российская газета от 05.12.2016г.
11. В.А. Кулишкин Краткий курс лекций по дисциплине «Основы информационной безопасности»: Учебное пособие. - СПб.: ПГУПС, 2008.­232 с.
	1. **Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**
12. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) - [Электронный ресурс] - Режим доступа: (http://fstec.ru/);
13. Электронный фонд нормативно-правовой документации. [Электронный ресурс] – Режим доступа: http://docs.cntd.ru/search/intellectual?q=% D0%93%D0%9E%D0%A1%D0%A2+%D0%A0+56205-2014+&itemtype;
14. Официальный сайт информационной сети ТЕХЭКСПЕРТ

[Электронный ресурс] - Режим доступа: http://www.cntd.ru/**,** свободный;

1. Официальный сайт технического комитета по разработке ГОСТов по информационной безопасности - [Электронный ресурс] - Режим доступа: (http://tk.gost.ru/wps/portal/tk362);
2. Информационно-поисковая система «МИМОЗА» (База данных о изобретениях и полезных моделях с 1994 г. по н.в.) (Установлена на компьютере преподавателя в ауд. 2/110);
3. Базу данных «Система ГОСТов по обеспечению информационной безопасности» (Свидетельство о государственной регистрации базы данных №2014621325 от 18.09.2014
	1. **Методические указания для обучающихся по освоению дисциплины**
4. В.А. Кулишкин Аттестация объектов информатизации по требованиям безопасности конфиденциальной информации: Учебное пособие (Методические указания по выполнению лабораторных работ). - СПб.: ПГУПС, 2006, 40 с.;
5. В.А. Кулишкин Организационное обеспечение информационной безопасности: Методические указания для выполнения лабораторных работ. - СПб.: ПГУПС, 2009, 87 с.;
6. В.А. Кулишкин Разработка организационно-распорядительных документов: Учебное пособие (Методические указания по выполнению лабораторных работ). - СПб.: ПГУПС, 2010, 65 с.;
7. В.А. Кулишкин Разработка должностных инструкций: Учебное пособие. - СПб.: ПГУПС, 2014, 100 с. Электронный вариант. База данных менеджмент образовательного процесса на кафедре;
8. В.А. Кулишкин Деловая игра «Аттестация объектов информатизации»: Учебное пособие. - СПб.: ПГУПС, 2012, 29 с.
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины
10. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) - [Электронный ресурс] - Режим доступа: (http://fstec.ru/);
11. Официальный сайт технического комитета по разработке ГОСТов по информационной безопасности - [Электронный ресурс] - Режим доступа: (http://tk.gost.ru/wps/portal/tk362);
12. Электронный фонд нормативно-правовой документации.

[Электронный ресурс] – Режим доступа: (http://docs.cntd.ru/search/ intellectual?q=%D0%93%D0%9E%D0%A1%D0%A2+%D0%A0+56205-2014+ &itemtype;

1. Система ГАРАНТ: http: //base.garant.ru/12148555/#ixzz3 Q6X8uNT J;
2. Система Консультант Плюс http://www.consultant.ru/document /cons doc LAW 156018/.
3. Методические указания для обучающихся по освоению дисциплины

Порядок изучения дисциплины следующий:

1. Освоение разделов дисциплины производится в порядке, приведенном в разделе 5 «Содержание и структура дисциплины». Обучающийся должен освоить все разделы дисциплины с помощью учебно-методического обеспечения, приведенного в разделах 6, 8 и 9 рабочей программы.
2. Для формирования компетенций обучающийся должен представить выполненные типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, предусмотренные текущим контролем (см. фонд оценочных средств по дисциплине).
3. По итогам текущего контроля по дисциплине, обучающийся должен пройти промежуточную аттестацию (см. фонд оценочных средств по дисциплине).
4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине:

* персональные компьютеры, локальная вычислительная сеть кафедры, проектор;
* методы обучения с использованием информационных технологий: компьютерный лабораторный практикум, демонстрация мультимедийных материалов;
* лабораторное программное обеспечение, разрабатываемое в ходе учебного процесса студентами совместно с преподавателем;
* Интернет-сервисы и электронные ресурсы: сайты, перечисленные в разделе 9 рабочей программы; электронные учебно-методические материалы, доступные через личный кабинет обучающегося на сайте sdo.pgups.ru; на выбор обучающегося - поисковые системы, профессиональные, тематические чаты и форумы, системы аудио и видео конференций, онлайн-энциклопедии и справочники.

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:

* Microsoft Windows 7;
* Office Standard 2010 Russian OpenLicensePack NoLevel AcademicEdition;
* Adobe Acrobat Reader DC (бесплатное, свободно распространяемое программное обеспечение; режим доступа <https://get.adobe.com/ru/reader/>);
* Visual Studio Professional 2010 Russian OLP NL AcademicEdition;
* Oracle Java SE Development Kit 8 (бесплатное, свободно распространяемое программное обеспечение; режим доступа <http://www.oracle.com/technetwork/java/javase/downloads/index.html>);
* NetBeans IDE 8.2 (бесплатное, свободно распространяемое программное обеспечение; режим доступа <https://netbeans.org/downloads/>).
1. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Материально-техническая база обеспечивает проведение всех видов учебных занятий, предусмотренных учебным планом по данной специальности, и соответствует действующим санитарным и противопожарным нормам и правилам.

Она содержит специальные помещения, укомплектованных специализированной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Материально-техническая база дисциплины включает:

* + - * помещения для проведения лекционных занятий, укомплектованные наборами демонстрационного оборудования (стационарными или переносными персональными компьютерами, настенными или переносными экранами, мультимедийными проекторами с дистанционным управлением и другими информационно-демонстрационными средствами) и учебно-наглядными пособиями (презентациями), обеспечивающими тематические иллюстрации в соответствии с рабочей программой дисциплины;
			* лабораторию информационной безопасности информационно-коммуникационных систем (ауд. 2-104), оснащенную программно-аппаратными средствами защиты информации в соответствии с требованиями ФГОС ВО; лаборатория также оборудована современной вычислительной техникой, комплектом проекционного оборудования для преподавателя;
			* помещения для выполнения курсовой работы, оснащенные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых для выполнения индивидуального задания программных средств (см. раздел 11), а также комплектом оборудования для печати;
			* помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации;
			* помещения для проведения групповых и индивидуальных консультаций, укомплектованные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых программных средств (см. раздел 11);
			* помещения для проведения текущего контроля и промежуточной аттестации.



Разработчик программы, доцент В.А. Кулишкин

«16» января 2017 г.