Учреждение образования
«Белорусский государственный университет транспорта»

Электротехнический факультет

Кафедра «Системы передачи информации»

СОГЛАСОВАНО
Заведующий кафедрой
_____ Шевчук В.Г.
30.03.2018 г.

СОГЛАСОВАНО
Декан электротехнического факультета
_____ Сатырев Ф.Е.
28.03.2018 г.

СОГЛАСОВАНО
Декан заочного факультета
_____ Пигунов В.В.
30.03.2018 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ИНФОРМАЦИОННОАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

для специальности

1-37 02 04 «Автоматика, телемеханика и связь на железнодорожном транспорте»
специализации 1-37 02 04 01 «Автоматика и телемеханика»

СОСТАВИТЕЛЬ:
П.М. Буй, доцент кафедры «Системы передачи информации»

Рассмотрено и утверждено на заседании кафедры «Системы передачи информации» «20» марта 2018 г. протокол № 3.

Рассмотрено и утверждено методической комиссией электротехнического факультета «28» марта 2018 г. протокол № 2.

Рассмотрено и утверждено методической комиссией заочного факультета «30» марта 2018 г. протокол № 3.

ОГЛАВЛЕНИЕ

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Краткая характеристика. Учебно-методический комплекс дисциплины (далее – УМКД) совокупность нормативно-методических документов и учебно-программных материалов, обеспечивающих реализацию дисциплины в образовательном процессе и способствующих эффективному освоению студентами учебного материала, а также средства компьютерного моделирования и интерактивные учебные задания для тренинга, средства контроля знаний и умений обучающихся.

УМКД «Информационная безопасность систем автоматики и телемеханики» разработан с целью унификации учебно-методического обеспечения и повышения качества учебного процесса для студентов дневной формы обучения специальности «Автоматика, телемеханика и связь на железнодорожном транспорте» специализации «Автоматика и телемеханика».

Требования к дисциплине.

В последнее время наблюдается резкое увеличение вычислительной мощности современных компьютеров при одновременном упрощении их эксплуатации, а также резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с их помощью в современных системах автоматики и телемеханики. Кроме того, в системах автоматики и телемеханики постоянно расширяется круг пользователей, имеющих непосредственный доступ к управлению и к массивам данных, повсеместно используются сетевые технологии, происходит объединение локальных сетей в глобальные, применяется удаленное управление. В связи с этим все более актуальным становится вопрос о защите информации в системах управления на транспорте и, в частности, в системах автоматики и телемеханики. Важными задачами являются анализ причин возникновения каналов утечки информации, определение методов и средств их блокировки, а также грамотная организация и построение комплексной системы информационной безопасности для систем автоматики и телемеханики. Поэтому важно, чтобы в процессе обучения студент освоил современные методы обеспечения информационной безопасности таких систем в условиях возникновения угроз.

Целью преподавания дисциплины «Информационная безопасность систем автоматики и телемеханики» является получение студентами базовых знаний по вопросам обеспечения информационной безопасности управляющих систем на транспорте в условиях возникновения угроз различных по виду, происхождению и характеру.

Основными задачами изучения дисциплины являются:

– изучение причин возникновения каналов несанкционированного доступа и утечки информации, методов и средств их блокировки;

– получение знаний о принципах организации и построения комплексной системы защиты информации в управляющих системах на транспорте.

Содержание дисциплины представлено в виде тем, которые характеризуются относительно самостоятельными укрупненными дидактическими единицами содержания обучения. Содержание тем опирается на приобретенные ранее студентами компетенции при изучении естественнонаучной дисциплины «Математика».

Дисциплина «Информационная безопасность систем автоматики и телемеханики» излагается посредством чтения лекций, проведения практических занятий.

При создании УМКД «Информационная безопасность систем автоматики и телемеханики» использовались следующие нормативные документы:

– Положение об учебно-методическом комплексе (УМК) № П-44-2010 от 06.10.2010;

– Положением о первой ступени высшего образования (утв. 18.01.2008 г. №68);

– Общегосударственным классификатором Республики Беларусь «Специальности и квалификации» ОКРБ 011-2009;

– образовательными стандартами по специальностям высшего образования;

– Порядком разработки, утверждения и регистрации учебных программ для первой ступени высшего образования (утв. Министром образования Республики Беларусь 2010г.).

2 ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

2.1 Перечень теоретического материала

1. Яковлев, В. В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта / В. В. Яковлев, А. А. Корниенко // Учебник для ВУЗов ж.-д. транспорта. – М.: УМК МПС России, 2002. – 328 с.
(Печатный вариант на кафедре)

2. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М.: Радио и связь, 2001. – 376с.
(Электронный вариант на кафедре)

3. Мао, Венбо Современная криптография: теория и практика / Венбо Мао // Пер с англ. – М.: Издательский дом «Вильямс», 2005. – 768с.
(Электронный вариант на кафедре)

4. Смит, Ричард Э. Аутентификация: от паролей до открытых ключей / Ричард Э. Смит. – М.: Издательский дом «Вильямс», 2002. – 432с.
(Электронный и печатный варианты на кафедре)

5. Буй, П.М. Криптографические методы защиты информации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в телекоммуникацииооных системах» / П.М. Буй, В.О. Матусевич. – Гомель : БелГУТ, 2010. – 56 с.
(Издана тиражем 150 экземпляров, имеется в библиотеке университета и на кафедре)

6. Буй, П.М. Средства аутентификации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в системах управления на транспорте» / П.М. Буй, Д.Д. Семиход. – Гомель : БелГУТ, 2010. – 39 с.
(Издана тиражем 150 экземпляров, имеется в библиотеке университета и на кафедре)

7. Белоусова, Е.С. Политика безопасности информационных систем : учеб.-метод. пособие для практ. работ / Е.С. Белоусова, П.М. Буй. – Гомель : БелГУТ, 2016. – 38 с.
(Издана тиражем 200 экземпляров, имеется в библиотеке университета и на кафедре)

8. Домарев, В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К.: ООО «ТИД “ДС”», 2001. – 688с.
(Электронный вариант на кафедре)

3 ПРАКТИЧЕСКИЙ РАЗДЕЛ

3.1 Перечень практических работ

1 Анализ угроз безопасности информационной системы;

2 Количественная оценка рисков информационной безопасности;

3 Качественная оценка рисков информационной безопасности;

4 Модель нарушителя информационной безопасности системы автоматики и телемеханики;

5 Правила разграничения доступа;

6 Обеспечение конфиденциальности, доступности и целостности информации в системе автоматики и телемеханики;

7 Изучение СТБ 34.101.1, СТБ 34.101.2 и СТБ 34.101.3;

8 Анализ структуры задания по безопасности;

9 Оценка симметричных методов шифрования в системах автоматики и телемеханики;

10 Оценка асимметричных методов шифрования в системах автоматики и телемеханики;

11 Формирование электронно-цифровой подписи документа;

12 Исследование методов управления криптографическими ключами;

13 Исследование показателей эффективности парольных средств аутентификации в системах автоматики и телемеханики;

14 Исследование показателей эффективности биометрических средств аутентификации в системах автоматики и телемеханики;

15 Исследование показателей эффективности комбинированных средств аутентификации в системах автоматики и телемеханики;

16 Обеспечение информационной безопасности критически важных объектов информатизации;

17 Политика безопасности информационной системы.

3.2 Учебно-методический материал по выполнению лабораторных, практических работ и расчетно-графической работы

1. Буй, П.М. Криптографические методы защиты информации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в телекоммуникацииооных системах» / П.М. Буй, В.О. Матусевич. – Гомель : БелГУТ, 2010. – 56 с.

(Издана тиражем 150 экземпляров, имеется в библиотеке университета и на кафедре)

2. Буй, П.М. Средства аутентификации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в системах управления на транспорте» / П.М. Буй, Д.Д. Семиход. – Гомель : БелГУТ, 2010. – 39 с.

(Издана тиражем 150 экземпляров, имеется в библиотеке университета и на кафедре)

3. Белоусова, Е.С. Политика безопасности информационных систем : учеб.-метод. пособие для практ. работ / Е.С. Белоусова, П.М. Буй. – Гомель : БелГУТ, 2016. – 38 с.

(Издана тиражем 200 экземпляров, имеется в библиотеке университета и на кафедре)

4 РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

4.1 Вопросы к зачету

1. Дайте понятие защищаемой информации
2. Дайте понятие защите информации
3. Дайте понятие эффективности защиты информации
4. Дайте понятие системы защиты информации
5. Дайте понятие средства защиты информации
6. Дайте понятие угрозы безопасности объекта
7. Дайте понятие уязвимости объекта
8. Дайте понятие источника угрозы
9. Дайте понятие атаки
10. Что такое конфиденциальность информации?
11. Что такое целостность информации?
12. Что такое доступность информации?
13. Какая из перечисленных угроз относится к угрозам против конфиденциальности информации?
14. Какая из перечисленных угроз относится к угрозам против доступности информации?
15. Какая из перечисленных угроз относится к угрозам против целостности информации?
16. Какая классификация источников угроз является общепризнанной?
17. Какая классификация уязвимостей объекта защиты является общепризнанной?
18. Какой из приведенных источников угроз относится к антропогенным?
19. Какой из приведенных источников угроз относится к техногенным?
20. Какой из приведенных источников угроз относится к стихийным?
21. Какой из перечисленных источников угроз является антропогенным внешним?
22. Какой из перечисленных источников угроз является антропогенным внутренним?
23. Какой из перечисленных источников угроз является техногенным внешним?
24. Какой из перечисленных источников угроз является техногенным внутренним?
25. Что такое модель нарушителя информационной безопасности?
26. Какой из перечисленный видов нарушителей информационной безопасности относится к внутренним?
27. Какой из перечисленный видов нарушителей информационной безопасности не относится к внутренним?
28. Какой из перечисленный видов нарушителей информационной безопасности относится к внешним?
29. Какой из перечисленный видов нарушителей информационной безопасности не относится к внешним?
30. Что из перечисленного относится к аппаратным методам защиты информации?

31. Что из перечисленного относится к программным методам защиты информации?

32. Что из перечисленного относится к организационным методам защиты информации?

33. Что из перечисленного представляет собой систему взглядов относительно направлений, средств и способов защиты жизненно важных интересов личности, общества и государства для Республики Беларусь?

34. Какой закон является основополагающим в Республике Беларусь в сфере защиты информации?

35. Какой закон направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе?

36. Какой закон определяет правовые основы, принципы, основные задачи и направления деятельности органов государственной безопасности Республики Беларусь?

37. Какой закон определяет правовые и организационные основы отнесения сведений к государственным секретам, защиты государственных секретов, осуществления иной деятельности в сфере государственных секретов в целях обеспечения национальной безопасности Республики Беларусь?

38. Как раскрывается аббревиатура ОАЦ в сфере защиты информации?

39. Какая серия стандартов Республики Беларусь в настоящее время охватывает большую часть вопросов по защите информации?

40. Что такое сертификация?

41. Что такое сертификат соответствия?

42. Что такое государственная экспертиза?

43. Что такое аттестация объектов информатизации по требованиям безопасности информации?

44. Как называется стандарт Республики Беларусь 34.101.1-2004?

45. Как называется стандарт Республики Беларусь 34.101.2-2004?

46. Как называется стандарт Республики Беларусь 34.101.3-2004?

47. Какой номер имеет стандарт Республики Беларусь «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Введение и общая модель»?

48. Какой номер имеет стандарт Республики Беларусь «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Функциональные требования безопасности»?

49. Какой номер имеет стандарт Республики Беларусь «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Гарантийные требования безопасности»?

50. Что из перечисленного является методом криптографического преобразования информации?

51. Что из перечисленного не является методом криптографического преобразования информации?

52. Какой из представленных алгоритмов относится к симметричным криптосистемам?

53. Какой из представленных алгоритмов относится к асимметричным криптосистемам?

54. Какой из представленных алгоритмов используется при создании электронной цифровой подписи?

55. Какой из представленных алгоритмов не относится к классическим симметричным криптосистемам?

56. К какому классу алгоритмов шифрования относится шифрование Цезаря?

57. К какому классу алгоритмов шифрования относится шифрование таблицами Вижинера?

58. К какому классу алгоритмов шифрования относится шифрование алгоритмом DES?

59. К какому классу алгоритмов шифрования относится шифрование алгоритмом RSA?

60. Для чего используется алгоритм Эль Гамаля?

61. Для чего используется алгоритм Диффи-Хеллмана?

62. Сколько циклов шифрования содержит алгоритм DES?

63. Какова длина ключа DES?

64. Какова длина информационного блока, шифрующегося алгоритмом DES?

65. Какое из перечисленных средств аутентификации относится к средствам, базирующимся на условных, заранее присваиваемых признаках (сведениях), известных субъекту?

66. Какое из перечисленных средств аутентификации относится к средствам, базирующимся на физических средствах, действующих аналогично физическому ключу?

67. Какое из перечисленных средств аутентификации относится к средствам, базирующимся на индивидуальных характеристиках субъекта, его физических данных, позволяющих выделить его среди других лиц?

68. Какое из перечисленных средств аутентификации относится к биометрическим?

69. Какое из перечисленных средств аутентификации не относится к биометрическим?

70. Определите вероятность подбора с первой попытки пароля длиной k символов алфавита A.

71. Определите вероятность подбора с десятой попытки пароля длиной k символов алфавита A.

72. Определите вероятность подбора за десять попыток пароля длиной k символов алфавита A.

73. Определите вероятность подбора с первой попытки PIN-кода длиной k символов.

74. Определите вероятность подбора с десятой попытки PIN-кода длиной k символов.

75. Определите вероятность подбора за десять попыток PIN-кода длиной k символов.

4.2 Критерии выставления контрольных сроков

В качестве критериев выставления оценок по контрольным срокам используются:

- посещаемость практических занятий;
- выполнение практических заданий;
- защита отчетов по практическим работам;
- участие студентов в НИРС.

Оценки первого и второго контрольных сроков

Отметка	Обоснование
10 (А)	Отсутствие пропусков занятий без уважительных причин, выполнение всех положенных к контрольному сроку практических заданий, защита отчетов по всем выполненным практическим работам, выраженная способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации (в частности активность студента в рамках НИРС)
9	Отсутствие пропусков занятий без уважительных причин, выполнение всех положенных к контрольному сроку практических заданий, защита отчетов по всем выполненным практическим работам, выраженная способность самостоятельно и творчески решать сложные проблемы в рамках тем изучаемой дисциплины
8	Отсутствие пропусков занятий без уважительных причин, выполнение всех положенных к контрольному сроку практических заданий и защита отчетов по всем выполненным практическим работам
7	Пропуск по неуважительным причинам менее 25% занятий и выполнение более 75% положенных к контрольному сроку практических заданий, защита отчетов по выполненным практическим работам
6	Пропуск по неуважительным причинам менее 25% занятий или выполнение более 75% положенных к контрольному сроку практических заданий с защитой отчетов по выполненным практическим работам
5	Пропуск по неуважительным причинам менее 25% занятий, выполнение более 75% положенных к контрольному сроку практических заданий, защита хотя бы одного отчета по практической работе
4	Пропуск по неуважительным причинам менее 50% занятий, выполнение более 50% положенных к контрольному сроку практических заданий, защита хотя бы одного отчета по практической работе
3	Пропуск по неуважительным причинам менее 25% занятий и выполнение без защиты более 75% положенных к контрольному сроку практических заданий
2	Пропуск по неуважительным причинам менее 25% занятий и выполнение без защиты более 50% положенных к контрольному сроку практических заданий
1	Пропуск по неуважительным причинам менее 50% занятий и выполнение без защиты более 50% положенных к контрольному сроку практических заданий
0	Пропуск по неуважительным причинам более 50% занятий или выполне-

	ние без защиты менее 50% положенных к контрольному сроку практических заданий
Не аттестован	Студент не подлежит аттестации по данной дисциплине

5 ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ

5.1 Учебная программа «Информационная безопасность систем автоматики и телемеханики» №20.37/уч от 30.05.2017 г

Учреждение образования
«Белорусский государственный университет транспорта»

УТВЕРЖДАЮ
Первый проректор
учреждения образования
«Белорусский государственный
университет транспорта
_____ Ю.Г. Самодум
«30» «05» 2017
Регистрационный № УД- 20.37 /уч.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-37 02 04 Автоматика, телемеханика и связь на железнодорожном транспорте
специализации:
1-37 02 04 01 Автоматика и телемеханика

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ»
СПЕЦИАЛИЗАЦИИ 1-37 02 04 01
«АВТОМАТИКА И ТЕЛЕМЕХАНИКА»
НА 2018/2019 УЧЕБНЫЙ ГОД.

Учебная программа пересмотрена и одобрена на заседании кафедры.
Утверждается со следующими изменениями:

В теме 6 «Криптографические методы защиты информации в системах автоматики и телемеханики» переименовать подразделы «Симметричные криптосистемы в системах автоматики и телемеханики» и «Асимметричные криптосистемы в системах автоматики и телемеханики» на «Симметричные методы шифрования. Алгоритмы DES и AES» и «Асимметричные методы шифрования. Алгоритмы RSA и Эль-Гамаля» соответственно.

пр. № 5 от « 22 » 05 2018 г.

Заведующий кафедрой «Системы передачи информации», доцент _____ В.Г. Шевчук

Утверждаю:
Декан электротехнического факультета , к.т.н., доцент _____ Ф.Е. Сатырев

Утверждаю:
Декан заочного факультета , к.т.н., доцент _____ В.В. Пигунов

Учебная программа составлена на основе образовательного стандарта ОСВО 1-37 02 04-2013 «Автоматика, телемеханика и связь на железнодорожном транспорте»

СОСТАВИТЕЛИ:

П.М. Буй, доцент кафедры «Системы передачи информации» учреждения образования «Белорусский государственный университет транспорта», кандидат технических наук, доцент;

Е.С. Белоусова, доцент кафедры «Системы передачи информации» учреждения образования «Белорусский государственный университет транспорта», кандидат технических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой «Системы передачи информации» учреждения образования «Белорусский государственный университет транспорта»
(протокол № 3 от 15 марта 2017 г.);
научно-методической комиссией электротехнического факультета учреждения образования «Белорусский государственный университет транспорта»
(протокол № 2 от 27 апреля 2017 г.);
научно-методической комиссией заочного факультета учреждения образования «Белорусский государственный университет транспорта»
(протокол № 3 от 14 апреля 2017 г.);
научно-методическим советом учреждения образования «Белорусский государственный университет транспорта»
(протокол № от мая 2017 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Актуальность изучения учебной дисциплины

В последнее время наблюдается резкое увеличение вычислительной мощности современных компьютеров при одновременном упрощении их эксплуатации, а также резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с их помощью в современных системах автоматики и телемеханики. Кроме того, в системах автоматики и телемеханики постоянно расширяется круг пользователей, имеющих непосредственный доступ к управлению и к массивам данных, повсеместно используются сетевые технологии, происходит объединение локальных сетей в глобальные, применяется удаленное управление. В связи с этим все более актуальным становится вопрос о защите информации в системах управления на транспорте и, в частности, в системах автоматики и телемеханики. Важными задачами являются анализ причин возникновения каналов утечки информации, определение методов и средств их блокировки, а также грамотная организация и построение комплексной системы информационной безопасности для систем автоматики и телемеханики. Поэтому важно, чтобы в процессе обучения студент освоил современные методы обеспечения информационной безопасности таких систем в условиях возникновения угроз.

Программа разработана на основе компетентностного подхода, требований к формированию компетенций, сформулированных в образовательном стандарте ОСВО 1-37 02 04-2013 «Автоматика, телемеханика и связь на железнодорожном транспорте».

Дисциплина относится к циклу общепрофессиональных и специальных дисциплин, осваиваемых студентами специальности 1-37 02 04 «Автоматика, телемеханика и связь на железнодорожном транспорте».

Цели и задачи учебной дисциплины

Целью преподавания дисциплины «Информационная безопасность систем автоматики и телемеханики» является получение студентами базовых знаний по вопросам обеспечения информационной безопасности управляющих систем на транспорте в условиях возникновения угроз различных по виду, происхождению и характеру.

Основными задачами дисциплины являются:

– изучение основных угроз информационной безопасности и уязвимостей объектов информатизации в системах автоматики и телемеханики;

– изучение методов и средств аутентификации субъектов и разграничения доступа;

– получение знаний о применяемых методах криптографического преобразования информации;

– получение представлений о построении комплексной системы защиты информации.

Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студент должен закрепить и развить следующие академические (АК) и социально-личностные (СЛК) компетенции, предусмотренные в образовательном стандарте ОСВО 1- 37 02 04-2013:

АК-1. Уметь применять базовые научно-теоретическими знания для решения теоретических и практических задач;

АК-2. Владеть системным и сравнительным анализом;

АК-3. Владеть исследовательскими навыками;

АК-4. Уметь работать самостоятельно;

АК-5. Быть способным порождать новые идеи (обладать креативностью);

АК-6. Владеть междисциплинарным подходом при решении проблем;

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером;

АК-9. Уметь учиться, повышать свою квалификацию в течении всей жизни;

СЛК-5. Быть способным к критике и самокритике;

СЛК-6. Уметь работать в команде.

В результате изучения дисциплины студент должен обладать следующими профессиональными компетенциями (ПК), предусмотренными образовательными стандартами ОСВО 1-37 02 04-2013:

ПК-7. Осуществлять мероприятия по организации и сохранению информационной безопасности систем железнодорожной автоматики, телемеханики и связи в соответствии с действующим законодательством;

ПК-8. Обоснованно выбирать методы и критерии защиты систем железнодорожной автоматики, телемеханики и связи от перенапряжений;

ПК-10. Давать оценку функциональным узлам систем железнодорожной автоматики, телемеханики и связи с точки зрения их информационной и функциональной безопасности;

ПК-44. Содействовать применению систем железнодорожной автоматики, телемеханики и связи, обеспечивающих защиту обрабатываемой информации.

Для приобретения профессиональных компетенций ПК-7, ПК-8, ПК-10 и ПК-44 в результате изучения дисциплины студент должен.

знать:

– системную методологию, правовое и нормативное обеспечение защиты информации;

– организационные и технические методы защиты информации;

– активные и пассивные мероприятия по защите информации и средства их реализации;

уметь:

– проводить анализ вероятных угроз информационной безопасности для заданных объектов;

– определять риски нарушения информационной безопасности систем автоматики и телемеханики;

– разрабатывать рекомендации по защите объектов различного типа от несанкционированного доступа;

владеть:

– современными техническими средствами защиты информации;

– принципами организации и построения комплексных систем защиты информации.

Структура содержания учебной дисциплины

Содержание дисциплины представлено в виде тем, которые характеризуются относительно самостоятельными укрупненными дидактическими единицами содержания обучения. Содержание дисциплины опирается на приобретенные ранее студентами компетенции при изучении общепрофессиональных и специальных дисциплин «Теория вероятности и математическая статистика», «Надежность устройств автоматики, телемеханики и связи», «Теоретические основы автоматики и телемеханики».

Форма получения высшего образования – дневная и заочная. По дневной форме обучения дисциплина изучается в 9 семестре.

В соответствии с учебным планом на изучение дисциплины отведено всего 110 часов, в том числе 72 аудиторных часа, из них лекции – 38 часов, практические занятия – 34 часа. Форма текущей аттестации – зачет. Трудоемкость дисциплины составляет 3 зачетных единицы.

Распределение аудиторных часов по семестрам, видам занятий дневной формы обучения

Семестр	Всего часов	Зачетных единиц	Аудиторных часов	Лекции	Практические занятия	Форма текущей аттестации
9	110	3	72	38	34	Зачет

Распределение аудиторных часов по семестрам, видам занятий заочной полной и сокращенной формам обучения

Курс	Семестр	Всего часов	Зачетных единиц	Аудиторных часов	Часов ауд. занятий в семестре по видам учебной работы				Количество видов отчетности				
					лекции	лабораторные занятия	практические занятия	СУРС	экзамены	зачеты	курсовые проекты	курсовые работы	контрольные работы
5	9	8		8	4		4						
5	10	102	3	8	2		6			1			
Итого:		110	3	16	6		10						
Всего часов:													
самостоятельное изучение аудиторных тем:									56				

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. **Введение в информационную безопасность**

Основные понятия информационной безопасности. Государственный стандарт Республики Беларусь 50922-2000 «Защита информации. Основные термины и определения». Особенности информации, как объекта защиты. Виды информации в соответствии с Законом Республики Беларусь «Об информации, информатизации и защите информации». Краткий исторический экскурс по вопросам информационной безопасности. Задачи в сфере обеспечения информационной безопасности.

Тема 2. **Угрозы информационной безопасности систем автоматики и телемеханики**

Понятие угрозы. Классификация угроз информационной безопасности систем автоматики и телемеханики по виду, происхождению, источникам и характеру возникновения. Классификация уязвимостей информационных объектов. Понятие риска. Способы оценки рисков. Понятие атаки. Модель нарушителя информационной безопасности систем автоматики и телемеханики. Статьи Уголовного кодекса Республики Беларусь по вопросам информационной безопасности.

Тема 3. **Правила разграничения доступа**

Смысл и необходимость разграничения доступа при организации информационного взаимодействия на объектах информатизации. Основные принципы организации разграничения доступа, и их применение.

Тема 4. **Методы защиты информации в системах автоматики и телемеханики**

Классификация методов защиты информации в системах автоматики и телемеханики по характеру проводимых мероприятий. Организационные методы. Аппаратные методы. Программные методы. Модели информационной безопасности. Обеспечение конфиденциальности, доступности и целостности информации.

Тема 5. **Сертификация и аттестация систем автоматики и телемеханики в сфере защиты информации**

Государственная политика информационной безопасности. Состав и основные функции государственной системы защиты информации Республики Беларусь. Оперативно-аналитический центр при Президенте Республики Беларусь, его цели и функции. Сертификация и аттестация средств защиты и объектов информации в Республике Беларусь. Стандарты Республики Беларусь серии 34.101. Задание по безопасности. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 62 от 30 августа 2013 года «О некоторых вопросах технической и криптографической защиты информации».

Тема 6. **Криптографические методы защиты информации в системах автоматики и телемеханики**

Классификация криптографических методов защиты информации в системах автоматики и телемеханики. Архивация и кодирование информации. Шифрование информации. Симметричные методы шифрования. Алгоритмы DES и AES. Асимметричные методы шифрования. Алгоритмы RSA и Эль-Гамаля. Хэш-функции. Управление криптографическими ключами в системах автоматики и телемеханики: генерация, хранение и распределение ключей.

Тема 7. **Средства аутентификации субъектов в системах автоматики и телемеханики**

Понятие идентификации и аутентификации. Классификация средств аутентификации в системах автоматики и телемеханики. Парольные средства аутентификации в системах автоматики и телемеханики. Средства аутентификации с использованием смарт-карт и электронных ключей в системах автоматики и телемеханики. Биометрические средства аутентификации.

Тема 8. **Информационная безопасность автоматизированных систем управления технологическими процессами**

Обзор инцидентов в сфере информационной безопасности. Понятие критически важного объекта информатизации и методы обеспечения его информационной безопасности. Постановление Совета Министров Республики Беларусь № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации». Особенности функциональной безопасности. Защита информации в АСУ ТП.

Тема 9. **Комплексный подход к обеспечению безопасности информационных систем**

Методы оценки эффективности средств обеспечения информационной безопасности. Методы и средства защиты информации от удаленных атак. Компьютерные вирусы и механизмы борьбы с ними. Комплексный подход при обеспечении защиты информации. Политика безопасности информационных систем. Ценностно-надежностные аспекты при организации комплексной защиты информации. Назначение и цель политики информационной безопасности. Концепция национальной безопасности Республики Беларусь.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (дневная форма обучения)

Номер темы, занятия	Название темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов		Материальное обеспечение занятия (наглядные методические пособия и др.)	Литература	Форма контроля знаний
		лекции	практические занятия			
1	**Тема 1. Введение в информационную безопасность (2 ч)**	2		Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,2,8]	
2	**Тема 2. Угрозы информационной безопасности систем автоматики и телемеханики (12 ч)**	4	8	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,7]	Отчет по практическим работам, защита практических работ
2.1	Понятие угрозы. Классификация угроз информационной безопасности систем автоматики и телемеханики по виду, происхождению, источникам и характеру возникновения. Классификация уязвимостей информационных объектов. Понятие риска. Способы оценки рисков.	2	6			
2.2	Понятие атаки. Модель нарушителя информационной безопасности систем автоматики и телемеханики. Статьи Уголовного кодекса Республики Беларусь по вопросам информационной безопасности.	2	2			
3	**Тема 3. Правила разграничения доступа (4 ч)**	2	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,8]	Отчет по практическим работам, защита практических работ

4	**Тема 4. Методы защиты информации в системах автоматики и телемеханики (6 ч)**	4	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,8]	Отчет по практическим работам, защита практических работ
4.1	Классификация методов защиты информации в системах автоматики и телемеханики по характеру проводимых мероприятий. Организационные методы. Аппаратные методы. Программные методы.	2				
4.2	Модели информационной безопасности. Обеспечение конфиденциальности, доступности и целостности информации.	2	2			
5	**Тема 5. Сертификация и аттестация систем автоматики и телемеханики в сфере защиты информации (8 ч)**	4	4	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,8]	Отчет по практическим работам, защита практических работ
5.1	Государственная политика информационной безопасности. Состав и основные функции государственной системы защиты информации Республики Беларусь. Оперативно-аналитический центр при Президенте Республики Беларусь, его цели и функции. Сертификация и аттестация средств защиты и объектов информации в Республике Беларусь. Стандарты Республики Беларусь серии 34.101.	2	2			
5.2	Задание по безопасности. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 62 от 30 августа 2013 года «О некоторых вопросах технической и криптографической защиты информации».	2	2			
6	**Тема 6. Криптографические методы защиты информации в системах автоматики и телемеханики (14 ч)**	6	8	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,3,5]	Отчет по практическим работам, защита практических работ
6.1	Классификация криптографических методов защиты информации в системах автоматики и телемеханики. Архивация и кодирование информации. Шифрование информации. Симметричные методы шифрования. Алгоритмы DES и AES..	4	2			
6.2	Асимметричные методы шифрования. Алгоритмы RSA и Эль-Гамаля. Хэш-функции. Управление криптографическими ключами в системах автоматики и телемеханики: генерация, хранение и распределение ключей.	2	6			
7	**Тема 7. Средства аутентификации субъектов в системах автоматики и телемеханики (12 ч)**	6	6	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональ-	[1,2,4,6]	Отчет по практическим работам, защита практических работ
7.1	Понятие идентификации и аутентификации. Классификация средств аутентификации в системах автоматики и телемеханики. Парольные средства аутентификации в системах автоматики и телемеханики.	2	2			
7.2	Средства аутентификации с использованием смарт-карт и электрон-	4	4			

	ных ключей в системах автоматики и телемеханики. Биометрические средства аутентификации.			ных компьютеров		
8	**Тема 8. Информационная безопасность автоматизированных систем управления технологическими процессами (6 ч)**	4	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2]	Отчет по практическим работам, защита практических работ
8.1	Обзор инцидентов в сфере информационной безопасности. Понятие критически важного объекта информатизации и методы обеспечения его информационной безопасности.	2	2			
8.2	Постановление Совета Министров Республики Беларусь № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации». Особенности функциональной безопасности. Защита информации в АСУ ТП.	2				
9	**Тема 9. Комплексный подход к обеспечению безопасности информационных систем (8 ч)**	6	2	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,7,8]	Отчет по практическим работам, защита практических работ
9.1	Методы оценки эффективности средств обеспечения информационной безопасности. Методы и средства защиты информации от удаленных атак. Компьютерные вирусы и механизмы борьбы с ними. Комплексный подход при обеспечении защиты информации. Политика безопасности информационных систем.	4				
9.2	Ценностно-надежностные аспекты при организации комплексной защиты информации. Назначение и цель политики информационной безопасности. Концепция национальной безопасности Республики Беларусь.	2	2			

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (заочная полная и сокращенная формы обучения)

Номер темы, занятия	Название темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов		Самостоятельное изучении материала, час	Материальное обеспечение занятия (наглядные методические пособия и др.)	Литература	Форма контроля знаний
		лекции	практические занятия				
1	**Тема 1. Введение в информационную безопасность (2 ч)**			2	Учебники, методическая литература, конспект лекций	[1,2,8]	
2	**Тема 2. Угрозы информационной безопасности систем автоматики и телемеханики (12 ч)**	2	2	8	Учебники, методическая литература, конспект лекций, класс персональных компьютеров	[1,7]	Отчет по практическим работам, защита практических работ
2.1	Понятие угрозы. Классификация угроз информационной безопасности систем автоматики и телемеханики по виду, происхождению, источникам и характеру возникновения. Классификация уязвимостей информационных объектов. Понятие риска. Способы оценки рисков.	1	2	5			
2.2	Понятие атаки. Модель нарушителя информационной безопасности систем автоматики и телемеханики. Статьи Уголовного кодекса Республики Беларусь по вопросам информационной безопасности.	1		3			
3	**Тема 3. Правила разграничения доступа (4 ч)**			4	Учебники, методическая литература, конспект лекций	[1,2,8]	
4	**Тема 4. Методы защиты информации в системах автоматики и телемеханики (6 ч)**	1		5	Учебники, методическая литература, конспект лекций, презентации с про-	[1,2,8]	
4.1	Классификация методов защиты информации в системах автоматики и телемеханики по характеру проводимых мероприятий. Орга-			2			

	низационные методы. Аппаратные методы. Программные методы.				ектора и ноутбука		
4.2	Модели информационной безопасности. Обеспечение конфиденциальности, доступности и целостности информации.	1		3			
5	**Тема 5. Сертификация и аттестация систем автоматики и телемеханики в сфере защиты информации (8 ч)**	1	2	5	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,8]	Отчет по практическим работам, защита практических работ
5.1	Государственная политика информационной безопасности. Состав и основные функции государственной системы защиты информации Республики Беларусь. Оперативно-аналитический центр при Президенте Республики Беларусь, его цели и функции. Сертификация и аттестация средств защиты и объектов информации в Республике Беларусь. Стандарты Республики Беларусь серии 34.101.		2	2			
5.2	Задание по безопасности. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 62 от 30 августа 2013 года «О некоторых вопросах технической и криптографической защиты информации».	1		3			
6	**Тема 6. Криптографические методы защиты информации в системах автоматики и телемеханики (14 ч)**		2	12	Учебники, методическая литература, конспект лекций, класс персональных компьютеров	[1,2,3,5]	Отчет по практическим работам, защита практических работ
6.1	Классификация криптографических методов защиты информации в системах автоматики и телемеханики. Архивация и кодирование информации. Шифрование информации. Симметричные методы шифрования. Алгоритмы DES и AES..		2	4			
6.2	Асимметричные методы шифрования. Алгоритмы RSA и Эль-Гамаля. Хэш-функции. Управление криптографическими ключами в системах автоматики и телемеханики: генерация, хранение и распределение ключей.			8			
7	**Тема 7. Средства аутентификации субъектов в системах автоматики и телемеханики (12 ч)**	1	2	9	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука, класс персональных компьютеров	[1,2,4,6]	Отчет по практическим работам, защита практических работ
7.1	Понятие идентификации и аутентификации. Классификация средств аутентификации в системах автоматики и телемеханики. Парольные средства аутентификации в системах автоматики и телемеханики.		2	2			
7.2	Средства аутентификации с использованием смарт-карт и электронных ключей в системах автоматики и телемеханики. Биометрические средства аутентификации.	1		7			

8	**Тема 8. Информационная безопасность автоматизированных систем управления технологическими процессами (6 ч)**		2	4	Учебники, методическая литература, конспект лекций, класс персональных компьютеров	[1,2]	Отчет по практическим работам, защита практических работ
8.1	Обзор инцидентов в сфере информационной безопасности. Понятие критически важного объекта информатизации и методы обеспечения его информационной безопасности.		2	2			
8.2	Постановление Совета Министров Республики Беларусь № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации». Особенности функциональной безопасности. Защита информации в АСУ ТП.			2			
9	**Тема 9. Комплексный подход к обеспечению безопасности информационных систем (8 ч)**	1		7	Учебники, методическая литература, конспект лекций, презентации с проектора и ноутбука	[1,2,7,8]	
9.1	Методы оценки эффективности средств обеспечения информационной безопасности. Методы и средства защиты информации от удаленных атак. Компьютерные вирусы и механизмы борьбы с ними. Комплексный подход при обеспечении защиты информации. Политика безопасности информационных систем.	1		3			
9.2	Ценностно-надежностные аспекты при организации комплексной защиты информации. Назначение и цель политики информационной безопасности. Концепция национальной безопасности Республики Беларусь.			4			

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

КРИТЕРИИ ОЦЕНОК РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ

Оценка	Показатели оценки
незачет	Недостаточно полный объем знаний в вопросах дисциплины; знание только незначительной части основной литературы, рекомендованной учебной программой дисциплины, использование научной терминологии, изложение ответа на вопросы с существенными ошибками; слабое владение инструментарием учебной дисциплины, некомпетентность в решении стандартных (типовых) задач; пассивность на практических занятиях, низкий уровень культуры исполнения заданий.
зачет	Систематизированные, глубокие и полные знания по всем поставленным вопросам в сфере информационной безопасности систем автоматики и телемеханики; точное использование научной терминологии, грамотное и логически правильное изложение ответа на вопросы, умение делать обобщения и обоснованные выводы; владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации в рамках учебной программы; достаточное усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины; умение оценивать угрозы, уязвимости и риски информационной безопасности, эффективность средств аутентификации, организовывать политику безопасности информационной системы; систематическая активная самостоятельная работа на практических занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Методы (технологии) обучения

Основными методами (технологиями), отвечающие целям изучения дисциплины, являются:

− элементы проблемного обучения, реализуемые при проведении всех видов учебных занятий по дисциплине;

− элементы учебно-исследовательской деятельности, реализуемые на практических занятиях и при самостоятельной работе.

Организация самостоятельной работы

При изучении дисциплины используются следующие формы самостоятельной работы:

− контролируемая самостоятельная работа в виде решения индивидуальных исследовательских задач в аудитории во время проведения практических занятий под контролем преподавателя в соответствии с расписанием;

− самостоятельная работа при подготовке к практическим занятиям.

Диагностика компетенций студента

Оценка учебных достижений студента на зачете производится по шкале «зачет-незачет».

Для оценки достижений студентов используется следующие формы:

− устные доклады на научно-технических конференциях (АК-1, АК-2, АК-3, АК-4, АК-7, АК-9, СЛК-6, ПК-7, ПК-8, ПК-10, ПК-44);

− тесты и контрольные опросы по отдельным темам (АК-1, АК-2, АК-4, АК-9, ПК-7, ПК-8, ПК-10);

− отчеты по практическим работам с их устной защитой (АК-1, АК-2, АК-3, АК-4, АК-7, АК-9, СЛК-5, СЛК-6, ПК-7, ПК-8, ПК-10);

− проведение зачета по дисциплине в устной форме (АК-1, АК-2, АК-4, АК-5, АК-7, СЛК-5, ПК-7, ПК-8, ПК-10, ПК-44).

ОСНОВНАЯ ЛИТЕРАТУРА

1. **Яковлев, В. В.** Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта / В. В. Яковлев, А. А. Корниенко // Учебник для ВУЗов ж.-д. транспорта. – М.: УМК МПС России, 2002. – 328 с.

2. **Романец, Ю. В.** Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М.: Радио и связь, 2001. – 376с.

3. **Мао, Венбо** Современная криптография: теория и практика / Венбо Мао // Пер с англ. – М.: Издательский дом «Вильямс», 2005. – 768с.

4. **Смит, Ричард Э.** Аутентификация: от паролей до открытых ключей / Ричард Э. Смит. – М.: Издательский дом «Вильямс», 2002. – 432с.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

5. **Буй, П.М.** Криптографические методы защиты информации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в телекоммуникацииооных системах» / П.М. Буй, В.О. Матусевич. – Гомель : БелГУТ, 2010. – 56 с.

6. **Буй, П.М.** Средства аутентификации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в системах управления на транспорте» / П.М. Буй, Д.Д. Семиход. – Гомель : БелГУТ, 2010. – 39 с.

7. **Белоусова, Е.С.** Политика безопасности информационных систем : учеб.-метод. пособие для практ. работ / Е.С. Белоусова, П.М. Буй. – Гомель : БелГУТ, 2016. – 38 с.

8. **Домарев, В. В.** Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К.: ООО «ТИД “ДС”», 2001. – 688с.

ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Тема 2

1 Анализ угроз безопасности информационной системы;

2 Количественная оценка рисков информационной безопасности;

3 Качественная оценка рисков информационной безопасности;

4 Модель нарушителя информационной безопасности системы автоматики и телемеханики;

Тема 3

5 Правила разграничения доступа;

Тема 4

6 Обеспечение конфиденциальности, доступности и целостности информации в системе автоматики и телемеханики;

Тема 5

7 Изучение СТБ 34.101.1, СТБ 34.101.2 и СТБ 34.101.3;

8 Анализ структуры задания по безопасности;

Тема 6

9 Оценка симметричных методов шифрования в системах автоматики и телемеханики;

10 Оценка асимметричных методов шифрования в системах автоматики и телемеханики;

11 Формирование электронно-цифровой подписи документа;

12 Исследование методов управления криптографическими ключами;

Тема 7

13 Исследование показателей эффективности парольных средств аутентификации в системах автоматики и телемеханики;

14 Исследование показателей эффективности биометрических средств аутентификации в системах автоматики и телемеханики;

15 Исследование показателей эффективности комбинированных средств аутентификации в системах автоматики и телемеханики;

Тема 8

16 Обеспечение информационной безопасности критически важных объектов информатизации;

Тема 9

17 Политика безопасности информационной системы.

17

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО ДИСЦИПЛИНЕ **«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ»** С ДРУГИМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
1 Микропроцессорные информационно-управляющие системы в железнодорожной автоматике и телемеханике	МТиИУС	Согласовано	
2 Системы управления базами данных	МТиИУС	Согласовано	