Учреждение образования
«Белорусский государственный университет транспорта»

Электротехнический факультет

Кафедра «Системы передачи информации»

СОГЛАСОВАНО
Заведующий кафедрой
_____ Шевчук В.Г.
20.03.2018 г.

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

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И БАЗ ДАННЫХ

для специальности

1-37 02 04 «Автоматика, телемеханика и связь на железнодорожном транспорте»
специализации 1-37 02 04 03 «Микропроцессорные информационно-управляющие системы»

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.

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 «Защита программного обеспечения и баз данных» 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 «Микропроцессорные информационно-управляющие системы».

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 системах управления на транспорте. Кроме того, в системах управления на транспорте постоянно расширяется круг пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных, повсеместно используются программные автоматизированные рабочие места сотрудников, применяются сетевые технологии, происходит объединение локальных сетей в глобальные. В связи с этим все более актуальным становится вопрос о защите программного обеспечения и баз данных в системах управления на транспорте. Важными задачами являются анализ причин возникновения каналов утечки информации из баз данных, определение методов и средств их блокировки, защита программного обеспечения, а также грамотная организация и построение комплексной системы защиты информации в системах управления на транспорте. Поэтому важно, чтобы в процессе обучения студент освоил современные методы защиты программного обеспечения и баз данных.

Целью преподавания дисциплины «Защита программного обеспечения и баз данных» является получение студентами базовых знаний по вопросам защиты программного обеспечения и обеспечения гарантированного разграничения доступа к информации в базах данных в условиях возникновения угроз различных по виду, происхождению и характеру.

Основными задачами изучения дисциплины являются:

– изучение методов защиты программного обеспечения;

– получение знаний о методах организации разграничения доступа к информации в базах данных.

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 «Защита программного обеспечения и баз данных» излагается посредством чтения лекций, проведения практических занятий.

При создании УМКД «Защита программного обеспечения и баз данных» 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 Буй, П. М. Криптографические методы защиты информации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в телекоммуникационных системах» / П. М. Буй, В. О. Матусевич ; М-во образования Респ. Беларусь, Белорус. гос. ун-т трансп. – 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 ; М-во образования Респ. Беларусь, Белорус. гос. ун-т трансп. – 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 / Е. С. Белоусова, П. М. Буй ; М-во трансп. и коммуникаций Респ. Беларусь, Белорус. гос. ун-т трансп. – Гомель : БелГУТ, 2016. – 38 с.

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

4 Корниенко, А. А. Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) : учеб. пособие для вузов / А. А. Корниенко, М. А. Еремеев, С. Е. Ададуров. – М. : Маршрут, 2006. – 252 с.

(Электронный вариант на кафедре)

5 Голиков, В. Ф. Методологические основы информационной безопасности : учеб.-метод. пособие / В. Ф. Голиков, И. И. Черная, О. Б. Зельманский. – Минск : БГУИР, 2012. – 72 с.

(Электронный вариант на кафедре)

6 Щеглов, А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и техника, 2005. – 384 с.

(Электронный вариант на кафедре)

7 Петренко, С. А. Политики информационной безопасности / С. А. Петренко, В. А. Курбатов. – М. : Компания АйТи, 2006. – 400 с.

(Электронный вариант на кафедре)

8 Защита информации в банковских технологиях : учеб.-метод. пособие / Л. М. Лыньков [и др.]. – Минск : БГУИР, 2009. – 198 с.

(Электронный вариант на кафедре)

3 ПРАКТИЧЕСКИЙ РАЗДЕЛ

3.1 Перечень практических работ

1. Анализ угроз безопасности информационной системы;
2. Модель нарушителя информационной безопасности;
3. Количественная оценка рисков информационной безопасности;
4. Качественная оценка рисков информационной безопасности;
5. Правила разграничения доступа;
6. Политика безопасности информационной системы;
7. Оценка симметричных методов шифрования для защиты программного обеспечения и баз данных;
8. Оценка асимметричных методов шифрования для защиты программного обеспечения и баз данных;
9. Изучение хэш-функций для защиты программного обеспечения и баз данных;
10. Формирование электронно-цифровой подписи для защиты программного обеспечения и баз данных;
11. Исследование методов управления криптографическими ключами для защиты программного обеспечения и баз данных;
12. Исследование показателей эффективности парольных средств аутентификации для защиты программного обеспечения и баз данных;
13. Исследование показателей эффективности биометрических средств аутентификации для защиты программного обеспечения и баз данных;
14. Исследование показателей эффективности комбинированных средств аутентификации для защиты программного обеспечения и баз данных.
15. Защита программного обеспечения от несанкционированного копирования и доступа;
16. Безопасность локальных сетей;
17. Списки управления доступом ACL.

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

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

32. Как раскрывается аббревиатура ОАЦ в сфере защиты информации?

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

34. 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?

35. Какой метод защиты программного обеспечения относится к методам собственной защиты?

36. Какой метод защиты программного обеспечения относится к методам использования средств защиты в составе вычислительной системы?

37. Какой метод защиты программного обеспечения относится к методам защиты с запросом информации?

38. Как раскрывается аббревиатура НСД в системах защиты информации?

39. Как раскрывается аббревиатура НСК в системах защиты информации?

40. Что из перечисленного является методом криптографического преобразования информации?

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

42. Какой из представленных алгоритмов относится к симметричным криптосистемам?

43. Какой из представленных алгоритмов относится к асимметричным криптосистемам?

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

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

46. К какому классу алгоритмов шифрования относится шифрование Цезаря?

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

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

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

50. Для чего используется алгоритм Эль Гамаля?

51. Для чего используется алгоритм Диффи-Хеллмана?

52. Сколько циклов шифрования содержит алгоритм DES?

53. Какова длина ключа DES?

54. Какова длина информационного блока, шифрующегося алгоритмом DES?

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

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

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

58. Какое из перечисленных средств аутентификации относится к биометрическим?

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

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

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

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

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

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

65. 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 (A)	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 выполнение 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 «Защита программного обеспечения и баз данных» №20.35/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-20.35 /уч.

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И БАЗ ДАННЫХ

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 03 «Микропроцессорные информационно-управляющие системы»

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
ПО ДИСЦИПЛИНЕ
«ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И БАЗ ДАННЫХ»
СПЕЦИАЛИЗАЦИИ 1-37 02 04 03
«МИКРОПРОЦЕССОРНЫЕ ИНФОРМАЦИОННО-
УПРАВЛЯЮЩИЕ СИСТЕМЫ»
НА 2018/2019 УЧЕБНЫЙ ГОД.

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

1. В тему 2 «Угрозы и модель нарушителя информационной безопасности» добавить подраздел «Риски нарушения информационной безопасности. Их количественная и качественная оценка»;
2. Из темы 3 «Правовое обеспечение и государственное регулирование защиты информации в Республике Беларусь» изъять подраздел «Постановление Совета Министров Республики Беларусь № 675 «О некоторых вопросах защиты информации»».
3. Из темы 8 «Комплексный подход к обеспечению безопасности информационных систем» изъять подраздел «Управление доступом» в связи с изложением данного материала в теме 5 «Управление доступом к информации в базах данных».

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

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

СОСТАВИТЕЛИ:

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

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

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой «Системы передачи информации» учреждения образования «Белорусский государственный университет транспорта»
(протокол № 3 от 15.03.2017 г.);
научно-методической комиссией электротехнического факультета учреждения образования «Белорусский государственный университет транспорта»
(протокол № 2 от 27.04.2017 г.);
научно-методическим советом учреждения образования «Белорусский государственный университет транспорта»
(протокол № __ от _____ 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 системах управления на транспорте. Кроме того, в системах управления на транспорте постоянно расширяется круг пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных, повсеместно используются программные автоматизированные рабочие места сотрудников, применяются сетевые технологии, происходит объединение локальных сетей в глобальные. В связи с этим все более актуальным становится вопрос о защите программного обеспечения и баз данных в системах управления на транспорте. Важными задачами являются анализ причин возникновения каналов утечки информации из баз данных, определение методов и средств их блокировки, защита программного обеспечения, а также грамотная организация и построение комплексной системы защиты информации в системах управления на транспорте. Поэтому важно, чтобы в процессе обучения студент освоил современные методы защиты программного обеспечения и баз данных.

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», специализации 1-37 02 04 03 «Микропроцессорные информационно-управляющие системы».

Цели и задачи учебной дисциплины

Целью преподавания дисциплины «Защита программного обеспечения и баз данных» является получение студентами базовых знаний по вопросам защиты программного обеспечения и обеспечения гарантированного разграничения доступа к информации в базах данных в условиях возникновения угроз различных по виду, происхождению и характеру.

Основными задачами изучения дисциплины являются: изучение методов защиты программного обеспечения; получение знаний о методах организации разграничения доступа к информации в базах данных; изучение современных алгоритмов шифрования данных.

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-теоретические 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 течение всей жизни;

СЛК-2. Быть способным к социальному взаимодействию;

СЛК-3. Обладать способностью к межличностным коммуникациям;

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-29. Владеть основными методами, способами и средствами получения, хранения, переработки информации, наличием навыков работы с компьютером как средством управления информацией.

ПК-32. Взаимодействовать со специалистами смежных профессий.

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

Для приобретения профессиональных компетенций ПК-29, ПК-32, ПК-34, ПК-35 и ПК-44 в результате изучения дисциплины студент должен

знать:

системную методологию, правовое и нормативное обеспечение защиты информации;

организационные и технические методы защиты программного обеспечения и баз данных;

каналы утечки информации из баз данных, их обнаружение и обеспечение информационной безопасности;

уметь:

проводить анализ рисков вероятных угроз программному обеспечению и информации в базах данных;

определять возможные каналы утечки информации из баз данных и обоснованно выбирать методы и средства их блокировки;

разрабатывать рекомендации по защите программного обеспечения и баз данных;

владеть:

методами реализации алгоритмов шифрования средствами инструментального программного обеспечения и применять их для решения практических задач.

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 естественнонаучной дисциплины «Высшая математика».

Форма получения высшего образования – дневная. 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 часов, из них лекции – 38 часов, практические занятия – 24 часов. Форма текущей аттестации – зачет. Трудоемкость дисциплины составляет 3 зачетных единиц.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. **Основные понятия и терминология защиты информации**

Государственный стандарт Республики Беларусь 50922-2000 «Защита информации. Основные термины и определения».

Тема 2. **Угрозы и модель нарушителя информационной безопасности**

Классификация угроз информационной безопасности по виду, происхождению, источникам и характеру возникновения. Риски нарушения информационной безопасности. Их количественная и качественная оценка. Модель нарушителя информационной безопасности.

Тема 3. **Правовое обеспечение и государственное регулирование защиты информации в Республике Беларусь**

Информация как объект права собственности. Концепция Национальной безопасности. Закон Республики Беларусь № 455-З «Об информации, информатизации и защите информации» от 10 ноября 2008 г. Закон Республики Беларусь № 113-З «Об электронном документе и электронной цифровой подписи» от 28 декабря 2009 г. 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.

Тема 4. **Методы и средства анализа безопасности программного обеспечения**

Методы и средства анализа безопасности программного обеспечения. Методы защиты программного обеспечения. Категории средств защиты программного обеспечения. Защита программного обеспечения от несанкционированного доступа. Защита программного обеспечения от несанкционированного копирования.

Тема 5. **Управление доступом к информации в базах данных**

Классификация компонент доступа, правила разграничения доступа к информации в базах данных. Принципы построения системы разграничения доступа к информации в базах данных. Механизмы управления доступом к информации в базах данных. Алгоритмы управления доступом к базах данных.

Тема 6. **Криптографические методы защиты программного обеспечения и баз данных**

Классификация криптографических методов защиты программного обеспечения и баз данных. Симметричные криптосистемы. Асимметричные криптосистемы. Хэш-функции. Электронная цифровая подпись: алгоритмы RSA, Эль Гамаля, DSA. Управление криптографическими ключами: генерация, хранение и распределение ключей.

Тема 7. **Средства аутентификации при защите программного обеспечения и баз данных**

Понятие идентификации и аутентификации. Классификация средств аутентификации при защите программного обеспечения и баз данных. Парольные средства аутентификации. Средства аутентификации с использованием смарт-карт и электронных ключей. Биометрические средства аутентификации. Протоколы сетевой аутентификации.

Тема 8. **Комплексный подход к обеспечению безопасности информационных систем**

Организационно-технические и режимные меры обеспечения безопасности информационных систем. Методы и средства защиты информации от удаленных атак через сеть Internet. Компьютерные вирусы и механизмы борьбы с ними. Защита информации в распределенных сетях. Комплексные системы защиты информации.

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. Основные понятия и терминология защиты информации (2 ч)**	2		Схемы, учебники, методическая литература, конспект лекций, мультимедийные презентации	[3,4,5,7]	
2	**Тема 2. Угрозы и модель нарушителя информационной безопасности (14 ч)**	6	8	Схемы, учебники, методическая литература, конспект лекций, мультимедийные презентации, класс персональных компьютеров (КПК)	[3,4,5,7]	Контрольные опросы, отчеты по практическим работам
3	**Тема 3. Правовое обеспечение и государственное регулирование защиты информации в Республике Беларусь (4 ч.)**	4		Схемы, учебники, методическая литература, конспект лекций, мультимедийные презентации	[3,4,5,7]	
4	**Тема 4. Методы и средства анализа безопасности программного обеспечения (8 ч.)**	4	4	Схемы, учебники, методическая литература, конспект лекций, мультимедийные презентации, КПК	[4,6,8]	Отчеты по практическим работам, электронные те-

						сты
5	**Тема 5. Управление доступом к информации в базах данных (8 ч)**	4	4	Схемы, учебники, методическая литература, конспект лекций, мультимедийные презентации, КПК	[2,3,6]	Отчеты по практическим работам, электронные тесты
6	**Тема 6. Криптографические методы защиты программного обеспечения и баз данных (20 ч.)**	10	10	Схемы, учебники, методическая литература, конспект лекций, мультимедийные презентации, КПК	[1,4,5,6]	Контрольные опросы, отчеты по практическим работам, электронные тесты
6.1	Симметричные криптосистемы	2	2			
6.2	Асимметричные криптосистемы	2	2			
6.3	Хэш-функции	2	2			
6.4	Электронная цифровая подпись	2	2			
6.5	Управление криптографическими ключами	2	2			
7	**Тема 7. Средства аутентификации при защите программного обеспечения и баз данных (12 ч.)**	6	6	Схемы, учебники, методическая литература, конспект лекций, мультимедийные презентации, КПК	[2,4,5,8]	Контрольные опросы, отчеты по практическим работам, электронные тесты
7.1	Парольные средства аутентификации	2	2			
7.2	Биометрические средства аутентификации	2	2			
7.3	Средства аутентификации с использованием смарт-карт и электронных ключей	2	2			
8	**Тема 8. Комплексный подход к обеспечению безопасности информационных систем (4 ч)**	2	2	Схемы, учебники, методическая литература, конспект лекций, мультимедийные презентации	[3,4,7]	Отчеты по практическим работам, электронные тесты

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

КРИТЕРИИ ОЦЕНОК РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ

Оценка	Показатели оценки
Незачет	Отсутствие приращения знаний и компетентности, фрагментарные знания, недостаточно полный объем знаний в вопросах основ защиты программного обеспечения и баз данных, а также методов организации разграничения доступа к информации в базах данных; знание 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 вопросам основ защиты программного обеспечения и баз данных, а также методов организации разграничения доступа к информации в базах данных; умение выбирать способы защиты информации, алгоритмы шифрования, средства идентификации и аутентификации; качественно и количественно оценивать риски ущерба при реализации угроз информационной безопасности; умение грамотно составлять политику безопасности; использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обобщения и обоснованные выводы; владение инструментарием учебной дисциплины, умение его использовать в постановке и решении научных и профессиональных задач; свободное владение типовыми решениями в рамках учебной программы; усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины; активная самостоятельная работа на практических занятиях, 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 работах 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 под контролем преподавателя в соответствии с расписанием;

− самостоятельная работа по подготовке к практическим работам.

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-2, СЛК-3, СЛК-5, ПК-29, ПК-32);

− тесты и контрольные опросы по отдельным темам (АК-1, АК-2, АК-4, АК-7, АК-9, ПК-7, ПК-8, ПК-10, ПК-29, ПК-44);

− отчеты по практическим работам с их устной защитой (АК-1, АК-2, АК-3, АК-4, АК-7, АК-9, СЛК-6, ПК-7, ПК-8, ПК-10, ПК-44);

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

ОСНОВНАЯ ЛИТЕРАТУРА

1 **Буй, П. М.** Криптографические методы защиты информации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в телекоммуникационных системах» / П. М. Буй, В. О. Матусевич ; М-во образования Респ. Беларусь, Белорус. гос. ун-т трансп. – Гомель : БелГУТ, 2010. – 56 с.

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 ; М-во образования Респ. Беларусь, Белорус. гос. ун-т трансп. – Гомель : БелГУТ, 2010. – 39 с.

3 **Белоусова, Е. С.** Политика безопасности информационных систем : учеб.-метод. пособие / Е. С. Белоусова, П. М. Буй ; М-во трансп. и коммуникаций Респ. Беларусь, Белорус. гос. ун-т трансп. – Гомель : БелГУТ, 2016. – 38 с.

4 **Корниенко, А. А.** Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) : учеб. пособие для вузов / А. А. Корниенко, М. А. Еремеев, С. Е. Ададуров. – М. : Маршрут, 2006. – 252 с.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

5 **Голиков, В. Ф.** Методологические основы информационной безопасности : учеб.-метод. пособие / В. Ф. Голиков, И. И. Черная, О. Б. Зельманский. – Минск : БГУИР, 2012. – 72 с.

6 **Щеглов, А. Ю.** Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и техника, 2005. – 384 с.

7 **Петренко, С. А.** Политики информационной безопасности / С. А. Петренко, В. А. Курбатов. – М. : Компания АйТи, 2006. – 400 с.

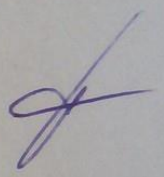
8 Защита информации в банковских технологиях : учеб.-метод. пособие / Л. М. Лыньков [и др.]. – Минск : БГУИР, 2009. – 198 с.

ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

18. Анализ угроз безопасности информационной системы;
19. Модель нарушителя информационной безопасности;
20. Количественная оценка рисков информационной безопасности;
21. Качественная оценка рисков информационной безопасности;

22. Правила разграничения доступа;
23. Политика безопасности информационной системы;
24. Оценка симметричных методов шифрования для защиты программного обеспечения и баз данных;
25. Оценка асимметричных методов шифрования для защиты программного обеспечения и баз данных;
26. Изучение хэш-функций для защиты программного обеспечения и баз данных;
27. Формирование электронно-цифровой подписи для защиты программного обеспечения и баз данных;
28. Исследование методов управления криптографическими ключами для защиты программного обеспечения и баз данных;
29. Исследование показателей эффективности парольных средств аутентификации для защиты программного обеспечения и баз данных;
30. Исследование показателей эффективности биометрических средств аутентификации для защиты программного обеспечения и баз данных;
31. Исследование показателей эффективности комбинированных средств аутентификации для защиты программного обеспечения и баз данных.
32. Защита программного обеспечения от несанкционированного копирования и доступа;
33. Безопасность локальных сетей;
34. Списки управления доступом ACL.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ
ПО ДИСЦИПЛИНЕ
«ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И БАЗ ДАННЫХ»
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. Автоматизированное проектирование микропроцессорных систем	Микропроцессорная техника и информационно-управляющие системы	Согласовано	
2. Микропроцессорные информационно-управляющие системы на железнодорожном транспорте	Микропроцессорная техника и информационно-управляющие системы	Согласовано