Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»
Кафедра прикладной математики и информатики

«Утверждаю»
Проректор по учебно-
методической работе
_____ Ю.А. Устименко
«23» июня 2022 г.

Рабочая программа дисциплины
Б1.О.26 Информационная безопасность

Направление подготовки: **09.03.03 Прикладная информатика**
Направленность (профиль): **Информационные системы организаций и предприятий**
Форма обучения: заочная
Курс – 5
Семестр – 9
Всего зачетных единиц – 3, часов – 108
Форма отчетности: зачет – 9 семестр

Программу разработал
кандидат физико-математических наук, доцент Кристалинский В.Р.

Одобрена на заседании кафедры
«16» июня 2022 г., протокол № 10

Заведующий кафедрой _____ С.В. Козлов

Смоленск
2022

1. Место дисциплины в структуре ОП

Дисциплина «Информационная безопасность» относится к дисциплинам обязательной части учебного плана направления подготовки 09.03.03 Прикладная информатика. Она изучается на 5 курсе в 9 семестре. При изучении данной дисциплины необходимы компетенции студентов, сформированные при изучении таких дисциплин, как «Разработка и стандартизация программных средств и информационных технологий», «Языки и методы программирования», «Проектирование программно-аппаратных комплексов» и др.

В современных условиях, в связи с расширением сферы применения информационных технологий возрастают угрозы, связанные с неправомерным доступом к информации, содержащей государственную или иную охраняемую законом тайну, несанкционированным внесением изменений в информационные системы.

Будущему специалисту важно знать существующие угрозы в сфере информационной безопасности и уметь им противодействовать. Поэтому компетенции, сформированные при изучении дисциплины, необходимы для написания выпускной квалификационной работы бакалавра и его дальнейшей профессиональной деятельности.

В связи с этим курс «Информационная безопасность» занимает важное место в предметной подготовке бакалавров по направлению подготовки 09.03.03 Прикладная информатика.

Изучение курса основано на традиционных методах высшей школы, тесной взаимосвязи со смежными курсами, обобщающими методологию исследований и проектирования социально-экономических информационных систем.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Компетенция	Индикаторы достижения
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать**: основные типы стандартных задач профессиональной деятельности и методы их решения с учетом требования информационной безопасности и применяя современные информационно-коммуникационные технологии на базе информационной и библиографической культуры; **Уметь:** решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применение информационно-коммуникационных технологий и с четом основных требований информационной безопасности; **Владеть**: приемами решения задач профессиональной деятельности на основе информационной и библиографической культуры с применение информационно-коммуникационных технологий и с четом основных требований информационной безопасности.
ПК-1. Способен проводить обследование организаций, выявлять информационные потребности пользователей, собирать детальную информацию, формировать требования к автоматизированной информационной системе (ERP-системе)	**Знать**: методику проведения обследования организаций с целью выявления информационных потребностей пользователей; требования, предъявляемые к логистической информационной системе; возможности типовых ИС, архитектуру, устройство и функционирование

	вычислительных сетей, коммуникационное оборудование и сетевые протоколы, теорию баз данных и основы программирования; основы бухгалтерского учета, управления торговлей, поставками, запасами, управления персоналом, управления организацией, экономической теории **Уметь**: выявлять информационные потребности пользователей, формулировать требования к логистической информационной системе, осуществлять сбор детальной информации для формализации требований пользователей заказчика.. **Владеть**: методами, способами и инструментами выявления информационных потребностей пользователей, методикой обследования организации, навыками по информированию заказчика о возможностях типовых ИС.

3. Содержание дисциплины

Тема 1. Основные составляющие информационной безопасности. Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.

Тема 2. Криптографические способы защиты информации. Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA

Тема 3. Антивирусная защита. Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы.

Тема 4. Сетевая безопасность. Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне:

SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS.

4. Тематический план

№ п/п	Разделы и темы	Всего часов	Формы занятий			
			лекции	практические занятия	лаборат. занятия	Самостоятельная работа
1	Основные составляющие информационной безопасности.	22	–	–	–	22
2	Криптографические способы защиты информации	31	4	–	6	22
3	Антивирусная защита	29	2	–	4	22
4	Сетевая безопасность	22		–	–	22
5	Зачет	4				4
Всего за семестр		**108**	**6**	**–**	**10**	**88+4**

5. Виды образовательной деятельности

Тема. Криптографические способы защиты информации.

Лекция 1. Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard).

Лекция 2. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA.

Тема. Антивирусная защита

Лекция 3. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ. Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы.

Занятия семинарского типа

Лабораторные занятия.

Лабораторное занятие № 1. *Программирование алгоритма шифра Цезаря*
Цель занятия: разработать программу, реализующую шифр Цезаря

Задания для аудиторной работы

Задание. Построить программу, реализующую шифр Цезаря.

Лабораторное занятие № 2 -3. *Программирование алгоритма шифра Полибия*
Цель занятия: разработать программу, реализующую шифр Полибия

Задания для аудиторной работы

Задание. Построить программу, реализующую шифр Полибия.

Лабораторное занятие № 4-5. *Программирование алгоритма шифра Lucifer*
Цель занятия: разработать программу, реализующую шифр Lucifer

Задания для аудиторной работы

Задание. Построить программу, реализующую шифр Lucifer.
Задание. Построить программу, реализующую алгоритм построения электронной цифровой подписи.

Самостоятельная работа

Текущая самостоятельная работа направлена на углубление и закрепление знаний студентов и развитие их практических умений. Она заключается в работе с лекционными материалами, поиске и обзоре литературы и электронных источников, информации по заданным темам курса, опережающей самостоятельной работе, в изучении тем, вынесенных на самостоятельную проработку, подготовке к лабораторным занятиям.

Самостоятельная внеаудиторная работа студентов состоит в:

- проработке лекционного материала, составлении конспекта лекций по темам, вынесенным на самостоятельное изучение;
- выполнении домашних заданий.

Темы для самостоятельного изучения

1. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.
2. Шифрование с помощью аналитических преобразований.
3. Модульная арифметика.
4. Методы защиты от вредоносных программ.
5. Антивирусные комплексы.
6. Основы построения локальной компьютерной сети.
7. Управление ключами шифрования и безопасность сети.
8. Цифровая подпись.
9. Система обнаружения вторжений (IDS).
10. Контроллеры целостности файлов.

Консультирование студентов осуществляться в индивидуальном порядке на занятиях и во внеурочное время. Выполнение самостоятельной работы оценивается по электронным материалам, подготовленным студентами. Результаты деятельности накапливаются в индивидуальных портфолио студентов.

6. Критерии оценивания результатов освоения дисциплины (модуля)

6.1. Оценочные средства и критерии оценивания для текущей аттестации

Теоретические вопросы

1. Перечислите основополагающие документы по информационной безопасности.
2. Понятие государственной тайны.
3. Что понимается под средствами защиты государственной тайны?
4. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
5. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
6. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?

7. Что такое криптография?
8. Что такое криптографический ключ?
9. Что такое криптографическая система?
10. Что такое шифр?
11. Как классифицируются алгоритмы шифрования?
12. Что такое криптостойкость?
13. Какие требования предъявляют к шифрам?
14. Что такое криптоанализ?
15. В чем заключается фундаментальное правило криптоанализа?
16. Что такое криптографическая атака?
17. Каковы виды криптографических атак?
18. Чем различаются блочные и поточные шифры?
19. Описать алгоритм работы сети Файстеля.
20. Как работает SP-сеть?
21. Описать алгоритм работы криптосистемы Lucifer.
22. Что такое асимметричные криптосистемы?
23. Каковы особенности асимметричных криптосистем?
24. Что такое однонаправленная функция? Примеры однонаправленных функций.
25. Как работает криптосистема RSA? Привести пример.
26. Как работает алгоритм Диффи-Хеллмана? Привести пример.
27. Как работает алгоритм Эль-Гамаля? Привести пример.
28. Какие злоумышленные действия могут производиться с электронными документами?
29. Что такое электронная цифровая подпись?
30. Описать алгоритм электронной цифровой подписи RSA.
31. Какие процедуры включает система ЭЦП?
32. Какую информацию содержит ЭЦП?
33. Что такое стандарты и спецификации в области информационной безопасности?
34. Какой документ называется «Оранжевой книгой»?
35. По каким критериям оценивается степень доверия, которую можно оказать информационной системе?
36. Что такое доверенная вычислительная база?
37. Что такое ядро и периметр безопасности?
38. Какие элементы должна включать в себя политика безопасности?
39. Что такое средства подотчетности?
40. Какие классы безопасности определены в «Оранжевой книге»?
41. Что такое рекомендации X.800
42. Какие сервисы безопасности выделяются в этих рекомендациях?
43. Какие механизмы используются для реализации этих функций?
44. На какие направления распределяется администрирование средств безопасности?
45. Что такое «Общие требования»?
46. Что такое класс, семейство, компонент и элемент?
47. Что такое профиль защиты и задание по безопасности?
48. Каковы классы функциональных требований «Общих критериев»?
49. Каковы оценочные уровни доверия?
50. Каков основной критерий классификации межсетевых экранов согласно требованиям Гостехкомиссии России?
51. Что такое вредоносные программы?
52. Как распространяются вредоносные программы?
53. Что такое уязвимость?
54. Каковы могут быть последствия заражения вредоносными программами?
55. Какими могут явные последствия заражения?
56. Каковы типы вредоносных программ?
57. Что такое компьютерные вирусы и какими они бывают?

58. Что такое сетевой червь?
59. Что такое троян?
60. Каковы жизненные циклы вирусов, червей и троянов?
61. Какие еще бывают вредоносные программы?
62. Какова юридическая ответственность за распространение вредоносных программ?
63. Что такое удаленная атака?
64. Каковы основные причины уязвимости хостов сети?
65. Что такое анализ сетевого трафика?
66. Что такое подмена доверенного объекта или субъекта РВС?
67. Как осуществляется внедрение ложного объекта?
68. Как ложный объект может быть использован для организации удаленной атаки?
69. Что такое удаленная атака «отказ в обслуживании» и какие они бывают»?
70. Какие типовые уязвимости позволяют реализовать успешные удаленные атаки?
71. Как ложный ARP-сервер позволяет осуществлять удаленную атаку «Ложный объект РВС»?
72. Что такое DNS-сервер?
73. Как осуществляется внедрение ложного DNS-сервера путем перехвата DNS-запроса?
74. Как осуществляется внедрение ложного DNS-сервера путем создания направленного «шторма» ложных DNS-ответов на атакуемый хост ?
75. Как осуществляется внедрение в сеть ложного сервера?
76. Как создается ложный маршрутизатор?
77. Как осуществляется подмена субъекта TCP-соединения?
78. Как нарушается работоспособность хоста?
79. Что такое межсетевой экран?
80. Каковы виды межсетевых экранов?
81. Что такое межсетевые экраны прикладного уровня?
82. Что такое межсетевые экраны с пакетной фильтраций?
83. Что такое гибридные межсетевые экраны?
84. Что такое виртуальная частная сеть и какими характеристиками она обладает?
85. Что такое пользовательская VPN?
86. Что такое узловая VPN?
87. Каковы технологии функционирования VPN?
88. Каковы типы систем VPN?
89. Что такое IDS?
90. Каковы цели использования IDS?
91. Каковы типы IDS?
92. Какие бывают датчики IDS?
93. Что такое сетевая IDS?
94. Каковы действия при обнаружении вторжения?
95. Что такое цифровой сертификат?
96. Что такое бюро сертификатов?
97. Что такое иерархическая модель доверия?
98. Что такое сетевая модель доверия?
99. Как осуществляется сеанс SSL между клиентом и сервером?
100. Каковы преимущества использования электронной почты?
101. Каковы основные риски, связанные с использованием электронной почты?
102. Каковы требования к системам контроля содержимого электронной почты?
103. Что такое политика использования электронной почты?
104. Каковы методики отнесения электронных писем к спаму?

Критерии оценивания теоретических вопросов

Каждому студенту предлагается ответить на 5 произвольных теоретических вопросов. Ответ по каждому вопросу оценивается от 0 до 1 балла (в зависимости от содержательности ответа). Итоговая оценка по теме в разрезе теоретических вопросов складывается по формуле:

$$R = 2 + \frac{3}{5}\sum_{i=1}^{5} Q_i ,$$

где Q_i – баллы за ответ по каждому из вопросов.

Задания для лабораторных работ и задания для самостоятельной работы

Полный список типовых задач и заданий для самостоятельной работы представлен в материалах каждой лабораторной работы.

Задания для лабораторных и самостоятельной работ, образцы решений основных типовых задач практики также размещены в системе дистанционного обучения СмолГУ (www.moodle.smolgu.ru).

Критерии оценивания заданий из лабораторных работ и заданий для самостоятельной работы

Уровень выполнения	Оценка
Задание выполнено в полном объёме.	5 (отлично)
Задание выполнено в полном объёме с незначительными техническими ошибками.	4 (хорошо)
Задание выполнено не полностью.	3 (удовлетворительно)
Задание не выполнено.	2 (неудовлетворительно)

Оценка за выполнение заданий по лабораторной работе вычисляется как среднее арифметическое оценок за каждое задание по данной лабораторной работе.

Задачи из лабораторных работ

Полный список типовых задач представлен в материалах лабораторных работ. Оценивание решения задач из лабораторных работ проводится по тем же критериям, что и оценивание решения задач на экзамене.

6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

Зачетная контрольная работа

1. Самостоятельно построить программный продукт, реализующий один из криптографических алгоритмов.
2. Создать описание алгоритма программы.
3. Подготовить документацию по программе.

Критерии оценивания зачетной контрольной работы

1. Нормы оценивания работы

№ п/п	Структурная часть контрольной работы	Количество баллов (*)
1	Правильно реализован каждый метод решения	1 балл
2	Анализ результатов	2 балла

(*) Возможна градация в 0,25 балла.

2. Шкала оценивания работы:

п/п	Оценка	Количество баллов
1	Отлично	4,75-5
2	Хорошо	3,75-4,5
3	Удовлетворительно	3-3,5
4	Неудовлетворительно	менее 3

Критерии получения зачета

Зачет выставляется по результатам работы студента в течение семестра согласно Положению о текущем контроле успеваемости и промежуточной аттестации обучающихся в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Смоленский государственный университет» (утверждено приказом ректора № 01-113 от 26.09.2019 г.; внесены дополнения приказом ректора № 01-48 от 30.04.2020).

Для получения зачета студент должен:

- выполнить задания лабораторных работ на оценку не ниже «удовлетворительно»;
- выполнить задания для самостоятельной работы на оценку не ниже «удовлетворительно»;
- ответить на теоретические вопросы на оценку не ниже «удовлетворительно».

7. Перечень основной и дополнительной учебной литературы

7.1 Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477968 (дата обращения: 19.09.2021).
2. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469758 (дата обращения: 19.09.2021).

7.2. Дополнительная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/467370 (дата обращения: 19.09.2021).
2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2021. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469133 (дата обращения: 19.09.2021). URL: http://znanium.com/catalog.php?bookinfo=220424.

7.3. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. www.servernews.ru – информационные материалы о средствах ИТ и средствах обеспечения ИБ
2. www.fstec.ru – сайт ФСТЭК РФ
3. www.infosec.ru – группа компаний Информзащита
4. www.anti-malware.ru – аналитический центр Anti-Malware

8. Материально-техническое обеспечение

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие программе дисциплины (модулей), учебная ауд. 224 на 12 посадочных мест.

Перечень материально-технического обеспечения, необходимого для реализации курса, включает в себя лабораторию, оснащенную персональными компьютерами, объединенные в сеть с выходом в Интернет, проектором и интерактивной доской, ауд.224 на 12 посадочных мест и 6 парт (12 посадочных мест).

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную

информационно-образовательную среду университета, ауд.224 на 12 посадочных мест и 6 парт (12 посадочных мест).

9. Программное обеспечение

1. Операционная система MS Windows XP, Linux.
2. Система программирования MS Visual Studio 19
3. Поисковые системы сети Интернет.