МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ИГУ»)

Институт математики и информационных технологий

Кафедра вычислительной математики и оптимизации

«УТВЕРЖДАЮ»
Директор ИМИТ ИГУ
М. В. Фалалеев
«25» мая 2022 г.

Рабочая программа дисциплины (модуля)

Б1.О.34 Программные средства защиты информации

Направление подготовки	01.03.02 Прикладная математика и информатика
Направленность (профиль) подготовки	Прикладная математика и информатика
Квалификация выпускника	бакалавр
Форма обучения	очная

Иркутск 2022 г.

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цели: ознакомление с теоретическими основами и практическими решениями, обеспечивающими защиту информации в ЭВМ, формирование практических умений и навыков, необходимых для приобретения квалификации бакалавра.

Задачи: формирование представлений о принципах работы и особенностях эксплуатации программных средств защиты информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина Б1.О.34 Программные средства защиты информации относится к обязательной части Блока 1 образовательной программы.
Для изучения данной учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: Б1.О.26 Информатика и программирование

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: Б1.О.2 Управление проектами, Б1.О.29 Базы данных и системы управления базами данных, Б1.О.31 Проектирование информационных систем.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки 01.03.02 Прикладная математика и информатика:
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

В результате освоения дисциплины обучающийся должен
знать: основные виды угроз информационной безопасности и способы противодействия этим угрозам; формальные модели безопасности;
уметь: соблюдать основные требования по противодействию наиболее распространенным угрозам информационной безопасности; составлять политики безопасности уровня методов предприятия;
владеть: основными навыками защиты информации; приемами анализа и классификации угроз информационной безопасности; навыками применения средств защиты информации; основными навыками организации защиты информации на предприятии .

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных ед., 108 час.

Форма промежуточной аттестации: зачет с оценкой.

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

Раздел дисциплины / тема	Сем.	Виды учебной работы				Формы текущего контроля; Формы промежут. аттестации
		Контактная работа преподавателя с обучающимися			Самост. работа	
		Лекции	Лаб. занятия	Практ. занятия		
Тема 1. Факторы воздействующие на информацию			10		9	Проверка лаб. работы
Тема 2. Методы защиты программного кода			10		9	Проверка лаб. работы
Тема 3. Формальные модели безопасности			10		9	Проверка лаб. работы
Тема 4. Защита от разрушающих программных воздействий			10		9	Проверка лаб. работы
Тема 5. Защита информации при передаче по каналам связи			14		10	Проверка лаб. работы
Итого (2 семестр):			54		46	зач.с оц.

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Раздел дисциплины / тема	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самост. работы
	Вид самост. работы	Сроки выполнения	Затраты времени		
Тема 1. Факторы воздействующие на информацию	Изучение учебной литературы, методических материалов, подготовка к занятиям	3 неделя	9	Проверка лаб. работы	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР дисциплины на educa.isu.ru

Тема 2. Методы защиты программного кода	Изучение учебной литературы, методических материалов, подготовка к занятиям	6 неделя	9	Проверка лаб. работы	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР дисциплины на educa.isu.ru
Тема 3. Формальные модели безопасности	Изучение учебной литературы, методических материалов, подготовка к занятиям	9 неделя	9	Проверка лаб. работы	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР дисциплины на educa.isu.ru
Тема 4. Защита от разрушающих программных воздействий	Изучение учебной литературы, методических материалов, подготовка к занятиям	12 неделя	9	Проверка лаб. работы	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР дисциплины на educa.isu.ru
Тема 5. Защита информации при передаче по каналам связи	Изучение учебной литературы, методических материалов, подготовка к занятиям	16 неделя	10	Проверка лаб. работы	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР дисциплины на educa.isu.ru
Общая трудоемкость самостоятельной работы (час.)			46		
Из них с использованием электронного обучения и дистанционных образовательных технологий (час.)			46		

4.3. Содержание учебного материала

Тема 1. Факторы воздействующие на информацию
Объекты защиты. Угрозы информационной безопасности. Классификация угроз. Методы определения актуальных угроз. Виды нарушителей. Модели угроз и модели нарушителей информационной безопасности.
Тема 2. Методы защиты программного кода
Защита от несанкционированного копирования и использования программ. Защита программного кода от статического и динамического анализа. Приёмы защищенного программирования. Защита баз данных.
Тема 3. Формальные модели безопасности
Комплексная система защиты информации. Методы разграничения доступа субъектов к объектам защиты. Подсистема регистрации событий безопасности. Политика безопасности уровня предприятия.

Тема 4. Защита от разрушающих программных воздействий
Виды и классификация вредоносного ПО. Классификация программных ошибок. Признаки наличия на компьютере вредоносных программ. Политика применения средств антивирусной защиты.
Тема 5. Защита информации при передаче по каналам связи
Виртуальные частные сети. Организация защищенных подключений. Межсетевые экраны.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

Тема занятия	Всего часов	Оценочные средства	Формируемые компетенции
Тема 1. Факторы воздействующие на информацию	5	ЛР 1 «Опредление факторов, воздействующих на информацию»	ОПК-4
	5	ЛР 2 «Угрозы и уязвимости»	ОПК-4
Тема 2. Методы защиты программного кода	5	ЛР 3 «Статический анализ программного кода»	ОПК-4
	5	ЛР 4 «Статический анализ обфусцированного кода»	ОПК-4
Тема 3. Формальные модели безопасности	5	ЛР 5 «Разграничение доступа к ресурсам ЭВМ»	ОПК-4
	5	ЛР 6 «Подсистема регистрации событий безопасности»	ОПК-4
Тема 4. Защита от разрушающих программных воздействий	5	ЛР 7 «Поиск и анализ вредоносного ПО»	ОПК-4
	5	ЛР 8 «Применение средств сбора данныз для анализа действий злоумышленника»	ОПК-4
Тема 5. Защита информации при передаче по каналам связи	5	ЛР 9. «Создание VPN»	ОПК-4
	4	ЛР 10 «Классификация средств защиты»	ОПК-4
	5	ЛР 11 «Подбор СЗИ под конфигурацию системы»	ОПК-4

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы

Тема	Задание	Формируемые компетенции
Тема 1. Факторы воздействующие на информацию	Изучение материалов БДУ ФСТЭК, рекомендаций НКЦ КИ, учебной и методической литературы по дисциплине	ОПК-4

Тема 2. Методы защиты программного кода	Изучение основ языка ассемблера в части работы команд переходов, сравнений, вызовов процедур (по абсолютным и относительным адресам), учебной и методической литературы по теме	ОПК-4
Тема 3. Формальные модели безопасности	Изучение мандатной, дискреционной, ролевой, СВС, комбинированной моделей разграничения доступа. Изучение руководства администратора СЗИ «Аура», учебной и методической литературы по теме	ОПК-4
Тема 4. Защита от разрушающих программных воздействий	Изучения принципов функционирования средств антивирусной защиты, профилей САВЗ.	ОПК-4
Тема 5. Защита информации при передаче по каналам связи	Изучение руководства администратора ViPNet, приказов ФСТЭК, устанавливающих требования к классам СЗИ, требований к классам межсетевых экранов, учебной и методической литературы по теме	ОПК-4

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов всех форм и видов обучения является одним из обязательных видов образовательной деятельности, обеспечивающей реализацию требований Федеральных государственных стандартов высшего образования. Согласно требованиям нормативных документов самостоятельная работа студентов является обязательным компонентом образовательного процесса, так как она обеспечивает закрепление получаемых на лекционных занятиях знаний путем приобретения навыков осмысления и расширения их содержания, навыков решения актуальных проблем формирования общекультурных и профессиональных компетенций, научно-исследовательской деятельности, подготовки к семинарам, лабораторным работам, сдаче зачетов и экзаменов. Самостоятельная работа студентов представляет собой совокупность аудиторных и внеаудиторных занятий и работ. Самостоятельная работа в рамках образовательного процесса в вузе решает следующие задачи:
– закрепление и расширение знаний, умений, полученных студентами во время аудиторных и внеаудиторных занятий, превращение их в стереотипы умственной и физической деятельности;
– приобретение дополнительных знаний и навыков по дисциплинам учебного плана;
– формирование и развитие знаний и навыков, связанных с научно-исследовательской деятельностью;
– развитие ориентации и установки на качественное освоение образовательной программы;
– развитие навыков самоорганизации;
– формирование самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации;
– выработка навыков эффективной самостоятельной профессиональной теоретической, практической и учебно-исследовательской деятельности.

Подготовка к лекции. Качество освоения содержания конкретной дисциплины прямо зависит от того, насколько студент сам, без внешнего принуждения формирует у себя установку на получение на лекциях новых знаний, дополняющих уже имеющиеся по данной дисциплине. Время на подготовку студентов к двухчасовой лекции по нормативам составляет не менее 0,2 часа.

Подготовка к практическому занятию. Подготовка к практическому занятию включает следующие элементы самостоятельной деятельности: четкое представление цели и задач его проведения; выделение навыков умственной, аналитической, научной деятельности, которые станут результатом предстоящей работы. Выработка навыков осуществляется с помощью получения новой информации об изучаемых процессах и с помощью знания о том, в какой степени в данное время студент владеет методами исследовательской деятельности, которыми он станет пользоваться на практическом занятии. Подготовка к практическому занятию нередко требует подбора материала, данных и специальных источников, с которыми предстоит учебная работа. Студенты должны дома подготовить к занятию 3–4 примера формулировки темы исследования, представленного в монографиях, научных статьях, отчетах. Затем они самостоятельно осуществляют поиск соответствующих источников, определяют актуальность конкретного исследования процессов и явлений, выделяют основные способы доказательства авторами научных работ ценности того, чем они занимаются. В ходе самого практического занятия студенты сначала представляют найденные ими варианты формулировки актуальности исследования, обсуждают их и обосновывают свое мнение о наилучшем варианте. Время на подготовку к практическому занятию по нормативам составляет не менее 0,2 часа.

Подготовка к семинарскому занятию. Самостоятельная подготовка к семинару направлена: на развитие способности к чтению научной и иной литературы; на поиск дополнительной информации, позволяющей глубже разобраться в некоторых вопросах; на выделение при работе с разными источниками необходимой информации, которая требуется для полного ответа на вопросы плана семинарского занятия; на выработку умения правильно выписывать высказывания авторов из имеющихся источников информации, оформлять их по библиографическим нормам; на развитие умения осуществлять анализ выбранных источников информации; на подготовку собственного выступления по обсуждаемым вопросам; на формирование навыка оперативного реагирования на разные мнения, которые могут возникать при обсуждении тех или иных научных проблем. Время на подготовку к семинару по нормативам составляет не менее 0,2 часа.

Подготовка к коллоквиуму. Коллоквиум представляет собой коллективное обсуждение раздела дисциплины на основе самостоятельного изучения этого раздела студентами. Подготовка к данному виду учебных занятий осуществляется в следующем порядке. Преподаватель дает список вопросов, ответы на которые следует получить при изучении определенного перечня научных источников. Студентам во внеаудиторное время необходимо прочитать специальную литературу, выписать из нее ответы на вопросы, которые будут обсуждаться на коллоквиуме, мысленно сформулировать свое мнение по каждому из вопросов, которое они выскажут на занятии. Время на подготовку к коллоквиуму по нормативам составляет не менее 0,2 часа.

Подготовка к контрольной работе. Контрольная работа назначается после изучения определенного раздела (разделов) дисциплины и представляет собой совокупность развернутых письменных ответов студентов на вопросы, которые они заранее получают от преподавателя. Самостоятельная подготовка к контрольной работе включает в себя: — изучение конспектов лекций, раскрывающих материал, знание которого проверяется контрольной работой; повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения; изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний; составление в мысленной форме ответов на поставленные в контрольной работе вопросы; формирование психологической установки на успешное выполнение всех заданий. Время на подготовку к контрольной работе по нормативам составляет 2 часа.

Подготовка к зачету. Самостоятельная подготовка к зачету должна осуществляться в течение всего семестра. Подготовка включает следующие действия: перечитать все лекции, а также материалы, которые готовились к семинарским и практическим занятиям в течение семестра, соотнести эту информацию с вопросами, которые даны к зачету, если информации недостаточно, ответы находят в предложенной преподавателем литературе. Рекомендуется делать краткие записи. Время на подготовку к зачету по нормативам составляет не менее 4 часов.

Подготовка к экзамену. Самостоятельная подготовка к экзамену схожа с подготовкой к зачету, особенно если он дифференцированный. Но объем учебного материала, который нужно восстановить в памяти к экзамену, вновь осмыслить и понять, значительно больше, поэтому требуется больше времени и умственных усилий. Важно сформировать целостное представление о содержании ответа на каждый вопрос, что предполагает знание разных научных трактовок сущности того или иного явления, процесса, умение раскрывать факторы, определяющие их противоречивость, знание имен ученых, изучавших обсуждаемую проблему. Необходимо также привести информацию о материалах эмпирических исследований, что указывает на всестороннюю подготовку студента к экзамену. Время на подготовку к экзамену по нормативам составляет 36 часов для бакалавров.

В ФБГОУ ВО «ИГУ» организация самостоятельной работы студентов регламентируется Положением о самостоятельной работе студентов, принятым Ученым советом ИГУ 22 июня 2012 г.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература:

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК-Пресс. – 2010. – 542 с. – ISBN: 978-5-94074-518-1 (25 экз.).
2. Основы информационной безопасности [Текст] : учеб. пособие / [и др.] ; рец.: Ф. И. Иванов, Е. Н. Духан ; Иркутский гос. ун-т, Ин-т мат., экон. и информ. - Иркутск : Изд-во ИГУ, 2013. - 113 с. : ил. ; 25 см. - Библиогр.: с. 112-113. - ISBN 978-5-9624-0791-3 (31 экз).

б) дополнительная литература:

1. Герман О.Н. Теоретико-числовые методы в криптографии: учебник для студ. учреждений высш. проф. образования / О.Н. Герман. – М.: Академия. – 2012. – 257 с. – ISBN: 978-5-7695-6786-5. Режим доступа: ЭЧЗ «Библиотех». – Неогранич. Доступ.
2. Конеев И. Р. Информационная безопасность предприятия: научное издание / И. Р. Конеев, А. В. Беляев. – СПб.: БХВ-Петербург, 2003. – 733 с. – ISBN 5-94157-280-8 (39 экз).
3. Бабаш А.В. Информационная безопасность. Лабораторный практикум: учеб. пособие / А. В. Бабаш. – М.: КноРус, 2013. – 131 с. – ISBN 978-5-406-02760-8 (50 экз.).

в) базы данных, информационно-справочные и поисковые системы:

1. Microsoft TechNet (https://technet.microsoft.com/ , режим доступа неограниченный).

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование

ЭТОТ РАЗДЕЛ НЕ ЗАПОЛНЯТЬ

6.2. Программное обеспечение

1. СЗИ от несанкционированного доступа «Аура 1.2.4»;
2. Hiew 6.50 (http://www.hiew.ru/indexr.html);
3. DosBox 0.74 (https://www.dosbox.com/download.php?main=1);
4. Программный комплекс ViPNetв составе:
ViPNet Administrator,
ViPNet Координатор,
ViPNet Client КС2;
5. Антивирус AVZ (https://z-oleg.com/secur/avz/download.php);
6. Autopsy (https://www.autopsy.com/);
7. SysInternals Suite (https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite).

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Оценочные средства текущего контроля

Вид контроля	Контролируемые темы	Контролируемые компетенции
Защита отчета о лабораторной работе	1 - 5	ОПК-4

Примеры оценочных средств текущего контроля

1. Контрольные вопросы к лабораторной работе 9
1. Для каких объектов можно разграничить доступ?
2. Какова функция списков рассылки копий?
3. Что нужно сделать в ЦУС, чтобы пересоздать дистрибутивы ключей?

2. Контрольные вопросы к лабораторной работе 6
1. Каковы требования, предъявляемые ФСТЭК к классу, по которому сертифицирована СЗИ (до 3 требуемого уровня защищенности ПД включительно)?
2. Каким образом включается аудит файловой системы?
3. Какие события отразятся в журнале при открытии файла на чтение?

7.2. Оценочные средства для промежуточной аттестации

Список вопросов для промежуточной аттестации:

1. Основное определение информационной безопасности. Направления ИБ. Механизмы. Инструментарий.
2. Методы защиты информации. Виды противников и нарушителей информационной безопасности.

3. Угрозы информационной безопасности. Связь уязвимости, угрозы, нарушителя и риска.
4. Виды защищаемой информации. Носители защищаемой информации
5. Основные законодательные акты в области защиты информации.
6. Три вида нарушений безопасности. Меры по противодействию угрозам нарушения конфиденциальности, целостности, доступности.
7. Построение модели угроз и методики оценки рисков. Качественные и количественные методики оценки рисков.
8. Цели и задачи организации в области обеспечения информационной безопасности. Взаимодействие между субъектами. Правила безопасности. Уровни формирования политик безопасности.
9. Классификация вредоносных программ. Меры по их профилактике. Признаки присутствия вредоносных программ на компьютере.
10. Классификация программных ошибок. Этапы возникновения ошибок в программном коде.
11. Формальные модели безопасности. Мандатные и дискреционные модели управления доступом.
12. Состав и назначение подсистем комплексной системы защиты информации.
13. Виртуальные частные сети: назначение, архитектура, принципы работы.
14. Методы защиты программ от несанкционированного копирования и использования. Методы защиты программ от изучения.
15. Методы защиты баз данных. Типовые уязвимости БД и СУБД.

Примеры оценочных средств для промежуточной аттестации:

Пример тестового задания
Выберите все правильные ответы

1. Что из перечисленного относится к механизмам информационной безопасности?
а) управление пользователями
б) персонал
в) антивирусное обеспечение
г) контроль доступа

2. Что из перечисленного относится к инструментам информационной безопасности?
а) реагирование на инциденты
б) антивирусное обеспечение
в) системы обнаружения атак
г) управление пользователями

3. Перечислите методы защиты информации
а) технические
б) административные
в) силовые
г) правовые

4. Доступность – это
а) получение авторизованного доступа к информации со стороны уполномоченных лиц в разрешенный период времени
б) получение полного прямого доступа к данным
в) возможность изменения данных
г) получение авторизованного доступа к данным

5. Укажите угрозы, источник которых расположен вне контролируемой зоны
а) перехват данных, передаваемых по каналам связи
б) применение подслушивающих устройств
в) перехват побочных электромагнитных излучений
г) хищение носителей с конфиденциальной информацией

6. При построении систем с защитой от угроз нарушения конфиденциальности

применяют следующие меры
а) дублирование серверов
б) обеспечение физической безопасности
в) разграничение доступа
г) обеспечение корректности транзакций

7 При построении систем с защитой от угроз нарушения целостности применяют следующие меры
а) использование цифровых подписей
б) создание запаса в пропускной способности сетевого оборудования
в) организация контроля за перемещением сотрудников
г) разделение обязанностей
д) минимизация привилегий

8 Какие меры НЕ применяются при построении систем с защитой от угроз нарушения доступности
а) резервное копирование информации
б) организация мандатного разграничения доступа к информационным ресурсам
в) использование кластеров

9 Набор прав и обязанностей, которые можно применить к сотруднику в зависимости от его производственных функций называется
а) мандатом
б) ролью
в) учетной записью
г) набором привилегий

10. Источником угрозы некомпетентное использование системных утилит является
а) несанкционированные программноаппаратные средства
б) природа
в) санкционированные программноаппаратные средства

Разработчик: Муценек В.Е., старший преподаватель кафедры Информационных технологий