Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ (Сибстрин)»

УТВЕРЖДАЮ
Декан факультета __ИИТ___
_____Л.В. Ильина
«_15_»_____05_____20_17_г.

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА
по дисциплине
Информационная безопасность и защита информации
(полное наименование дисциплины)

Направление подготовки **09.03.02 «Информационные системы и технологии»,**
(код и наименование направления подготовки)
Наименование профиля Информационные системы и технологии
(наименование профиля)

Тип образовательной программы Программа академического Бакалавриата (2017-2021) **статус:** Вариативная часть

кафедра ИСТ **факультет** ИИТ **курс** 2,3

Таблица 1

Семестр и форма контроля	форма обучения:			Вид занятий и количество часов	форма обучения:		
	очная	очно-заочная	заочная		очная	очно-заочная	заочная
семестр (ы)	8	–	–	лекции, час	14	–	–
экзамен (ы)	8	–	–	практические (семинарские) занятия, час	14	–	–
зачёт (ы)	-	–	–	лабораторные занятия, час	14	–	–
курсовая работа	–	–	–	**Всего аудиторных занятий**, час	**42**	–	–
курсовой проект	–	–	–	самостоятельная работа, час	102	–	–
индивидуальное задание	-	–	–	**Итого по дисциплине**, час	**144**		

Общая трудоёмкость дисциплины составляет _4,0__ зачётных единиц

Рабочая программа обсуждена на заседании кафедры __ИСТ_____
и одобрена «15»_____05_____ 2017 г.

Заведующий кафедрой **ИСТ** _____ / Задорожный А.Ф./

1. ПАСПОРТ РАБОЧЕЙ УЧЕБНОЙ ПРОГРАММЫ ПО ДИСЦИПЛИНЕ
Информационная безопасность и защита информации
(полное наименование дисциплины)

Таблица 1.1

Основание для реализации дисциплины

Код и наименование направления подготовки:	09.03.02 Информационные системы и технологии (Академический бакалавриат)
Год утверждения ФГОС ВО:	2015
Наименование профиля подготовки:	-
Наименование кафедры, реализующей дисциплину:	Информационных систем и технологий
Наименование выпускающей кафедры (кафедр):	Информационных систем и технологий
Наименование примерной программы / профессионального стандарта (организация, год утверждения):	Проф. стандарты «Специалист по информационным системам» и «Руководитель проектов в области информационных технологий» Мин. труда и соц. защиты РФ, 2014 г.

Данная дисциплина нацелена на формирование следующих компетенций (в соответствии с **Картой реализации компетенций ОП вуза**, утверждённой деканом факультета):

Таблица 1.2

Карта формирования компетенций по дисциплине

Код и наименование компетенции	Требования к уровню освоения (по компонентам)
ОПК-4 Понимание сущности и значения информации в развитии современного информационного общества, соблюдения основных требований к информационной безопасности, в том числе государственной тайны.	**знать:** – Цели защиты информации. – Теоретические основы компьютерной безопасности. – Требования, предъявляемые к обеспечению безопасности информационных технологий. **уметь:** – Настраивать интерфейсы и наборы прав доступа, а также определять список пользователей, обладающих конкретным видом интерфейса и набором прав. – Проводить корректировку существующей конфигурации. – Уметь проводить сохранение и восстановление данных. – Разрабатывать процедуры управления объектами. – Вести и обрабатывать журналы. – Пользоваться средствами отладчика (точки останова, пошаговое выполнение) для отладки модулей конфигурации. **владеть:** – Навыками использования операционных систем реального времени в информационных системах. – Навыками создания управляющих последовательных и параллельных программ. – Основами функционирования операционных систем реального времени при управлении внешними устройствами. – Методами практического использования современных операционных систем реального времени компьютеров для обработки информации.
ПК-11.Способность к проектированию базовых и прикладных информационных технологий	**знать:** – Основные компоненты, принципы распространения и сопровождения систем информационной безопасности. – Сферы применения систем информационной безопасности. – Основы администрирования систем информационной безопасности.
	уметь: – Настраивать интерфейсы и наборы прав доступа, а также определять список

Код и наименование компетенции	Требования к уровню освоения (по компонентам)
	пользователей, обладающих конкретным видом интерфейса и набором прав. – Проводить корректировку существующей конфигурации. – Уметь проводить сохранение и восстановление данных. – Разрабатывать процедуры управления объектами. – Вести и обрабатывать журналы. – Пользоваться средствами отладчика (точки останова, пошаговое выполнение) для отладки модулей конфигурации
	владеть: – Средствами администрирования информационных систем. – Методами настройки файловых систем. – Способами планирования заданий пользователей. – Характеристика сетевой технологии internet. – Основные угрозы информационной безопасности организации при использовании Internet. – Основные приёмы защиты корпоративных сетей при использовании Internet.

Таблица 1.3

Характеристика уровней освоения дисциплины

Уровень освоения	Характеристика
1	**2**
Пороговый (удовлетворительно) 51 – 64 балла	Достигнутый уровень оценки результатов обучения показывает, что студент обладает необходимой системой знаний и владеет некоторыми умениями по дисциплине, способен понимать и интерпретировать освоенную информацию.
Продвинутый (хорошо) 65 – 84 балла	Достигнутый уровень оценки результатов обучения показывает, что студент продемонстрировал глубокие прочные знания и развитые практические умения и навыки, может сравнивать, оценивать и выбирать методы решения заданий, работать целенаправленно, используя связанные между собой формы представления информации.
Углубленный (отлично) 85 – 100 баллов	Достигнутый уровень оценки результатов обучения свидетельствует о том, что студент способен обобщать и оценивать информацию, полученную на основе исследования нестандартной ситуации; использовать сведения из различных источников, успешно соотнося их с предложенной ситуацией.

Примечание.

1. Количественные показатели уровня освоения дисциплины обучающимися, представленные в колонке **1**, являются **базовыми**.

2. По решению кафедры на основе **Положения о рейтинговой системе студентов НГАСУ (Сибстрин)** и при согласовании с председателем УМК факультета система балльного оценивания и её количественные показателя могут быть изменены.

2. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

2.1. Цель и задачи освоения дисциплины

Цель дисциплины:

Целью преподавания дисциплины является ознакомление студентов с основными сведениями о российском и зарубежном законодательстве в области информационной безопасности. Изучение основных средств и методов защиты информации. Получение навыков работы со специализированным программным обеспечением по обеспечению безопасности и защиты информации в информационных системах.

Задачи дисциплины:

В ходе освоения дисциплины студенты должны получить следующие знания и навыки:

- изучить основные понятия, ознакомится с методами защиты информации;

- изучить технические средства организации информационной безопасности;
- изучить основные функции современных систем информационной безопасности;
- привить умение управлять системами информационной безопасности;
- изучить меры по защите информации от несанкционированного доступа;
- изучить инструментальные средства разработки программ защиты информации;
- выполнять администрирование и конфигурирование систем информационной безопасности;
- привить умение самостоятельно изучать учебную литературу по системам информационной безопасности.

2.2. Место дисциплины в структуре ОП

Таблица 2.1

Предшествующие и сопутствующие дисциплины

№ п/п	Статус дисциплины по УП (базовая/вариативная)	Семестр	Наименование дисциплины («входные» знания, умения и компетенции)
Предшествующие дисциплины:			
1.	Базовая	4,5	Инструментальные средства информационных систем (ОС) (ОПК-6, ПК-11)
2.	Базовая	6	Инфокоммуникационные системы и сети (ОПК-6, ПК-12)
Сопутствующие дисциплины нет			

Таблица 2.2

Обеспечиваемые (последующие) дисциплины

№ п/п	Статус дисциплины по УП (базовая/вариативная)	Семестр	Наименование дисциплины
1.		8	Защита выпускной квалификационной роботы (ОПК-1,4,5,6 ПК-11,12,13,22,24,25)

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Темы учебной дисциплины

Тема 1. Средства и методы защиты информации.
Цели защиты информации. Теоретические основы информационной безопасности. Требования, предъявляемые к обеспечению безопасности информационных технологий. Организационно-правовое обеспечение информационной безопасности. Правовая база защиты информации
Тема 2. Сохранность и защита программных систем.
Общие технические средства и методы защиты информации. Криптографические методы защиты информации. Программно-аппаратные средства обеспечения информационной безопасности
Тема 3. Защита информации в сетях.
Модель OSI. Протоколы безопасности. Описание сетевых атак.
Тема 4. Средства защиты от несанкционированного доступа
Каналы утечки информации. Организационные меры по защите конфиденциальной информации. Межсетевое экранирование.
Тема 5. Персональные данные. Информационная система персональных данных
Основные определения. Категории персональных данных. Уровень за-щищенности персональных данных.
Тема 6. Системы информационной безопасности

Организационные вопросы корпоративной безопасности. Установка решения Kaspersky Security Center. Развертывание системы защиты на предприятии.

Тема 7. Аттестация объектов информатизации по требованиям безопасности информации

Организационные вопросы корпоративной безопасности. Установка решения Kaspersky Security Center. Развертывание системы защиты на предприятии.

3.2 Практические и семинарские занятия и их содержание

1. Криптография. Основные алгоритмы шифрования.
2. Шифрование и электронно-цифровая подпись документов. Программы защиты данных.
3. Обзор решения организации корпоративной безопасности. Инструменты управления безопасностью организации.
4. Изучение передовых технологий защиты от вредоносных программ. Инструменты защиты бизнеса от современных динамично развивающихся угроз.
5. Изучение средств защиты клиентских компьютеров. Установка и настройка параметров системы управления Kaspersky Security Center.
6. Риски потери данных в современных бизнес процессах.

3.3. Лабораторные занятия и их содержание

1. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации и знакомство с понятием криптографии.
2. Генерация открытых и закрытых ключей электронной цифровой подписи и шифрования. Изучение работы криптопровайдеров и программ защиты данных.
3. Изучение задач по управлению и обслуживанию системы защиты сети организации в программе Kaspersky Security Center.
4. Управление настройками сервера администрирования Kaspesky Security Center. Контроль рабочих мест.
5. Управление настройками сервера администрирования Kaspesky Security Center. Обслуживание рабочих мест.
6. Резервное копирование в Windows

3.4. Курсовой проект (работа) и его характеристика

[не предусмотрено]

3.5. Индивидуальное задание и его характеристика

[не предусмотрено]

Таблица 1

Распределение учебных часов по видам занятий

Темы дисциплин	Часы								
	лекции			практ. (лаб.) занятия			сам. работа		
Форма обучения (очная, очно-заочная, заочная):	О	О-З	З	О	О-З	З	О	О-З	З
Тема 1. Средства и методы защиты информации.	2			2(2)			14		
Тема 2. Сохранность и защита программных систем.	2			2(2)			16		
Тема 3. Защита информации в сетях.	2			2(2)			14		
Тема 4. Средства защиты от несанкционированного	2			2(2)			20		

Темы дисциплин	Часы								
	лекции			практ. (лаб.) занятия			сам. работа		
Форма обучения (очная, очно-заочная, заочная):	О	О-З	З	О	О-З	З	О	О-З	З
доступа									
Тема 5. Персональные данные. Информационная система персональных данных	2			2(2)			12		
Тема 6. Системы информационной безопасности	2			2(2)			14		
Тема 7. Аттестация объектов информатизации по требованиям безопасности информации	2			2(2)			12		
Итого:	14			14(14)			102		

3.6. Вопросы к зачету(экзамену)

1. Свойства информации
2. Субъекты информационной безопасности
3. Понятие авторизации
4. Понятие аутентификации
5. Основные алгоритмы шифрования
6. Определение вида шифра
7. Вирусы
8. Сетевые атаки
9. Межсетевой экран
10. Электронная цифровая подпись
11. Задачи DLP систем
12. Компоненты защиты Kaspersky Endpoint
13. Основные причины потери информации
14. Назначение и функционал Kaspersky Security Center
15. Агент администрирования Kaspersky Security Center
16. Методы резервного копирования
17. Системы резервного копирования
18. Виды резервного копирования
19. Разработка и внедрение системы резервного копирования
20. Аттестация объекта информатизации
21. Аккредитацию органов по аттестации

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

4.1. Основная и дополнительная литература

- Основная литература

1. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие / В. И. Аверченков. - Брянск : Брянский государственный технический университет, 2012. - 268 с.
2. Аверченков В.И**.** Защита персональных данных в организации [Электронный ресурс] : монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. - Брянск : Брянский государственный технический университет, 2012. - 124 с.
3. Башлы П.Н. Информационная безопасность **и** защита информации [Электронный ресурс] : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. -

Информационная безопасность **и** защита информации ; 2019-02-17. - Москва : Евразийский открытый институт, 2012. - 311 с.

- Дополнительная литература

1. О. Ю. Гаценко. Защита информации : основы организационного управления / О. Ю. Гаценко. - Санкт-Петербург : Сентябрь, 2001. - 227 с.
2. В. В. Арутюнов. Защита информации : учеб.-метод. пособие для вузов культуры и искусств и др. учеб. заведений / В. В. Арутюнов. - Москва : Либерея-Бибинформ, 2008. - 56 с.

- Периодические издания

1. Журнал "Информационные технологии и вычислительные системы".
2. Журнал "Информационные процессы и системы".
3. Журнал "Информационные технологии".

4.2. Информационные учебно-методические ресурсы

- Программное обеспечение

1. Microsoft Windows 7 (или более поздняя версия).
2. Microsoft Office 2007 (или более поздняя версия).
3. Turbo Pascal 6 (или более поздняя версия).
4. КриптоПРО CSP 3.6 (или более поздняя версия).
5. ViPNet CryptoFile 4 (или более поздняя версия).
6. ViPNet CSP 4.2 (или более поздняя версия).
7. Kaspersky security center 10 (или более поздняя версия).
8. Kaspersky Endpoint Security 10 (или более поздняя версия).

- Базы данных

1. Электронный каталог библиотеки НГАСУ (Сибстрин). – http://mega.sibstrin.ru/MegaPro/Web

- Интернет-ресурсы

1. *http:// support.kaspersky.ru (*Онлайн курсы Лаборатории Касперского)
2. *https://www.CryptoPro.ru/CertSrv* (Удостоверяющий центр КриптоПро)
3. https://files.infotecs.ru (Учебные материалы Infotecs)
4. http://www.cyberforum.ru/pascal/thread33245.html (Описание простых шифров с примерами Pascal)
5. *www.do.sibstrin.ru* (MOODLE- Портал дистанционного обучения НГАСУ (Сибстрин)).

4.3. Методические рекомендации по организации изучения дисциплины

Таблица 4.1

Используемые образовательные технологии

№ п/п	Наименование технологии	Вид занятий	Краткая характеристика
1.	Метод проблемного изложения материала.	Лекции	При проблемном изложении материала осуществляется снятие (разрешение) последовательно создаваемых в учебных целях проблемных ситуаций (задач). При рассмотрении каждой задачи преподаватель задает соответствующие вопросы и совместно со студентами формулирует итоговые ответы. Данный метод способствует развитию самостоятельного мышления обучающегося и направлен на формирование творческих способностей.
2.	Самостоятельная работа.	Лабораторные занятия	Самостоятельное изучение учебно-методической и справочной литературы позволит студенту осознанно выполнять задания и вести последующие свободные дискуссии по освоенному материалу.
3.	Интерактивная форма обучения.	Лекции, лабораторные работы	Технология интерактивного обучения – совокупность способов целенаправленного усиленного взаимодействия преподавателя и обучающегося, создающего условия для их развития. Современная интерактивная технология широко использует компьютерные технологии, мультимедийную технику и компьютерные сети.

Таблица 4.2

Используемые информационные ресурсы

№ п/п	Наименование информационных ресурсов	Вид занятий	Краткая характеристика
1.	Программное обеспечение	Лекционные, практические и лабораторные занятия, самостоятельная работа.	Изложение теоретического материала, выполнение аудиторных и индивидуальных заданий.
2.	Интернет-ресурсы	Лекции, лабораторные занятия, самостоятельная работа.	Самостоятельное обучение, выполнение аудиторных и индивидуальных заданий.

Таблица 4.3

Виды (формы) самостоятельной работы

:№ п/п	Наименование информационных ресурсов	Вид занятий	Краткая характеристика
1.	Программное обеспечение	Лекционные, практические и лабораторные занятия, самостоятельная работа.	Изложение теоретического материала, выполнение аудиторных и индивидуальных заданий.
2.	Базы данных	Практические занятия, самостоятельная работа.	Выполнение аудиторных заданий.
3.	Интернет-ресурсы	Лекции, лабораторные занятия, самостоятельная работа.	Самостоятельное обучение, выполнение аудиторных заданий.

5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Таблица 5.1

Требования к условиям реализации дисциплины

№ п/п	Вид аудиторного фонда	Вид занятий	Требования
1.	Лекционная аудитория	**Лекции**	Оснащение специализированной учебной мебелью. Оснащение техническими средствами обучения: настенный экран с дистанционным управлением, мультимедийное оборудование.
2.	Компьютерный класс	**Практические и лабораторные занятия**	Оснащение специализированной учебной мебелью. Оснащение техническими средствами обучения: ПК с возможностью подключения к локальным сетям и Интернету. Наличие ВТ из расчёта один ПК на два студента.

Таблица 5.2

Перечень материально-технического обеспечения дисциплины

№ п/п	Вид и наименование оборудования	Вид занятий	Краткая характеристика
1.	IBM PC-совместимые персональные компьютеры	**Практические и лабораторные занятия**	Процессор серии не ниже Pentium IV. Оперативная память не менее 512 Мбайт. ПК должны быть объединены локальной сетью с выходом в Интернет, установлен пакет MatLab+Simulink.
2.	Мультимедийные средства	**Лекции, практические и лабораторные занятия**	Демонстрация с ПК электронных презентаций, документов Word, электронных таблиц, графических изображений.

6. ВЫЯВЛЕНИЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

6.1. Фонд оценочных средств (ФОС) по дисциплине

Таблица 6.1

Паспорт фонда оценочных средств (ФОС) по дисциплине

п/п	Наименование оценочного средства	Технология	Вид аттестации	Коды формируемых компетенций
1.	Контрольные работы	Средство проверки умений проверять полученные знания для решения задач по пройденной теме	Промежуточные	**ОПК-4, ПК-11**
2.	Билеты к экзамену	Письменный экзамен	Итоговая аттестация по дисциплине	**ОПК-4, ПК-11**

6.2. Технология выявления уровня освоения дисциплины

При реализации дисциплины реализуются следующие технологии проведения промежуточной и итоговой аттестации по дисциплине для обеспечения условий достижения обучающимися соответствующего уровня освоения:

Краткий комментарий:

Экзамен сдают студенты, выполнившие все задания и защитившие все лабораторные работы, но имеющие рейтинг ниже 50 баллов, а также те студенты, которые хотят повысить экзаменационную оценку, проставленную по рейтингу.

Автор-разработчик _____ / Суханов А.С. /