

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 22.08.2025 10:48:57
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a196149ad36

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет Математики и информационных технологий
Кафедра Математического моделирования

Рабочая программа дисциплины (модуля)

дисциплина **Основы управления информационной безопасностью**

Блок Б1, базовая часть, Б1.Б.36

цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

10.03.01

Информационная безопасность

код

наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

Разработчик (составитель)
к. ф.-м. н., доцент
Гнатенко Ю. А.
ученая степень, должность, ФИО

1. Перечень планируемых результатов обучения по дисциплине (модулю)	3
1.1. Перечень планируемых результатов освоения образовательной программы	3
1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы .	3
2. Место дисциплины (модуля) в структуре образовательной программы	4
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся	4
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....	5
4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)	5
4.2. Содержание дисциплины, структурированное по разделам (темам)	5
5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю).....	8
6. Учебно-методическое и информационное обеспечение дисциплины (модуля)	8
6.1. Перечень учебной литературы, необходимой для освоения дисциплины	8
6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем	9
6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства	10
7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)	10

1. Перечень планируемых результатов обучения по дисциплине (модулю)

1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа:

Способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)
Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)
Способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Формируемая компетенция (с указанием кода)	Этапы формирования компетенции	Планируемые результаты обучения по дисциплине (модулю)
Способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)	1 этап: Знания	Обучающийся должен знать: содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем (АС) и подсистем безопасности АС
	2 этап: Умения	Обучающийся должен уметь: определять комплекс мер для обеспечения информационной безопасности АС
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: профессиональной терминологией в области управления ИБ
Способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	1 этап: Знания	Обучающийся должен знать: методику формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности
	2 этап: Умения	Обучающийся должен уметь: пользоваться методикой формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности
	3 этап: Владения	Обучающийся должен владеть:

	(навыки / опыт деятельности)	навыками формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности
Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)	1 этап: Знания	Обучающийся должен знать: основные методы управления информационной безопасностью
	2 этап: Умения	Обучающийся должен уметь: разрабатывать предложения по совершенствованию системы управления ИБ АС
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: методиками ФСТЭК России, ФСБ России по аттестации и сертификации объектов информатизации

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина реализуется в рамках базовой части. Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Теория информации», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Цифровая экономика», «Теоретические основы защиты информации», «Сети и системы передачи информации», «Техническая защита информации», «Электронный бизнес».

Дисциплина изучается на 4 курсе в 7 семестре

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зач. ед., 108 акад. ч.

Объем дисциплины	Всего часов
	Очная форма обучения
Общая трудоемкость дисциплины	108
Учебных часов на контактную работу с преподавателем:	
лекций	12
практических (семинарских)	18
лабораторных	18
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	34,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	24

Формы контроля	Семестры
-----------------------	-----------------

экзамен	7
---------	---

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	Наименование раздела / темы дисциплины	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
		Контактная работа с преподавателем			СР
		Лек	Пр/Сем	Лаб	
1	Система управления информационной безопасностью	12	18	18	24
1.1	Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.	2	0	0	3
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	2	2	0	3
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security	2	2	0	3
1.4	Современные методы и средства анализа и управление рисками информационных систем компаний	2	2	0	3
1.5	Правовые меры обеспечения информационной безопасности.	2	2	4	3
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	2	2	4	3
1.7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	0	4	4	3
1.8	Протоколирование и аудит, шифрование, контроль целостности	0	4	6	3
	Итого	12	18	18	24

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Система управления информационной безопасностью	
1.1	Основные понятия информационной	Понятие информационной безопасности.

	безопасности. Угрозы информационной безопасности в информационных системах.	Основные составляющие информационной безопасности. Управление информационной безопасностью. Важность и сложность проблемы информационной безопасности. Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Вредительские программы.
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	Роль стандартов ИБ. Оранжевая книга как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security	Этапы создания системы управления ИБ. Содержание этапов разработки и внедрения системы управления ИБ. Категорирование активов компании. Оценка защищенности информационной системы компании. Оценка информационных рисков. Обработка информационных рисков. Внедрение процедур системы управления ИБ. Расчет рисков по угрозе информационной безопасности. Описание архитектуры ИС. Расчет рисков по угрозе конфиденциальность.
1.4	Современные методы и средства анализа и управление рисками информационных систем компаний	Обоснование необходимости инвестиций в информационную безопасность компании. Методика FRAP. Методика OCTAVE (октэйв). Методика RiskWatch (риск вэтч).
1.5	Правовые меры обеспечения информационной безопасности.	Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии. Нормативные акты предприятия по

		информационной безопасности. Формы правовой защиты информации на предприятии. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	Общие положения организационной защиты. Особенности организационной защиты компьютерных информационных систем и сетей. Служба безопасности предприятия

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Система управления информационной безопасностью	
1.5	Правовые меры обеспечения информационной безопасности.	ЛАБОРАТОРНАЯ РАБОТА № 1 ПРАВОВЫЕ ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	ЛАБОРАТОРНАЯ РАБОТА №2: РЕАЛИЗАЦИЯ МОДЕЛИ ПОЛИТИКИ БЕЗОПАСНОСТИ
1.7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	ЛАБОРАТОРНАЯ РАБОТА № 3 ПРИМЕНЕНИЕ ИНВЕРСИОННОГО МЕТОДА ДЛЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ.
1.8	Протоколирование и аудит, шифрование, контроль целостности	ЛАБОРАТОРНАЯ РАБОТА №4: ПОСТРОЕНИЕ ЧАСТНОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Система управления информационной безопасностью	
1.2	Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	Сертификация СУИБ на соответствие ISO 27001.
1.3	Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security	Разработка политики ИБ
1.4	Современные методы и средства анализа и управление рисками информационных систем компаний	Разработка методики оценки рисков ИБ
1.5	Правовые меры обеспечения информационной безопасности.	Нормативные акты предприятия по информационной безопасности
1.6	Организационные меры обеспечения безопасности компьютерных информационных систем	Служба безопасности предприятия

1.7	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	Проведение внутреннего аудита ИБ
1.8	Протоколирование и аудит, шифрование, контроль целостности	Организация работы службы безопасности предприятия

5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)

Для эффективного освоения дисциплины изучение материала курса предполагает самостоятельную внеаудиторную работу, которая включает в себя выполнение индивидуальных заданий, подготовку к практическим и лабораторным занятиям, подготовку к докладам, конспектирование. Для успешного выполнения домашних заданий следует обратиться к задачам, решенным на предыдущих практических занятиях, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделах основная и дополнительная литература. Если, несмотря на изученный материал, задание выполнить не удастся, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия или лектора по дисциплине.

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1. Перечень учебной литературы, необходимой для освоения дисциплины

Основная учебная литература:

1. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия – Телеком, 2013. – 216 с. : ил. – (Вопросы управления информационной безопасностью. Вып. 4). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=253578> (дата обращения: 21.06.2021). – Библиограф. в кн. – ISBN 978-5-9912-0274-9. – Текст : электронный.
2. Основы управления информационной безопасностью: учебное пособие для вузов / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия – Телеком, 2013. – 244 с. : ил. – (Вопросы управления информационной безопасностью. Вып. 1). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=253575> (дата обращения: 21.06.2021). – Библиограф. в кн. – ISBN 978-5-9912-0271-8. – Текст : электронный.

Дополнительная учебная литература:

1. Коваленко, Ю. И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю. И. Коваленко. – Москва : Горячая линия – Телеком, 2012. – 140 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=253538> (дата обращения: 21.06.2021). – Библиограф. в кн. – ISBN 978-5-9912-0261-9. – Текст : электронный.

2. Кришталюк, А. Н. Правовые аспекты системы безопасности: курс лекций / А. Н. Кришталюк ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 204 с. : табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=428612> (дата обращения: 21.06.2021). – Библиогр. в кн. – Текст : электронный.

6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем

№ п/п	Наименование документа с указанием реквизитов
1	Договор на доступ к ЭБС ZNANIUM.COM между БашГУ в лице директора СФ БашГУ и ООО «Знаниум» № 3/22-эбс от 05.07.2022
2	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между БашГУ в лице директора СФ БашГУ и ООО «Электронное издательство ЮРАЙТ» № 1/22-эбс от 04.03.2022
3	Договор на доступ к ЭБС «Университетская библиотека онлайн» между БашГУ и «Нексмедиа» № 223-950 от 05.09.2022
4	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-948 от 05.09.2022
5	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-949 от 05.09.2022
6	Соглашение о сотрудничестве между БашГУ и издательством «Лань» № 5 от 05.09.2022
7	ЭБС «ЭБ БашГУ», бессрочный договор между БашГУ и ООО «Открытые библиотечные системы» № 095 от 01.09.2014 г.
8	Договор на БД диссертаций между БашГУ и РГБ № 223-796 от 27.07.2022
9	Договор о подключении к НЭБ и о предоставлении доступа к объектам НЭБ между БашГУ в лице директора СФ БашГУ с ФГБУ «РГБ» № 101/НЭБ/1438-П от 11.06.2019
10	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между УУНиТ в лице директора СФ УУНиТ и ООО «Электронное издательство ЮРАЙТ» № 1/23-эбс от 03.03.2023

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»)

№ п/п	Адрес (URL)	Описание страницы
1	https://www.garant.ru/	справочно-правовая система по законодательству Российской Федерации
2	http://www.consultant.ru/	Справочно-правовая система «Консультант +»
3	http://bdu.fstec.ru/	Банк данных угроз безопасности информации [Электронный ресурс] / ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
4	http://fstec.ru/	Официальный сайт ФСТЭК России [Электронный ресурс] / ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование программного обеспечения
AcademicEdition Networked Volume Licenses RAD Studio XE5 Professional Concurrent App / Плавающая – 60 шт. Бессрочная / ООО«Фермомобайл» / № 04182 от 03.12.2013
Visual Studio Community 2019 v.16.3 / OLP. Бессрочная / https://visualstudio.microsoft.com/ru/vs/community/
Kaspersky Endpoint Security / 950 / ООО «Смартлайн»/ №44/013 от 06.12.2021
Office Standart 2010 RUS OLP NL Acdmc / 200, Бессрочная / ООО «Компания Фермо» / № Ф-04211 от 12.03.2021
Windows 10 Education N / Бессрочная / Microsoft Imagine. Подписка №8001361124 от 04.10.2017 г.

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Тип учебной аудитории	Оснащенность учебной аудитории
Лаборатория аппаратных средств вычислительной техники. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия.
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций, учебная аудитория курсового проектирования (выполнения курсовых работ)	Доска, учебная мебель, проектор, экран, компьютеры, учебно-наглядные пособия.
Читальный зал: помещение для самостоятельной работы	учебная мебель, учебно-наглядные пособия, компьютеры