

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 30.10.2025 10:53:05
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 ***Б1.О.11 Информационная безопасность***

обязательная часть

Направление

01.04.02 ***Прикладная математика и информатика***
код наименование направления

Программа

Цифровые технологии в нефтегазовой отрасли

Форма обучения

Очно-заочная

Для поступивших на обучение в
2023 г.

Разработчик (составитель)
к.ф.-м.н., доцент
Викторов С. В.
ученая степень, должность, ФИО

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций	3
2. Цели и место дисциплины (модуля) в структуре образовательной программы	3
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).....	6
6. Учебно-методическое и информационное обеспечение дисциплины (модуля)	9
6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля).....	9
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	12
7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)	13

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)
ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1. Основные методы получения новых знаний с помощью информационных технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности; - стандарты оформления программной документации и причины нарушения компьютерной безопасности.	Обучающийся должен: знать способы получения на основе информационных технологий новых знаний для решения профессиональных задач с учетом требований информационной безопасности и причин нарушения безопасности компьютерных систем.
	ОПК-4.2. Применять информационные технологии в практической деятельности и анализировать полученные решения вычислительных задач; - на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств защиты информации; ориентироваться в современных и перспективных математических методах защиты информации.	Обучающийся должен: уметь применять информационные технологии для анализа и оценивания эффективности средств защиты информации; ориентироваться в современных и перспективных методах защиты информации.
	ОПК-4.3. Владение информационными технологиями как средством получения новых знаний; методами информационной и кадровой безопасности в коммуникационной деятельности.	Обучающийся должен: владеть навыками применения методов защиты информации в компьютерных системах; методами информационной и кадровой безопасности в коммуникационной деятельности.

2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:

Дисциплина «Информационная безопасность» является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

Основной задачей преподавания дисциплины является подготовка специалистов, обладающих знаниями, навыками, умениями в сфере обеспечения информационной безопасности организаций различных форм собственности.

Уровень освоения содержания дисциплины предполагает:

- Знакомство с основными понятиями информационной безопасности, информационными угрозами, их классификацией, и возможными последствиями для организаций различных форм собственности;

- Уяснение вопросов обеспечения информационной безопасности организации и проблем создания (концептуального проектирования) систем информационной безопасности;

- Принятие обоснованных решений по выбору политики информационной безопасности (ИБ) и оценки эффективности инвестиций в ИБ.

Знания, навыки и умения, приобретенные в процессе изучения дисциплины в ходе лекций, лабораторных занятий и самостоятельной работы, должны всесторонне использоваться студентами в процессе дальнейшей профессиональной деятельности.

В структуре образовательной программы дисциплина находится в обязательной части.

Дисциплина изучается на 3 курсе в 5 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 2 зач. ед., 72 акад. ч.

Объем дисциплины	Всего часов
	Очно-заочная обучения
Общая трудоемкость дисциплины	72
Учебных часов на контактную работу с преподавателем:	
лекций	4
практических (семинарских)	
лабораторных	8
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	59,8

Формы контроля	Семестры
зачет	5

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	Теоретические основы информационной безопасности	4	0	4	25
1.1	Основные понятия теории информационной безопасности	2	0	2	7
1.2	Информация как объект защиты	0	0	0	4
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	0	0	0	6
1.4	Угрозы информационной безопасности	2	0	2	8
2	Методология защиты информации	0	0	4	34,8
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	0	0	2	10
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	0	0	2	8
2.3	Политика и модели безопасности	0	0	0	8
2.4	Обзор международных стандартов информационной безопасности	0	0	0	8,8
	Итого	4	0	8	59,8

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Теоретические основы информационной безопасности	
1.1	Основные понятия теории информационной безопасности	История становления и предметная информационная безопасность область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации». Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации.
1.4	Угрозы информационной безопасности	Анализ уязвимостей системы. Классификация угроз информационной безопасности.

№ п/п	Тема и содержание	Задания по самостоятельной работе студентов
----------	-------------------	---

		<p>Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.</p>
--	--	---

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Теоретические основы информационной безопасности	
1.1	Основные понятия теории информационной безопасности	<p>Построения систем защиты. Задачи защиты информации. Средства реализации комплексной защиты информации.</p>
1.4	Угрозы информационной безопасности	Выбор мер защиты информации для автоматизированного рабочего места.
2	Методология защиты информации	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	<p>Методы защиты от несанкционированного доступа. Организационные и инженерно-технические методы защиты от несанкционированного доступа. Построение систем защиты от угрозы утечки по техническим каналам. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности информации.</p>
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	<p>Защита целостности информации при хранении, обработке, транспортировке. Построение систем защиты от угрозы отказа доступа к информации. Семантический анализ.</p>

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

		СР	
1	2	6	8
1.	Модуль 1	30	
1.1.	Основные понятия теории информационной безопасности. Информация как объект защиты	15	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к контрольной работе;
1.2.	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности. Угрозы информационной безопасности	15	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к контрольной работе;
2.	Модуль 2	23.8	
2.1.	Построение систем защиты от угрозы нарушения конфиденциальности. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	10	подготовка к индивидуальному опросу; подготовка к лабораторным работам;
2.2.	Политика и модели безопасности. Обзор международных стандартов информационной безопасности	13.8	подготовка к индивидуальному опросу; подготовка к лабораторным работам; подготовка к тестированию;
	Всего часов:	53.8	

Внеаудиторными формами и инструментами самостоятельной работы студентов по дисциплине являются: работа с конспектом лекций, изучение дополнительного теоретического материала, подготовка к занятиям, тестированию/контрольной работе.

Наименование тем на самостоятельное изучение:

1. Информационные войны и информационное противоборство.
2. Определение и основные виды информационных войн
3. Информационно-техническая война.
4. Информационно-психологическая война.

Вопросы для самоконтроля

1. Чем отличаются понятия «информационная война» и «информационное противоборство»?
2. Чем отличается информационная война от обычного вооруженного конфликта?
3. Какие виды информационных войн Вы можете выделить?
4. Приведите пример межкорпоративной информационной войны.
5. Можно ли рассматривать рекламу как средство ведения информационной борьбы?
6. Какие приемы ведения информационной войны используются во время предвыборных кампаний, приведите примеры.
7. Что такое информационное оружие? Какие виды оружия применяются в ходе ведения информационной войны?
8. Каковы цели информационной войны?
9. Каковы средства и методы защиты от информационно-технического оружия?
10. Каковы особенности информационно-психологической войны?

Рекомендуемая учебно-методическая литература:

1. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации): юридическая ответственность за правонарушения : учебное пособие / В. К. Новиков. – Москва : Горячая линия – Телеком, 2015. – 175 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=457171>.
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>.
3. Беляков, С. Л. Основы разработки программ на языке C++ для систем информационной безопасности : учебное пособие : [16+] / С. Л. Беляков, А. В. Боженюк, М. В. Петряева ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 152 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=612164>.
4. Сычев, Ю. Н. Основы информационной безопасности: учебно-практическое пособие : учебное пособие / Ю. Н. Сычев. – Москва : Евразийский открытый институт, 2010. – 328 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=90790>.

5. Галатенко, В. А. Основы информационной безопасности: Курс лекций : учебное пособие / В. А. Галатенко ; под ред. В. Б. Бетелина. – Изд. 3-е. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006. – 208 с. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=233063>.

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

6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)

Основная учебная литература:

1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562348> (дата обращения: 20.06.2023).
2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=574729> (дата обращения: 20.06.2023).
3. Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=362895> (дата обращения: 20.06.2023).

Дополнительная учебная литература:

1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562348> (дата обращения: 20.06.2023).
2. Основы информационной безопасности: учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – Москва : Горячая линия – Телеком, 2011. – 558 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=253056> (дата обращения: 20.06.2023).

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	http://www.anti-malware.ru/	Независимый информационно-аналитический портал по безопасности
2	https://securelist.ru/enciklopediya	Энциклопедия информационно й безопасности
3	http://www.content-filtering.ru/	Интернет- СМИ "Ваш личный Интернет" - помощь родителям в организации безопасного доступа детей в сеть Интернет
4	http://internetsecure.ru/	Набор технологий и программ для безопасной работы в сети с компьютером
5	http://www.securityportal.ru/	Сайт по защите информации, защите приватности, безопасным сетевым взаимодействиям,

6	http://www.oszone.net/6213/	криптографии. Обеспечение безопасности детей при работе в Интернет (статья, ссылки, материалы)
7	http://download.live.com/familysafety	Семейная безопасность — Windows Live - программа от компании Microsoft
8	http://nicekit.ru/	Программа родительского контроля
9	http://www.etika.ru/	Этика — сайт создан специально для пользователей Рунета, которые хотят работать в этичной, корректной и безопасной среде и готовы участвовать в создании такой среды
10	http://ru.wikipedia.org/wiki/Netiquette	Сетевой этикет — Википедия
11	http://www.securitylab.ru/software/1423/	Каталог программ «Защита детей от интернет угроз» (описание, сравнение, оценки)
12	http://laste.arvutikaitse.ee/rus/html/etusivu.htm	Основы безопасности в Интернете для молодежи интерактивный курс по Интернет-безопасности
13	http://www.antispam.ru/	Проект Антиспам.Ру
14	http://saferinternet.ru/	Портал Российского Оргкомитета по

		проведению Года Безопасного Интернета (ресурсы, ссылки, документы, материалы по проблематике)
15	http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?a id=cs_teach_kids	Вопросы безопасности — сайт от компании Symantec
16	http://www.microsoft.com/rus/protect/default.mspx#	Вопросы обеспечения информационно й безопасности от компании Microsoft
17	http://www.infoforum.ru/	Национальный форум информационно й безопасности "ИНФОФОРУМ " — электронное периодическое издание по вопросам информационно й безопасности
18	http://www.itn.ru/communities.aspx?cat_no=71586&tmpl=com	Обеспечение информационно й безопасности в учебных заведениях. 4 этапа защиты компьютера — советы от компании Microsoft.
19	http://www.citforum.ru/security/	CITFORUM — информационная безопасность (большое количество материалов по теме)

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

Наименование программного обеспечения
--

Kaspersky Endpoint Security
Office Standart 2007 Russian OpenLicensePack NoLevel Acdmc
Windows 10

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

Тип учебной аудитории	Оснащенность учебной аудитории
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, учебная мебель, проектор, экран, учебно-наглядные пособия.
Лаборатория технической защиты информации. 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.
Лаборатория программно-аппаратных средств обеспечения информационной безопасности. 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.
Лаборатория электричества и магнетизма. Учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций.	Доска, учебная мебель, оборудование для проведения лабораторных работ.
Читальный зал: помещение для самостоятельной работы.	Учебная мебель, учебно-наглядные пособия, компьютеры с доступом к сети «Интернет» и ЭИОС Филиала.