Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ

Декан факультета
СГФ
(наименование факультета)
И.В. Цевелева
(подпись, ФИО)
«____»_____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Введение в криптографию»

Направление подготовки Специальность	*46.03.02 Документоведение и архивоведение*
Направленность (профиль) образовательной программы Специализация	*Документационное обеспечение управления организацией*

Обеспечивающее подразделение
Кафедра «Истории и архивоведения»

Комсомольск-на-Амуре 2023

Разработчик рабочей программы:

д.т.н. профессор кафедры «Информационная безопасность автоматизированных систем		В.А.Челухин
(должность, степень, ученое звание)	(подпись)	(ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой *ИБАС*_____ (наименование кафедры)		А.А.Обласов
	(подпись)	(ФИО)
Заведующий выпускающей кафедрой[1]___ *Истории и культурологии* (наименование кафедры)		Ж. В.Петрунина
	(подпись)	(ФИО)

[1] Согласовывается, если РПД разработана не на выпускающей кафедре.

1 Общие положения

Рабочая программа дисциплины «Введение в криптографию» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Минобрнауки Российской Федерации 29 октября 2020 г. N 1343, и основной профессиональной образовательной программы подготовки «Документационное обеспечение управления организацией» по направлению подготовки «46.03.02 Документоведение и архивоведение».

Задачи дисциплины	Ознакомить студентов с основами криптографии и сформировать достаточно глубокие знания о: - Основных понятиях криптографии; - Основных задачах криптографии;
Основные разделы / темы дисциплины	Изучение теоретических принципов криптографии; Симметричная криптография Криптография с открытым ключом. Основные понятия о криптоанализе.

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины «Введение в криптографию» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой:

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по дисциплине
Общепрофессиональные		
ОПК-1 способностью использовать теоретические знания и методы исследования на практике	способность использовать теоретические знания и методы исследования криптографии на практике	*Знать:* З1(ОПК-1-2) виды информационных угроз; *Уметь: У1(ОПК-1-2) применять алгоритмы криптографии для защиты информации* *Владеть: Н1(ОПК-1-2) современными методами криптографической защиты информации*

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Введение в криптографию» изучается на 2 курсе в 4 семестре. Дисциплина входит в состав блока «Дисциплины (модули)» базовой части.
Место дисциплины (этап формирования компетенции) отражено в схеме формирования компетенций, представленной в документе *Оценочные материалы*, размещённом на сайте университета *www.knastu.ru / Наш университет / Образование / «Документоведение и архивоведение»/Оценочные материалы*).

4 Содержание дисциплины (модуля), структурированное по темам

(разделам) с указанием отведенного на них количества академических часов и видов учебной работы

4.1 Структура и содержание дисциплины для заочной формы обучения

Дисциплина «Введение в криптографию» изучается на 2 «курс» курсе в 4 семестре.

Общая трудоёмкость дисциплины составляет 3_ з.е., 108_ ч., в том числе контактная работа обучающихся с преподавателем _26 ч., промежуточная аттестация в форме зачета, 78 ч., самостоятельная работа обучающихся, в т.ч. контрольная работа 4 ч.

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
« Основные понятия и определения крипто-графии. История криптографии.	4					
Криптография с закрытыми ключами.	6			2		
Криптография с открытыми ключами	6			2		
Понятие о крипто ана-лизе	5					
Криптографическая стойкость	5					
Зачет	-	-	-	-		-
ИТОГО по дисциплине	**26**			4		78

* реализуется в форме практической подготовки

5 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обсуждаются и утверждаются на заседании кафедры. Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю) хранится на кафедре-разработчике в бумажном или электронном виде, также фонды оценочных средств доступны студентам в личном кабинете – раздел учебно-методическое обеспечение.

6 Учебно-методическое и информационное обеспечение дисциплины

(модуля)

6.1 Основная и дополнительная литература

Перечень рекомендуемой основной и дополнительной литературы представлен на сайте университета *www.knastu.ru / Наш университет / Образование / «Документоведение и архивоведение / Рабочий учебный план / Реестр литературы.*

6.2 Методические указания для студентов по освоению дисциплины

1. Введение в криптографию: Учебное пособие / Ященко В.В., - 4-е изд. - М.:МЦНМО, 2014. - 352 с // ZNANIUM.COM.: электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog/product/958585, ограниченный. – Загл. с экрана.

6.3 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Каждому обучающемуся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, с которыми у университета заключен договор.

Перечень рекомендуемых профессиональных баз данных и информационных справочных систем представлен на сайте университета *www.knastu.ru / Наш университет / Образование / «Документоведение и архивоведение / Рабочий учебный план / Реестр ЭБС.*

Актуальная информация по заключенным на текущий учебный год договорам приведена на странице Научно-технической библиотеки (НТБ) на сайте университета ***https://knastu.ru/page/3244***

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

На странице НТБ можно воспользоваться интернет-ресурсами открытого доступа по укрупненной группе направлений и специальностей (УГНС) «Документоведение и архивоведение» ***https://knastu.ru/page/539***

7 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) - русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

7.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традицион-

ные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

7.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

7.3 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

7.4 Методические рекомендации для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

8 Материально-техническое обеспечение, необходимое для осуществления образовательного процесса по дисциплине (модулю)

Для реализации программы дисциплины «Введение в криптографию» используется материально-техническое обеспечение:

Лицензионный сертификат № 47019898 от 11.06.2010

Microsoft® Office Professional Plus 2007 Russian
Microsoft® Office 2007 Russian
Лицензионный сертификат № 45806198 от 19.08.2009
Лицензионный сертификат № 43816080 от 21.04.2008
Лицензионный сертификат № 45286522 от 24.03.2009
Лицензионный сертификат № 44684774 от 19.08.2009
Лицензионный сертификат № 45503970 от 10.09.2008
Лицензионный сертификат № 44076027 от 07.06.2008
Лицензионный сертификат № 44260421 от 10.07.2008

Программа фиксации и контроля исходного состояния программного комплекса "Фикс" (версия 2.0.1) Лицензия № ЦС50-3309К325148

ПО ViPNet Client for Windows 4.x (КС2)
Сертификат № c6UJ9A007MHU/l-2 от 09.07.2018
Сертификат № c6UJ9A007MHU/l-3 от 09.07.2018
Сертификат № C6UJ9A007MHU/1-4 от 09.07.2018
Сертификат № c6UJ9A007MHU/l-5 от 09.07.2018
Сертификат № c6UJ9A007MHU/l-6 от 09.07.2018

8.1 Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства. Состав программного обеспечения, необходимого для освоения дисциплины, приведен на сайте университета *www.knastu.ru / Наш университет / Образование / Документоведение и архивоведение / Рабочий учебный план / Реестр ПО.*

Актуальные на текущий учебный год реквизиты / условия использования программного обеспечения приведены на странице ИТ-управления на сайте университета:

https://knastu.ru/page/1928

8.2 Учебно-лабораторное оборудование

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование	Назначение оборудования
325/3	Лаборатория программно-аппаратных средств защиты информации	Восемь ноутбуков Lenovo B500, проектор + экран для демонстрации.	Для проведения видео лекций, работы со специальными программами, проектными работами.

8.3 Технические и электронные средства обучения

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- зал электронной информации НТБ КнАГУ;
- компьютерные классы факультета.

9 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использо-

вания). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.