МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

Кафедра №51

«УТВЕРЖДАЮ»
Руководитель направления
доц.,к.ю.н.,доц.
(должность, уч. степень, звание)
Е.И.Сергеева
(подпись)
«25» июня 2020 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Название дисциплины)

Код направления	40.03.01
Наименование направления	Юриспруденция
Наименование направленности	Общая направленность
Форма обучения	очно-заочная

Санкт-Петербург 2020 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

доц.,к.т.н.,доц. _____20.05.2020 А.А.Овчинников

должность, уч.степень,звание подпись, дата инициалы,фамилия

Программа одобрена на заседании кафедры № 51

«20» мая 2020 г, протокол № 10

Заведующий кафедрой № 51

доц.,к.т.н.,доц. _____20.05.2020 А.А.Овчинников

должность, уч.степень,звание подпись, дата инициалы,фамилия

Ответственный за ОП 40.03.01(00)

доцент, к.ю.н.,,доц. _____ 25.06.2020 А.В.Баженов

должность, уч.степень,звание подпись, дата инициалы,фамилия

Заместитель директора института (декана факультета) № 9 по методической работе

доц.,к.ю.н.,доц. _____25.06.2020 Е.И.Сергеева

должность, уч.степень,звание подпись,дата инициалы,фамилия

Аннотация

Дисциплина «Основы информационной безопасности» входит в базовую часть образовательной программы подготовки обучающихся по направлению 40.03.01 «Юриспруденция» направленность «Уголовное право». Дисциплина реализуетсякафедрой №51.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-3 «владеть основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией»,

ОК-4 «способность работать с информацией в глобальных компьютерныхсетях»;

общепрофессиональныхкомпетенций:

ОПК-5 «способность логически верно, аргументированно и ясно строить устную и письменную речь»,

ОПК-7 «способность владеть необходимыми навыками профессионального общения на иностранном языке».

Содержание дисциплины охватывает круг вопросов, связанных с защитой компьютерной информации, существующих методов и информационных технологий этой защиты и оценкой их стойкости в информационных системах.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в формеэкзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения подисциплине

1.1. Цели преподавания дисциплины

Цель курса - научить студентов понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности.

В курс включены основные методы криптографии, применяемые в защите информации. Анализ криптографических алгоритмов органически связан с синтезом криптоалгоритмов и криптопротоколов. В результате изучения курса студенты должны получить представление об основном криптографическом инструментарии, необходимом для использования защищенных информационных систем.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоенияОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-3 «владеть основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией»:

знать - основные методы, способы и средства получения, хранения, переработки информации с учётом мер по еёзащите

уметь - формировать и реализовывать комплекс мер по обеспечению безопасности информации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз

владеть навыками - работы с компьютером как средством управления защищённой информацией

иметь опыт деятельности - в применении методов, способов и средств защиты информации в зависимости от условий задачи защиты информации;

ОК-4 «способность работать с информацией в глобальных компьютерных сетях»:

знать - существующие меры по обеспечению безопасности информации в глобальных компьютерных сетях

уметь - выбирать и применять средства защиты информации в зависимости от условий задачи защиты информации в глобальныхсетях

владеть навыками - установки и настройки средств обеспечения безопасности и целостности данных для информационных систем и технологий

иметь опыт деятельности - в пользовании криптографическими библиотеками для ЭВМ для решения прикладных задач в защищенных информационных системах;

ОПК-5 «способность логически верно, аргументированно и ясно строить устную и письменную речь»:

знать - основные виды угроз в сфере информационной безопасности и методы противодействия этимугрозам

уметь - логически верно, аргументированно и ясно оценивать риски от различных угроз в сфере информационной безопасности

владеть навыками – употребления отечественной терминологии в области криптографии для выражения количественных и качественных требований по защите информации

иметь опыт деятельности - применения технологий информационной защиты в своей профессиональной деятельности;

ОПК-7 «способность владеть необходимыми навыками профессионального общения на иностранном языке»:
знать – основные аналоги терминам и понятиям в области информационной безопасности на иностранном языке
уметь – составлять документацию на иностранном языке с применением терминов в области информационнойбезопасности
владеть навыками – профессионального общения на иностранном языке в области информационнойбезопасности
иметь опыт деятельности - по работе с литературой по информационной безопасности на иностранном языке.

2. Место дисциплины в структуреОП

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Информатика и информационные технологии в юридическойдеятельности;
- Информационноеправо.

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении другихдисциплин:

- Производственная преддипломнаяпрактика.

3. Объем дисциплины в ЗЕ/академ.час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебнойработы	Всего	Трудоемкость по семестрам
		№6
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
Аудиторные занятия, всего час., ***В том числе***	34	34
лекции (Л), (час)	17	17
Практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)	27	27
Самостоятельнаяработа,всего (час)	47	47
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Экз.	Экз.

4. Содержаниедисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видамзанятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр6					
Раздел 1. Основные понятия криптографии	2		2		6
Раздел 2. Симметричные шифры	6		4		8
Раздел 3. Криптография с открытым ключом	4		6		12
Раздел 4. Криптографические протоколы	5		5		12
Текущий контроль					9
Итого в семестре:	17		17		47
Итого:	17	0	17	0	47

4.2. Содержание разделов и тем лекционныхзанятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Тема 1.1. Основные определения Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно-техническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде. Тема 1.2. Задачи информационной безопасности Задача обеспечения конфиденциальности. Определение шифра. Задача обеспечения аутентификации, понятия об электронной цифровой подписи (ЭЦП). Основные задачи в области управления ключами. Криптопротоколы: обеспечение идентификации, разделение секрета, выработка ключа, цифровые деньги.
2	Тема 2.1. Исторические шифры Подстановочные шифры и перестановочные шифры. Шифр Цезаря, аффинный шифр, шифр моноалфавитной замены. Шифр Виженера. Цилиндр Джефферсона. Полиалфавитные шифры. Роторные машины. Тема 2.2. Блоковые шифры Понятие стойкости, предположения об исходных условиях криптоанализа, совершенная стойкость. Одноразовый блокнот. Шифр Вернама. Принципы построения блоковых шифров. Свойства смешивания и рассеивания. Составные шифры,

	итеративные шифры. SP-сети, сети Файстеля. Современные системы шифрования: алгоритмы DES, ГОСТ 28147-89, AES. Режимы блокового шифрования: ECB, CBC, CFB, OFB. Режим счетчика. Многократное шифрование. Тема 2.3. Потоковые шифры Требования к поточным шифрам. Методы построения больших периодов в поточных шифрах. Регистры сдвига с линейной обратной связью (РСЛОС). m-последовательности. Алгоритм Берлекэмпа-Месси. Построение потоковых шифров на основе РСЛОС. Нелинейное комбинирование РСЛОС: генератор Геффе, шифры с контролем тактов. Применение поточного шифрования.
3	Тема 3.1. Математические основы систем с открытым ключом Модульная арифметика. Алгоритм Евклида и его сложность. Расширенный алгоритм Евклида. Основные теоремы о вычетах. Функция Эйлера. Теоремы Эйлера, Ферма. Факторизация. Логарифмирование в конечных полях. Оценки сложности “трудных” проблем, на которых строятся системы с открытым ключом. Быстрое возведение в степень. Тема 3.2. Основные алгоритмы с открытым ключом Система Меркли-Хеллмана. Схема RSA. Атаки на RSA. Схема шифрования Эль-Гамаля. Система Мак-Элиса. Криптографические хэш-функции. Понятие о цифровой подписи. Подпись RSA. Подпись Эль-Гамаля. Подпись DSA. ЭЦП ГОСТ Р 34.10-94 и ГОСТ Р 34.10-01.
4	Тема 4.1. Основные протоколы с открытым ключом Выработка ключа. Протокол Диффи-Хелмана. Гибридные системы шифрования: цифровой конверт. Доказательство с нулевым разглашением. Схема идентификации Фиата-Шамира. Схема идентификации Гиллу-Квискуотера. Инфраструктура открытых ключей. Сертификаты открытых ключей. Тема 4.2. Специальные протоколы Слепая подпись. Протоколы разделения секрета и вручения бит. Протоколы цифровых денег и электронного голосования. Защищенные распределенные вычисления.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице4.

Таблица 4 – Практические занятия и ихтрудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисцип-лины
Учебным планом не предусмотрено				

4.4. Лабораторныезанятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	№ раздела дисциплины
Семестр 6			
1	Моно- и полиалфавитные шифры	1	1,2
2	Шифры гаммирования	2	2
3	Блочное шифрование	2	2
4	Криптографические протоколы	2	4
5	Хэш-функции	2	3
6	Ассиметричные системы шифрования	2	3
7	Электронная цифровая подпись	2	3
8	Методы доступа к информации	2	4
	Всего:	17	

4.5. Курсовое проектирование(работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельнойработы	Всего, час	Семестр 6, час
1	2	3
Самостоятельная работа, всего	47	47
Изучение теоретического материала дисциплины (ТО)	37	37
Подготовка к текущему контролю (ТК)	10	10

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине(модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 8-10.

6. Перечень основной и дополнительнойлитературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основнойлитературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляровв библиотеке (кроме электронных экземпляров)
004 М 87	Мошак Н. Н. Организациябезопасногодоступа к информационным ресурсам [Текст]: учебноепособие / Н. Н. Мошак, Т. М. Татарникова. приборостроения. - СПб.: Изд- во ГУАП, 2014. - 121 с.	40
Х404.3 М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А Клейменов. - 5-е изд., стер. - М.: Академия, 2011. - 331 с.	25

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительнойлитературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.4 К 84	Крук, Е. А. Методы программирования и прикладные алгоритмы [Текст]: учебное пособие в 3 ч. Ч. 1 / Е. А. Крук, А. А. Овчинников; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 178с.	40
004 М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография /Н.Н. Мошак. – Электрон.Текстовые дан. – СПб.: Изд-во ГУАП, 2014. – 197 с.	40

7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоениядисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование
https://www.pgpru.com/	Проект "OpenPGP в России"

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса подисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
1	Операционная система MS Windows *
2	Среда разработки MS Visual Studio
3	Пакет MS Office
4	Математический пакет MatLab

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочныхсистем

№ п/п	Наименование
1	http://libgost.ru/ Библиотека ГОСТов и нормативных документов

9. Материально-техническая база, необходимая для осуществления образовательного процесса подисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Фонд аудиторий ГУАП для проведения занятий лекционного и семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	
2	Вычислительная лаборатория МЦИТ ГУАП	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся подисциплине

10.1. Состав фонда оценочных средств приведен в таблице13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Экзамен	Список вопросов к экзамену; Задачи.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОК-3 «владеть основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией»	
1	Экономика
1	Информатика и информационные технологии в юридической деятельности
6	Основы информационной безопасности
ОК-4 «способность работать с информацией в глобальных компьютерных сетях»	
1	Информатика и информационные технологии в юридической деятельности
2	Учебная практика по получению первичных профессиональных умений и навыков
2	Правовая защита информации
3	Технические средства обеспечения правоохранительной деятельности
3	Экологическое право
5	Информационное право
6	Основы информационной безопасности
7	Криминология
7	Криминалистика
8	Конституционный механизм разделения властей
9	Производственная преддипломная практика
ОПК-5 «способность логически верно, аргументированно и ясно строить устную и письменную речь»	
1	Теория государства и права
1	Иностранный язык
1	Экономика
1	История
2	Правовая культура и юридическая риторика
2	История государства и права зарубежных стран
5	Информационное право
6	Основы информационной безопасности
6	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности
7	Криминология
8	Нотариат и адвокатура
9	Производственная преддипломная практика
ОПК-7 «способность владеть необходимыми навыками профессионального общения на иностранном языке»	
1	Иностранный язык
1	Информатика и информационные технологии в юридической деятельности
2	Иностранный язык в сфере юриспруденции
2	Основы социального государства
6	Основы информационной безопасности

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенцийприменяетсяшкламодульно–рейтинговойсистемыуниверситета.Втаблице 15 представлены 100–балльная и 4-балльная шкалы для оценки сформированности

компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
85 ≤К≤ 100	«отлично» «зачтено»	- обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно егоизлагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностьюнаправления; - умело обосновывает и аргументирует выдвигаемые имидеи; - делает выводы иобобщения; - свободно владеет системой специализированныхпонятий.
70 ≤К≤ 84	«хорошо» «зачтено»	- обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенныхнеточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научныеположения; - делает выводы иобобщения; - владеет системой специализированныхпонятий.
55 ≤К≤ 69	«удовлетво-рительно» «зачтено»	- обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки инеточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научныеположения; - затрудняется в формулировании выводов иобобщений; - частично владеет системой специализированныхпонятий.
К≤ 54	«неудовлетворительно» «не зачтено»	- обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретномнаправлении; - испытывает трудности в практическом примененииизнаний; - не может аргументировать научныеположения; - не формулирует выводов иобобщений.

10.4. Типовые контрольные задания или иныематериалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) дляэкзамена

№ п/п	Перечень вопросов (задач) для экзамена
1	Задача обеспечения секретности.
2	Шифры подстановок. Примеры.
3	Шифры перестановок. Примеры.
4	Стойкость шифров. Модель атакующего. Уровни атаки
5	Симметричные шифры. Свойства, принципы построения.
6	Итеративные блоковые шифры. Сети Файстеля. Примеры.
7	Шифр DES.
8	Шифр FEAL
9	Шифр ГОСТ 28147-89.
10	Шифр AES
11	Режимы блокового шифрования.
12	Асимметричные шифры. Свойства, принципы построения.
13	Система RSA.
14	Система Меркли-Хеллмана
15	Система Эль-Гамаля
16	Задача обеспечения аутентификации. Цифровая подпись.
17	Подпись RSA.
18	Подпись Эль-Гамаля.
19	Криптографические хэш-функции. Свойства, применение
20	Распределение симметричных ключей. Протокол Диффи-Хеллмана.
21	Распределение симметричных ключей. Цифровой конверт.
22	Распределение открытых ключей. Сертификаты открытых ключей

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф.зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Учебным планом не предусмотрено

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	Учебным планом не предусмотрено

4. Вопросы для проведения промежуточной аттестации при тестировании (таблица19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	Учебным планом не предусмотрено

5. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач /заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
1	Задание 1. Основы модульной арифметики (50 вариантов) Пример задания: Вариант 1. Вычислить: -17 mod44 -31 mod17 -49 mod16 -76 mod11 23 mod 50
2	Задание 2. Нахождение мультипликативных обратных с помощью алгоритма Евклида (50 вариантов) Пример задания: Вариант 1. Вычислить: 8011^{-1} mod16732
3	Задание 3. Быстрое возведение в степень (50 вариантов) Пример задания: Вариант 1. Вычислить: 19^{220} mod 73
4	Задание 4. Системы с открытым ключом: системы RSA, Мак-Элиса, Эль-Гамаля (индивидуальные варианты) Пример задания: Построить открытый и секретный ключи, зашифровать и расшифровать сообщение с помощью системы Мак-Элиса, для сообщения m = 100101. Параметр M определяется индивидуальным номером студента, остальные параметры системы выбрать самостоятельно.
5	Задание 5. Системы ЭЦП: системы RSA, Эль-Гамаля (индивидуальные варианты) Пример задания: Построить открытый и секретный ключи, подписать и проверить подпись сообщения с помощью системы Эль-Гамаля. Сообщение M определяется индивидуальным номером студента, размер открытого модуля p > 19, остальные параметры ЭЦП выбрать самостоятельно.

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «Омодульно-рейтинговой системе оценки качества учебной работы студентов вГУАП».

11. Методические указания для обучающихся по освоениюдисциплины

Цель дисциплины - научить студентов понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности.

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другимидисциплинами.

Планируемые результаты при освоении обучающимся лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретнойтеме;

– получение опыта творческой работы совместно спреподавателем;

– развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческогомышления.

– появление необходимого интереса, необходимого для самостоятельнойработы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшиегоды;

– научится методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различныхформулировках);

– получение точного понимания всех необходимых терминов ипонятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Основные понятия криптографии
Тема 1.1. Основныеопределения
Тема 1.2. Задачи информационной безопасности
Раздел 2. Симметричныешифры
Тема 2.1 Исторические шифры
Тема 2.2 Блоковые шифры
Тема 2.3 Потоковые шифры
Раздел 3. Криптография с открытым ключом
Тема 3.1 Математические основы систем с открытым ключом
Тема 3.2 Основные алгоритмы с открытым ключом
Раздел 4. Криптографические протоколы
Тема 4.1 Основные протоколы с открытым ключом
Тема 4.2 Специальные протоколы

Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках даннойдисциплины;
– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
– получение новой информации по изучаемойдисциплине;
– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению, а также с содержанием соответствующего лекционного курса, при необходимости – изучить самостоятельно дополнительную литературу. В соответствии с заданием обучающийся должен подготовить необходимые данные, выполнить задание лабораторной работы, получить требуемые результаты, оформить и защитить отчет по лабораторнойработе

Структура и форма отчета о лабораторной работе

Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы.

Требования к оформлению отчета о лабораторной работе

По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативнойдокументации».

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и

навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются учебно-методический материал подисциплине.

Для развития у студентов навыков самостоятельного овладения теоретическим материалом ряд тем дисциплины на лекционных занятиях дается обзорно, что предполагает их самостоятельное детальное изучение.

Примерные темы для самостоятельного изучения:

1. Метод тотального опробования ключей. Определение числа ключей в ряде конкретных схемшифраторов.
2. Протоколы цифровых денег
3. Роторныемашины.
4. Многократноешифрование.
5. Методы построения больших периодов в поточныхшифрах.
6. m-последовательности.
7. Нелинейное комбинированиеРСЛОС
8. Методы целочисленнойфакторизации
9. Методы вычисления дискретныхлогарифмов
10. Постквантоваякриптография
11. Доказательства с нулевымразглашением
12. Защищенные распределенныевычисления
13. Методы анализа хэш-функций. Вычисление вероятностейколлизий

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя экзамен.

Экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «Омодульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой