МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП

_____ Е.В Илова

«02» июня 2024 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой ИБ

_____ Т.Г. Гурская

«23» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы информационной безопасности в профессиональной деятельности

Составитель(-и)	**Выборнова О.Н., доцент, к.т.н., доцент кафедры ИБ** **Гурская Т.Г., доцент, к.т.н., доцент кафедры ИБ**
Направление подготовки	**45.05.01 Перевод и переводоведение.**
Направленность (профиль) ОПОП	**Лингвистическое обеспечение межгосударственных отношений (английский язык)**
Квалификация (степень)	**специалист**
Форма обучения	**очная**
Год приема	**2020**
Курс	**5**
Семестры	**9**

Астрахань, 2024

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целью освоения дисциплины (модуля) «Основы информационной безопасности в профессиональной деятельности» является развить общепрофессиональные компетенции в сфере информационной безопасности для эффективного и безопасного использования информационно-коммуникационных технологий в профессиональной деятельности.

1.2. Задачи освоения дисциплины (модуля):

- познакомить студентов с базовыми понятиями защиты информации, средствами и способами защиты информации.
- подготовить к безопасному использованию информационно-коммуникационных технологий в своей профессиональной деятельности.
- привить навыки использования разнообразных средств и методов обеспечения информационной безопасности.
- мотивировать самообразование и профессиональное развитие в области защиты информации (ЗИ).

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Основы информационной безопасности в профессиональной деятельности» относится к обязательной части и осваивается в 9 семестре.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями):

Информационные технологии в лингвистике и переводе.

Знания: основных понятий информатики, архитектуры ЭВМ и устройства ПК, представления данных в ЭВМ, основных закономерностей создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов.

Умения: использовать программные и аппаратные средства персонального компьютера, обосновывать актуальность и практическую значимость разрабатываемых мероприятий по обеспечению экономической безопасности.

Навыки и (или) опыт деятельности: навыки поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.): навыки прогнозирования возможных угроз экономической безопасности.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для который необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

1. Производственная (преддипломная) практика.
2. Дипломная работа.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины (модуля) направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки /специальности: ОПК-1, ОПК-2.

общепрофессиональных (ОПК): способностью работать с различными источниками информации, информационными ресурсами и технологиями, осуществлять поиск, хранение, обработку и анализ информации из разных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, владеть стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке (ОПК-1);

способностью соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности (ОПК-2).

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
способностью работать с различными источниками информации, информационными ресурсами и технологиями, осуществлять поиск, хранение, обработку и анализ информации из разных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, владеть стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке (ОПК-1)	ИОПК-1.1. Знать: роль информации в современном обществе, основы информационных технологий и информационной безопасности.	ИОПК-1.2. Уметь: применять информационные технологии и основы информационной безопасности для обеспечения объективных потребностей личности, общества и государства.	ИОПК-1.3. Владеть навыками использования информационных технологий и основ информационной безопасности для обеспечения объективных потребностей личности, общества и государства.

способностью соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности (ОПК-2)	ИОПК-2.1. Знать: основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	ИОПК-2.2. Уметь: применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности.	ИОПК-523. Владеть: навыками работы с нормативными правовыми актами, нормативными и методическими документами, регламентирующими деятельность по защите информации в сфере профессиональной деятельности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) в зачетных единицах 2 зачетные единицы, в том числе 26 часов, выделенных на контактную работу обучающихся с преподавателем (из них 13 часов – лекции, 13 часов – лабораторные работы) и 46 часов – на самостоятельную работу обучающихся.

Таблица 2 – Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
			Л	ПЗ	ЛР	КР	СР	
1	Место и роль информационной безопасности в системе национальной безопасности Российской Федерации.	9	3		3		10	Опрос. Доклад
2	Источники и классификация угроз информационной безопасности.		3		3		10	Опрос. Отчет по лабораторной работе 1.
3	Основные способы и средства защиты информации при работе на компьютере.		3		3		10	Опрос. Отчет по лабораторной работе 2
4	Правовые основы организации защиты		4		4		16	Опрос. Доклад

	государственной тайны и конфиденциальной информации.							
ИТОГО			**13**		**13**		**46**	**зачет**

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; КР – курсовая работа; СР – самостоятельная работа.

Таблица 3 – Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции		Общее количество компетенций
		ОПК 1	ОПК 2	
Место и роль информационной безопасности в системе национальной безопасности Российской Федерации.	16	+	+	2
Источники и классификация угроз информационной безопасности.	16	+	+	2
Основные способы и средства защиты информации при работе на компьютере.	16	+	+	2
Правовые основы организации защиты государственной тайны и конфиденциальной информации.	24	+	+	2
ИТОГО	72			

Краткое содержание каждой темы дисциплины (модуля)

Место и роль информационной безопасности в системе национальной безопасности Российской Федерации.

Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений». Объект и субъект защиты информации. Состав средств и мер защиты информации. Классификация средств и мер защиты информации. Основные сервисы ИБ. Концепция ИБ. Задачи системы безопасности.

Правовое обеспечение безопасности правового статуса субъектов информационной сферы. Содержание и структура законодательства. Конституция РФ. Федеральные законы, нормативные правовые акты Президента РФ, подзаконные акты Правительства РФ. Приказы ФСТЭК и ФСБ. Доктрина информационной безопасности РФ (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.). Закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ. Общие положения. Правовой режим информации. Право распространения и предоставления информации. Правовой статус обладателя информации. Правовой режим информационных технологий. Требования к государственным информационным системам. Порядок регулирования использования информационно-телекоммуникационных сетей. Защита информации.

Источники и классификация угроз информационной безопасности.

Понятие об источниках, носителях и получателях информации. Классификация источников информации. Источники технической и экономической информации при научных исследованиях, разработке, производстве и эксплуатации продукции, на различных этапах и видах коммерческой деятельности. Виды носителей информации (люди, физические поля, электрические сигналы и материальные тела).

Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства, и системы. Побочные электромагнитные излучения и наводки. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

Виды потенциальных угроз безопасности информации. Преднамеренные и случайные воздействия на источники информации. Утечка информации и ее особенности. Подходы к оценке уровня угрозы. Факторы, влияющие на возможность реализации угроз.

Характеристики каналов утечки информации. Структура технических каналов утечки информации. Отличия технического канала утечки информации от канала связи. Виды технических каналов утечки информации. Типовая структура технического канала утечки информации. Основные характеристики технических каналов утечки информации. Способы комплексного использования злоумышленниками технических каналов утечки информации.

Основные способы и средства защиты информации при работе на компьютере.

Технологические основы обработки конфиденциальных документов. Политика безопасности. Организация информации в сети Интернет. Службы сети Интернет. Интернет-провайдер (ISP). Адресация. Переадресация. Доменные имена. Длинные доменные имена. Виды доменных имен. Протоколы передачи данных. Семейство протоколов TCP/IP. Интернет. Безопасность. Браузер «Tor». Антивирусное программное обеспечение. Программы блокировки баннерной рекламы. Программы-фильтры спама. Программы восстановления после сбоя. Понятие «социальная сеть». Структура социальной сети. Социальная сеть «Вконтакте». Социальная сеть «Одноклассники». Деструктивная информация. Криптография как механизм защиты.

Понятие криптографии. Методы криптографии. Основные требования к шифрам для криптозащиты информации Криптографические методы защиты информации в среде Интернет. Шифрование электронной почты. Почтовые клиенты: Outlook, Thinderbird, The Bat. Электронная цифровая подпись (ЭЦП). определение, предназначение, состав.

Предмет и задачи программно-аппаратной защиты информации, основные подходы к защите данных от НСД. Основные принципы обеспечения информационной безопасности вычислительных систем с помощью программно-аппаратных средств. Функциональные требования по защите вычислительных систем. Особенности программно-аппаратного обеспечения безопасности в интерактивной среде. Защита электронной почты от злонамеренных и нежелательных воздействий, фальшивая и анонимная почта. Защита информационной среды от нежелательных информационных материалов, средства фильтрации сетевой информации/

Правовые основы организации защиты государственной тайны и конфиденциальной информации.

Категорирование информации. Определение общедоступной информации. Определение информации ограниченного доступа. Право на доступ к информации. Общие положения ФЗ «О государственной тайне». Понятие государственной тайны. Порядок отнесения сведений к государственной тайне (ГТ). Порядок засекречивания и рассекречивания. Сведения, не подлежащие отнесению к ГТ. Степени секретности сведений, составляющих ГТ. Порядок распоряжения сведениями, составляющими ГТ.

Система защиты сведений, составляющих ГТ. Допуск должностных лиц и граждан РФ к ГТ. Основания отказа должностному лицу или гражданину в допуске к ГТ. Постановление Правительства РФ от 04.09.1995 г. № 870 «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности». Указ Президента Российской Федерации от 24 января 1998 г. № 64 «О перечне сведений, отнесенных к государственной тайне» (с изменениями от 24 января 1998 г.) . Особенности работы с персоналом, владеющим конфиденциальной информацией. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Запрещенная к распространению информация. Нормативные акты, запрещающие распространение подобной информации. Постановление Правительства РФ от 03.11.1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. Указ Президента РФ от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ. 1997. № 10.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

При подготовке к лекционным занятиям необходимо воспользоваться учебно-методической литературой (основной) из п.8.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой (дополнительной) из п.8.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8 (основной), (дополнительной), Интернет-ресурсами.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер радела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
Место и роль информационной безопасности в системе национальной безопасности Российской Федерации.	Подготовка к устному опросу. «Доктрина информационной безопасности РФ». Закон РФ «Об информации, информационных технологиях и о защите информации». Подготовка доклада	10	Внеаудиторная, изучение учебных пособий
Источники и классификация угроз информационной безопасности.	Подготовка к устному опросу ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». Составление терминологического словаря.	10	Внеаудиторная, изучение учебных пособий

	Подготовка отчета по лабораторной работе 1		
Основные способы и средства защиты информации при работе на компьютере.	Подготовка к устному опросу. Составление терминологического словаря по документу «ФЗ РФ «Об электронной подписи». Подготовка отчета по лабораторной работе 2	10	Внеаудиторная, изучение учебных пособий
Правовые основы организации защиты государственной тайны и конфиденциальной информации.	Подготовка к устному опросу. Подготовка доклада	16	Внеаудиторная, изучение учебных пособий

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно

Отчет по лабораторной работе

Оформляется и отчитывается в электронном виде: формат листа А4, книжная ориентация страницы. Отчеты по всем лабораторным работам имеют единый титульный лист, на котором указывается наименование дисциплины, ФИО и группа исполнителя, ФИО преподавателя, принимающего отчеты. В отчете по каждой лабораторной работе должно быть представлено наименование работы, цель, ход выполнения работы (скриншоты, вычисления, краткое текстовое описание), выводы по результатам работы.

Доклад

Оформляется в электронном виде в форме презентации Power Point и пояснительной записки на листах формата А4 и может содержать задание, краткие необходимые теоретические сведения, полученные по каждому пункту задания результаты и выводы.

Выступление с докладом состоит из представления аудитории собранного материала и ответов на вопросы преподавателя и других обучающихся. В случае если оформление и поведение студента во время выступления соответствуют указанным требованиям, студент получает максимальное количество баллов.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Место и роль информационной безопасности в системе национальной безопасности Российской Федерации.	Обзорная лекция	Не предусмотрено	Защита доклада
Источники и классификация угроз информационной безопасности.	Лекция - презентация	Не предусмотрено	Выполнение лабораторной работы 1.

Основные способы и средства защиты информации при работе на компьютере.	Лекция - презентация	Не предусмотрено	Выполнение лабораторной работы 2
Правовые основы организации защиты государственной тайны и конфиденциальной информации.	Лекция - презентация	Не предусмотрено	Защита доклада

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

6.2. Информационные технологии

– использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т.д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т. е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

– использование виртуальной обучающей среды (LMS Moodle «Электронное обучение») или иных информационных систем, сервисов и мессенджеров.

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 10 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты

6.3.2. Современные профессиональные базы данных и информационные справочные системы

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Справочная правовая система КонсультантПлюс: http://www.consultant.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Основы защиты информации» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

№ п/п	Контролируемый раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
1.	Место и роль информационной безопасности в системе национальной безопасности Российской Федерации.	ОПК-1, ОПК-2	Вопросы для обсуждения. Доклад
2.	Источники и классификация угроз информационной безопасности.	ОПК-1, ОПК-2	Вопросы для обсуждения. Лабораторная работа 1.
3.	Основные способы и средства защиты информации при работе на компьютере.	ОПК-1, ОПК-2	Вопросы для обсуждения. Лабораторная работа 2.
4.	Правовые основы организации защиты государственной тайны и конфиденциальной информации.	ОПК-1, ОПК-2	Вопросы для обсуждения. Доклад

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлет-ворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлет-ворительно»	не способен правильно выполнить задание

7.3. Контрольные задания или иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Место и роль информационной безопасности в системе национальной безопасности Российской Федерации.

1. Вопросы для обсуждения.

1. Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений».
2. Объект и субъект защиты информации.
3. Состав средств и мер защиты информации. Классификация средств и мер защиты информации.
4. Основные сервисы ИБ. Концепция ИБ. Задачи системы безопасности.
5. Правовое обеспечение безопасности правового статуса субъектов информационной сферы.
6. Содержание и структура законодательства. Конституция РФ. Федеральные законы, нормативные правовые акты Президента РФ, подзаконные акты Правительства РФ. Приказы ФСТЭК и ФСБ.
7. Доктрина информационной безопасности РФ (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.).
8. Закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ. Общие положения. Правовой режим информации. Право распространения и предоставления информации.
9. Правовой статус обладателя информации. Правовой режим информационных технологий. Требования к государственным информационным системам. Порядок регулирования использования информационно-телекоммуникационных сетей.
10. Защита информации.

2. Доклад

Подготовить доклад по теме «Регламентация информационного обмена и информационной безопасности в … (стране по выбору учащегося)»

Источники и классификация угроз информационной безопасности.

1. Вопросы для обсуждения.

1. Понятие об источниках, носителях и получателях информации. Классификация источников информации. Источники технической и экономической информации при научных исследованиях, разработке, производстве и эксплуатации продукции, на различных этапах и видах коммерческой деятельности.
2. Виды носителей информации (люди, физические поля, электрические сигналы и материальные тела).
3. Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства, и системы.
4. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
5. Виды потенциальных угроз безопасности информации. Преднамеренные и случайные воздействия на источники информации.
6. Утечка информации и ее особенности. Подходы к оценке уровня угрозы. Факторы, влияющие на возможность реализации угроз.

7. Характеристики каналов утечки информации. Структура технических каналов утечки информации. Отличия технического канала утечки информации от канала связи.
8. Виды технических каналов утечки информации. Типовая структура технического канала утечки информации.
9. Основные характеристики технических каналов утечки информации.
10. Способы комплексного использования злоумышленниками технических каналов утечки информации.

2. Лабораторная работа 1

Парольная защита

Под **несанкционированным доступом к информации** (НСД) согласно руководящим документам Гостехкомиссии будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС. НСД может носить случайный или намеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

- организационные;
- технологические;
- правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация — это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация — это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя, В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

- индивидуального объекта заданного типа;
- знаний некоторой известной только ему и проверяющей стороне информации;

- индивидуальных биометрических характеристик.

Кпервой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем "подделать" биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (direct password authentication). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted third party authentication). При этом третью сторону называют сервером аутентификации (authentication server) или арбитром (arbitrator).

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

- по хранимой копии пароля или его свёртке (plaintext-equivalent);
- по некоторому проверочному значению (verifier-based);
- без непосредственной передачи информации о пароле проверяющей стороне (zero-knowledge);
- с использованием пароля для получения криптографического ключа (cryptographic).

Впервую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь").

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и

распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя — некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя — некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя — совокупность его идентификатора и его пароля. База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под **парольной системой** будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система представляет собой "передний край обороны" всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему. Ниже перечислены типы угроз безопасности парольных систем:

1. Разглашение параметров учетной записи через:
   - подбор в интерактивном режиме;
   - подсматривание;
   - преднамеренную передачу пароля его владельцем другому лицу;
   - захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);
   - перехват переданной по сети информации о пароле;
   - хранение пароля в доступном месте.
2. Вмешательство в функционирование компонентов парольной системы через:
   - внедрение программных закладок;
   - обнаружение и использование ошибок, допущенных на стадии разработки;
   - выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

- выбрать пароль, который легко запомнить и также легко подобрать;
- записать пароль, который сложно запомнить, и положить запись в доступном месте;
- ввести пароль так, что его смогут увидеть посторонние:
- передать пароль другому лицу намеренно или под влиянием заблуждения.

В дополнение к выше сказанному необходимо отметить существование "парадокса человеческого фактора". Заключается он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

Выбор паролей

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

Таблица 1

Требование к выбору пароля	**Получаемый эффект**
Установление минимальной длины пароля	Усложняет задачу злоумышленника при попытке подсмотреть пароль или подобрать пароль методом «тотального опробования»
Использование в пароле различных групп символов	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования»
Проверка и отбраковка пароля по словарю	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю
Установление максимального срока действия пароля	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования», в том числе без непосредственного обращения к системе защиты (режим off-line)
Установление минимального срока действия пароля	Препятствует попыткам пользователя заменить пароль на старый после его смены по предыдущему требованию
Ведение журнала истории паролей	Обеспечивает дополнительную степень защиты по предыдущему требованию
Применение эвристического алгоритма, бракующего пароли на основании данных журнала истории	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю или с использованием эвристического алгоритма
Ограничение числа попыток ввода пароля	Препятствует интерактивному подбору паролей злоумышленником
Поддержка режима принудительной смены пароля пользователя	Обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля
Использование задержки при вводе неправильного пароля	Препятствует интерактивному подбору паролей злоумышленником

Запрет на выбор пароля самими пользователями и автоматическая генерация паролей	Исключает возможность подобрать пароль по словарю. Если алгоритм генерации паролей не известен злоумышленнику, последний может подбирать пароли только методом «тотального опробования»
Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действия системного администратора, имеющего доступ к паролю в момент создания учетной записи

2. Примеры.

Пример 1.

Задание определить время перебора всех паролей, состоящих из 6 цифр.

Алфавит составляют цифры n=10.

Длина пароля 6 символов k=6.

Таким образом, получаем количество вариантов: $C=n^k=10^6$

Примем скорость перебора s=10 паролей в секунду. Получаем время перебора всех паролей $t= C/s=10^5$секунд≈1667минут≈28часов≈1,2 дня.

Примем, что после каждого из m=3 неправильно введенных паролей идет пауза в v=5 секунд. Получаем время перебора всех паролей T=t*5/3=16667секунд≈2778минут≈46часов≈1,9 дня.

$T_{итог} = t+T = 1,2 + 1,9 = 3,1$ дня

Пример 2.

Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.

Алфавит составляют символы n=10.

Длина пароля рассчитывается: $k=\log_n C= \lg C$.

Определим количество вариантов C= t * s=10лет*10 паролей в сек. = $10*10*365*24*60*60≈3,15* 10^9$ вариантов

Таким образом, получаем длину пароля: $k=\lg (3,15*10^9) = 9,5$ Очевидно, что длина пароля должна быть не менее 10 символов.

3. Задания.

1. Определить время перебора всех паролей с параметрами. Алфавит состоит из n символов.

Длина пароля символов k.

Скорость перебора s паролей в секунду.

После каждого из m неправильно введенных паролей идет пауза в v секунд

вариант	n	k	s	m	v
1	33	10	100	0	0
2	26	12	13	3	2
3	52	6	30	5	10
4	66	7	20	10	3
5	59	5	200	0	0
6	118	9	50	7	12
7	128	10	500	0	0
8	150	3	200	5	3
9	250	8	600	7	3
10	500	5	1000	10	10

2. Определить минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

вариант	n	t	s
1	33	100	100
2	26	120	13
3	52	60	30
4	66	70	20
5	59	50	200
6	118	90	50
7	128	100	500
8	150	30	200
9	250	80	600
10	500	50	1000

3. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

вариант	k	t	s
1	5	100	100
2	6	120	13
3	10	60	30
4	7	70	20
5	9	50	200
6	11	90	50
7	12	100	500
8	6	30	200
9	8	80	600
10	50	50	1000

3. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист с названиями университета, факультета, кафедры, учебной дисциплины и лабораторной работы, номером варианта, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы.

Основные способы и средства защиты информации при работе на компьютере.

1. Вопросы для обсуждения.

1. Технологические основы обработки конфиденциальных документов. Политика безопасности.
2. Организация информации в сети Интернет. Службы сети Интернет. Интернет-провайдер (ISP). Адресация. Переадресация. Доменные имена. Длинные доменные имена. Виды доменных имен.
3. Протоколы передачи данных. Семейство протоколов TCP/IP. Интернет. Безопасность. Браузер «Тор».

4. Антивирусное программное обеспечение.
5. Программы блокировки баннерной рекламы. Программы-фильтры спама. Программы восстановления после сбоя.
6. Понятие «социальная сеть». Структура социальной сети. Социальная сеть «Вконтакте». Социальная сеть «Одноклассники».
7. Деструктивная информация.
8. Криптография как механизм защиты. Понятие криптографии. Методы криптографии. Основные требования к шифрам для криптозащиты информации
9. Криптографические методы защиты информации в среде Интернет. Шифрование электронной почты. Почтовые клиенты: Outlook, Thinderbird, The Bat.
10. Электронная цифровая подпись (ЭЦП). определение, предназначение, состав.
11. Предмет и задачи программно-аппаратной защиты информации, основные подходы к защите данных от НСД.
12. Основные принципы обеспечения информационной безопасности вычислительных систем с помощью программно-аппаратных средств.
13. Функциональные требования по защите вычислительных систем. Особенности программно-аппаратного обеспечения безопасности в интерактивной среде.
14. Защита электронной почты от злонамеренных и нежелательных воздействий, фальшивая и анонимная почта.
15. Защита информационной среды от нежелательных информационных материалов, средства фильтрации сетевой информации.

2. Лабораторная работа 2

Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

Цель работы: освоение средств защищенных версий операционной системы Windows, предназначенных для

· разграничения доступа субъектов к папкам и файлам;

Подготовка к выполнению работы: по материалам лекций вспомнить и подготовить для включения в отчет о лабораторной работе определения понятий

· *дискреционная политика безопасности*;

· *мандатная политика безопасности*;

· *субъект доступа*;

· *объект доступа*;

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

1) в чем достоинства и недостатки дискреционной политики безопасности?

2) в чем достоинства и недостатки мандатной политики безопасности?

3) в чем заключается тождественность объектов и тождественность субъектов компьютерной системы?

4) кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?

Порядок выполнения работы:

1. После собеседования с преподавателем и получения допуска к работе войти в систему с указанным общим именем учетной записи (с правами обычного пользователя).

2. Освоить средства разграничения доступа пользователей к папкам:

· выполнить команду «Свойства» контекстного меню папки, содержащей отчеты студентов о выполненных лабораторных работах;

· открыть вкладку «Безопасность» и включить в отчет сведения о субъектах, которым разрешен доступ к папке и о разрешенных для них видах доступа;

· с помощью кнопки «Дополнительно» открыть окно дополнительных параметров безопасности папки (вкладка «Разрешения»);

· включить в отчет сведения о полном наборе прав доступа к папке для каждого из имеющихся в списке субъектов;

· открыть вкладку «Владелец», включить в отчет сведения о владельце папки и о возможности его изменения обычным пользователем;

· открыть папку «Аудит», включить в отчет сведения о назначении параметров аудита, устанавливаемых на этой вкладке, и о возможности их установки обычным пользователем;

· закрыть окно дополнительных параметров безопасности и с помощью кнопки «Изменить» а затем кнопки «Добавить» открыть окно выбора пользователя или группы;

· с помощью кнопок «Дополнительно» и «Поиск» открыть список зарегистрированных пользователей и групп и выбрать пользователя с именем своей индивидуальной учетной записи, созданной при выполнении лабораторной работы №1 (или предварительно создав новую учетную запись);

· назначить ему права на полный доступ к папке с отчетами о выполненных лабораторных работах;

· включить в отчет копии экранных форм, использованных при выполнении заданий данного пункта.

3. Освоить средства разграничения доступа пользователей к файлам:

· выполнить команду «Свойства» контекстного меню файла с одним из отчетов о ранее выполненных лабораторных работах;

· повторить все задания п. 2, но применительно не к папке, а к файлу;

· включить в отчет ответ на вопрос, в чем отличие определения прав на доступ к файлам по сравнению с определением прав на доступ к папкам.

4. Ознакомиться с правами доступа к файлам и папкам, назначаемым операционной системой по умолчанию:

· выполнить команду «Свойства» - «Безопасность» контекстного меню одной из папок с документами зарегистрированного в системе пользователя (например, « Мои Документы»);

· включить в отчет сведения о правах доступа пользователей к данной папке и о ее владельце;

· повторить два предыдущих пункта для папки с документами другого зарегистрированного пользователя;

· повторить два предыдущих пункта для папки «Общие документы»;

· включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта, и ответы на вопросы

¨ как обеспечивается операционной системой разграничение доступа к личным документам пользователей (по умолчанию);

¨ где (по умолчанию) должны находиться документы, предназначенные для совместного использования.

5. Включить в отчет о лабораторной работе ответы на контрольные вопросы:

· какая политика безопасности лежит в основе разграничения доступа к объектам в защищенных версиях операционной системы Windows?

· в чем уязвимость принятой в защищенных версиях операционной системы Windows политики разграничения доступа?

· как работает механизм наследования при определении прав на доступ субъектов к объектам в защищенных версиях операционной системы Windows?

· какой стандартный механизм работы с личными и общими документами предлагается в защищенных версиях операционной системы Windows и насколько, на Ваш взгляд, он удобен?

· каковы основные виды доступа к файлам и папкам?

6. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист с названиями университета, факультета, кафедры, учебной дисциплины и лабораторной работы, номером варианта, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы;
- ответы на контрольные вопросы.

Правовые основы организации защиты государственной тайны и конфиденциальной информации.

1. Вопросы для обсуждения.

1. Категорирование информации. Определение общедоступной информации. Определение информации ограниченного доступа. Право на доступ к информации.
2. Общие положения ФЗ «О государственной тайне». Понятие государственной тайны.
3. Порядок отнесения сведений к государственной тайне (ГТ). Порядок засекречивания и рассекречивания.
4. Сведения, не подлежащие отнесению к ГТ. Степени секретности сведений, составляющих ГТ.
5. Порядок распоряжения сведениями, составляющими ГТ. Система защиты сведений, составляющих ГТ.
6. Допуск должностных лиц и граждан РФ к ГТ. Основания отказа должностному лицу или гражданину в допуске к ГТ.
7. Постановление Правительства РФ от 04.09.1995 г. № 870 «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности».
8. Указ Президента Российской Федерации от 24 января 1998 г. № 64 «О перечне сведений, отнесенных к государственной тайне» (с изменениями от 24 января 1998 г.) Особенности работы с персоналом, владеющим конфиденциальной информацией.
9. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
10. Запрещенная к распространению информация. Нормативные акты, запрещающие распространение подобной информации.
11. Постановление Правительства РФ от 03.11.1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти.
12. Указ Президента РФ от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ. 1997. № 10.

2. Доклад

Тематика докладов

1. Виды информации.
2. Отрасли законодательства, регламентирующие деятельность по защите информации.
3. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
4. Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.

5. Требования к сотрудникам организации, допущенным к секретной (конфиденциальной) информации.
6. Органы лицензирования и сертификации в области ИБ.
7. Защита электронной почты от злонамеренных и нежелательных воздействий, фальшивая и анонимная почта
8. Порядок организации защиты ПДн
9. Понятие угрозы информационной безопасности. Классификация угроз ИБ
10. Классификация нарушителей информационной безопасности
11. Компьютеные «Вирусы». Их виды
12. Способы борьбы с компьютерными вирусами
13. Понятие и структура социальных сетей.
14. Распространение деструктивного материала через социальные сети и его влияние.
15. Передача информации в среде Интернет.
16. Программное обеспечение для безопасной работы в среде Интернет.
17. Основы конфиденциального документооборота
18. Технологические основы обработки конфиденциальных документов
19. Международные стандарты информационного обмена
20. Требования к сотрудникам организации, допущенным к секретной (конфиденциальной) информации.
21. Определение требований к защищенности информации
22. Типы нарушителей в сфере ИБ. Модель нарушителя в сфере ИБ.
23. Электронная цифровая подпись (ЭЦП)
24. Криптография как механизм защиты
25. Почтовые клиенты: Outlook, Thinderbird, The Bat.
26. Криптографические методы защиты информации.
27. Политика безопасности.
28. Общие положения сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
29. Система сертификации.
30. Порядок сертификации.

Вопросы к зачету

1. Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений».
2. Категорирование информации.
3. Виды возможных нарушений информационной системы. Общая классификация информационных угроз.
4. Объект и субъект защиты информации.
5. Определение понятия «Система информационной безопасности».
6. Допуск должностных лиц и граждан РФ к ГТ. Основания отказа должностному лицу или гражданину в допуске к ГТ.
7. Общие положения ФЗ «О государственной тайне». Порядок отнесения сведений к государственной тайне (ГТ).
8. Порядок засекречивания и рассекречивания. Сведения, не подлежащие отнесению к ГТ.
9. Степени секретности сведений, составляющих ГТ. Порядок распоряжения сведениями, составляющими ГТ.
10. Правовое урегулирование защиты информации. Стандарты ИБ.
11. Основы конфиденциального документооборота.
12. Особенности работы с персоналом, владеющим конфиденциальной информацией.
13. Регулирование правовых отношений в области защиты государственной тайны.

14. Конституция РФ. Федеральные законы, нормативные правовые акты в области информационной безопасности и защиты информации.
15. Законодательство о персональных данных. Принципы и условия обработки персональных данных, их конфиденциальность. Права субъектов персональных данных.
16. Особенности программно-аппаратного обеспечения безопасности в интерактивной среде.
17. Предмет и задачи программно-аппаратной защиты информации.
18. Классификация типовых программно-аппаратных средств обеспечения ИБ
19. Управление доступом пользователей в операционных системах
20. Криптография – как механизм защиты информации. Безопасность информации и защита информации.
21. Основные требования к шифрам для криптозащиты информации. Основные типы шифров.
22. ЭЦП: определение, предназначение, состав.
23. Криптографические методы защиты информации в среде Интернет.
24. Почтовые клиенты: Outlook, Thinderbird, The Bat. Сертификаты открытого и закрытого ключа.
25. Организация информации в сети Интернет.
26. Службы и протоколы сети Интернет: название службы, назначение и соответствующий протокол.
27. Сетевая безопасность. Антивирусные программы. Описание, примеры, достоинства и недостатки.
28. Социальные сети. Понятие, структура, типы, назначение, возможности. Примеры.
29. Деструктивная информация и ее распространение в среде Интернет.
30. Антивирусное программное обеспечение.
31. Программы блокировки баннерной рекламы.
32. Программы-фильтры спама.
33. Программы восстановления после сбоя.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
способностью работать с различными источниками информации, информационными ресурсами и технологиями, осуществлять поиск, хранение, обработку и анализ информации из разных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, владеть стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке (ОПК-1)				
1.	Задание закрытого типа	К угрозам информационной безопасности со стороны человеческого фактора НЕ относятся: 1) Действия уволенных или недовольных сотрудников 2) Анализаторы протоколов 3) Халатность 4) Низкая квалификация работников	2	2
2.		К техническим средствам обеспечения информационной безопасности и защиты информации относятся: 1) Недопущение ведения важных работ одним человеком	2	2

		2) Резервирование особо важных компьютерных подсистем 3) Защита авторских прав программистов		
3.		К техническим угрозам информационной безопасности НЕ относится: 1) Ошибки в программном обеспечении 2) Сетевые атаки, в том числе DoS- и DDoS-атаки 3) Промышленный шпионаж 4) Компьютерные вирусы, черви, троянские кони	3	2
4.		К организационным средствам обеспечения информационной безопасности и защиты информации относятся: 1) Совершенствование законодательства и судопроизводства 2) Тщательный подбор персонала 3) Установка средств обнаружения и тушения пожара, обнаружения утечек воды	2	2
5.		Цели защиты информации (указать несколько правильных ответов): 1) Целостность данных 2) Конфиденциальность данных 3) Доступность данных 4) Открытость данных	1,2,3	2
6.	Задание открытого типа	Какие меры относится к правовым мерам, направленным на обеспечение информационной безопасности и защиты информации?	Правовые нормы: разработка норм, устанавливающих ответственность за компьютерные преступления; защита авторских прав программистов; совершенствование законодательства и судопроизводства; общественный контроль за разработчиками компьютерных систем и приятие международных договоров, регламентирующих эту деятельность.	2
7.		Какие меры относится к техническим мерам, направленным на обеспечение информационной безопасности и защиты информации?	Технические меры: защита от несанкционированного доступа к информационной системе; резервирование особо важных компьютерных подсистем; организация вычислительных сетей с возможностью перераспределения ресурсов при нарушении в работе	2

			отдельных звеньев; установка средств обнаружения и тушения пожара, обнаружение утечек воды; принятие конструкционных мер защиты от хищений, диверсий, взрывов; установка резервного электропитания, оснащение помещений замками, сигнализацией.	
8.		В чем заключаются права обладателя информации в соответствии с ФЗ № 149 «Об информации, информационных технологиях и защите информации»?	Обладатель информации вправе: • разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа; • использовать информацию, в том числе распространять ее по своему усмотрению; • передавать информацию другим лицам по договору или на ином установленном законом основании.	2
9.		Какие меры относится к организационным мерам, направленным на обеспечение информационной безопасности и защиты информации?	Организационные меры: охрана вычислительного центра (ВЦ); тщательный подбор персонала; недопущение ведения важных работ одним человеком; наличие плана восстановления работоспособности ВЦ после выхода его из строя; обслуживание ВЦ сторонней организацией или лицами, незаинтересованными в сокрытии факторов нарушения работы центра; выбор места расположения центра.	2
10.		Правило разграничения доступа	Правило разграничения доступа заключается в следующем: лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа,	2

			содержатся все категории, определенные для данного документа.	
способностью соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности (ОПК-2)				
11.	Задания закрытого типа	Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» не может быть ограничен доступ к (указать несколько правильных ответов): 1) Информации о состоянии окружающей среды 2) Персональным данным граждан (физических лиц) 3) Информации о деятельности государственных органов и органом местного самоуправления, а также об использовании бюджетных средств	1,3	2
12.		Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» запрещается распространение информации, которая направлена на (указать несколько правильных ответов): 1) Пропаганду войны 2) Разжигание национальной вражды 3) Разжигание расовой или религиозной ненависти и вражды	1,2,3	2
13.		Конституция РФ содержит следующие нормы (указать несколько правильных ответов): 1) Конституция имеет высшую юридическую силу, прямое действие и применяется на всей территории Российской Федерации 2) Законы и иные правовые акты не должны противоречить Конституции РФ 3) Нормы международного права и международные договоры РФ являются частью ее правовой системы. Если международным договором РФ установлены иные правила, чем предусмотренные законом, то применяются правила международного договора	1,3	2
14.		Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» защита информации есть принятие мер, направленных на (указать несколько правильных ответов): 1) Предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования,	1,2,3	2

		копирования, предоставления, распространения и иных неправомерных действий в отношении информации 2) Соблюдение конфиденциальности информации ограниченного доступа 3) Реализацию права доступа к информации		
15.		Конституция РФ гарантирует следующие права и свободы (указать несколько правильных ответов): 1) Свободу мысли и слова 2) Право собираться мирно, без оружия, проводить собрания, митинги и демонстрации, шествия и пикетирование 3) Свободу массовой информации	1,2,3	2
16.	Задания открытого типа	Что понимается под тайной, секретностью и конфиденциальностью информации?	Тайна, или секретность и конфиденциальность информации, – это состояние информации в определенный период времени, которое характеризуется ограничением на ее распространение и доступ к ней в связи с ее защитой и охраной государством или иным обладателем документированной информации. Конфиденциальная информация (документы), составляющая тайну, за исключением государственной, – информация ограниченного доступа и распространения.	2
17.		Каким требованиям должна отвечать информация, отнесенная к служебной тайне?	Информация может являться служебной тайной, если она отвечает следующим требованиям: • отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости; • является конфиденциальной информацией другого лица (коммерческая тайна, банковская тайна, секрет производства (ноу-хау), служебный секрет	4

			производства, персональные данные); • не является государственной тайной и не попадает под перечень сведений, составляющих государственную тайну; • получена представителем государственного органа или органа местного самоуправления только в силу исполнения обязанностей по службе в случаях и в порядке, установленных федеральным законодательством, и имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам.	
18.		Основные направления обеспечения информационной безопасности в области обороны страны в соответствии с военной политикой Российской Федерации	В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются: а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий; б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства; в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере; г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;	4

			д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.	
19.		Дать определение информационной безопасности Российской Федерации	Информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства	2
20.		Что понимается под системой защиты от несанкционированного использования и копирования	Под системой защиты от несанкционированного использования и копирования понимается комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов.	2

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

Методические рекомендации по выполнению лабораторных и контрольных работ, проведению зачета

Отчет по лабораторной работе

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

Доклад

Доклад представляется в виде ответа по презентации по выбранной теме. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов

Основаниями для снижения оценки за задание являются:

- неполный ответ для теоретический заданий;
- небрежное выполнение.

Задание не может быть засчитано, если:

- представленный материал не соответствует заявленной теме

Оценивание студентов на **зачете** осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе зачета.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных и тематических контрольных работ. Он предусматривает проверку готовности студентов к плановым занятиям, оценку качества и самостоятельности выполнения заданий на практических занятиях, проверку правильности решения задач, выданных на самостоятельную проработку.

На зачете осуществляется комплексная проверка знаний, навыков и умений студентов по всему теоретическому материалу дисциплины и с проверкой практических навыков и умений по разработке документов различных видов. Теоретические знания оцениваются путем компьютерного тестирования или на основании письменных ответов студентов по нескольким теоретическим вопросам.

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Ответ на занятии*	13/4	52	По расписанию
2.	*Выполнение лабораторной работы*	2/10	20	
3.	*Доклад*	2/9	18	
Всего			**90**	-
Блок бонусов				
4.	*Посещение занятий без пропусков*	1	3	
5.	*Своевременное выполнение всех заданий*	1	3	
6.	*Активность студента на занятии*	1	4	

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Всего			**10**	-
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Основы информационной безопасности : Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - М. : Горячая линия - Телеком, 2011. – URL : http://www.studentlibrary.ru/book/ISBN5935172925.html (ЭБС «Консультант студента»).

2. Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А.А. - М. : ДМК Пресс, 2012. - URL : http://www.studentlibrary.ru/book/ISBN9785940746478.html (ЭБС «Консультант студента»).

3. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 4. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202749.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература:

1. Хорев, П.Б. Программно-аппаратная защита информации : рек. кафедрой информационной безопасности Российского государственного социального университета для студентов вузов, обучающихся по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев. - М. : ФОРУМ, 2009. - 352 с. - (Высшее образование). - ISBN 978-5-91134-353-8. (12 экз.)

2. Мельников, В.П. Информационная безопасность и защита информации [Текст] : учеб.пособие для вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 4-е изд., стер. – М. : Академия, 2009. – 332 с. (19 экз.)
3. Информационная безопасность и защита информации / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785940747680.html (ЭБС «Консультант студента»).
4. Защита информации: учебное пособие / Ю.М. Краковский - Ростов н/Д : Феникс, 2016. - (Высшее образование). URL: - http://www.studentlibrary.ru/book/ISBN9785222269114.html (ЭБС «Консультант студента»).

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебные аудитории, библиотеки АГУ, компьютерные классы, мультимедийные аудитории.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).