Министерство образования Красноярского края
краевое государственное бюджетное профессиональное образовательное учреждение
«Красноярский колледж радиоэлектроники и информационных технологий»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущей и промежуточной аттестации

ПО МЕЖДИСЦИПЛИНАРНОМУ КУРСУ
07.02 СЕРТИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 07
СОАДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ И СЕРВЕРОВ

для студентов специальности

09.02.07 Информационные системы и программирование

г. Красноярск, 2022

Составлена в соответствии с федеральным государственным образовательным стандартом СПО по специальности 09.02.07 Информационные системы и программирование

ОДОБРЕНО
Старший методист
_____ Т. В. Клачкова
«27» сентября 2022 г.

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ М. А. Полютова
«30» сентября 2022 г.

РАССМОТРЕНО

на заседании цикловой комиссии укрупненной группы специальностей 09.00.00 Информатика и вычислительная техника №1

Протокол №1 от «26» сентября 2022 г.

Председатель ЦК _____ Е.А. Ивашова

АВТОР: Казанкова А.А., преподаватель высшей квалификационной категории КГБПОУ «ККРИТ»

ПРОВЕРЕНО
Методист
_____Е.И. Макарова
«___»_____ 20__ г

СОДЕРЖАНИЕ

1 ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Область применения

Фонд оценочных средств предназначен для проверки результатов освоения междисциплинарного курса 07.02 Сертификация информационных систем, который является обязательной частью профессионального учебного цикла программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.07 Информационные системы и программирование.

Фонд оценочных средств позволяет оценить:

1.1.1. Освоенные умения и усвоенные знания:

Освоенные знания	***Усвоенные умения***
З 1. требования к безопасности сервера базы данных;	*У 1.* разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных;
З 2. государственные стандарты и требования к обслуживанию баз данных.	*У 2.* владеть технологиями проведения сертификации программного средства;

В результате освоения междисциплинарного курса 07.02 Сертификация информационных систем обучающийся должен:

иметь практический опыт:

- разработке политики безопасности SQL сервера, базы данных и отдельных объектов базы данных;
- применении законодательства Российской Федерации в области сертификации программных средств информационных технологий;

1.1.2. Освоение общих и профессиональных компетенций по профессиональному модулю:

ОК 1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 5 Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 9 Использовать информационные технологии в профессиональной деятельности.

ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языке.

ПК 7.4Осуществлять администрирование баз данных в рамках своей компетенции.

ПК 7.5Проводить аудит систем безопасности баз данных и серверов, с использованием регламентов по защите информации.

Формой промежуточной аттестации в соответствии с учебным планом специальности является дифференцированный зачет и экзамен (по семестрам).

Распределение оценивания результатов обучения по видам контроля.

1.2 Система контроля и оценки освоения программы учебной дисциплины (МДК)

Контролируемые элементы учебной дисциплины (темы)	Контролируемые знания, умения	Вид контроля	Форма контроля	Контрольно-оценочные материалы
Тема 1. Обеспечение качества информационных систем	знать: – законодательство Российской Федерации в области защиты информации; – способы защиты и сохранности информации баз данных.	Текущий	Выполнение практических заданий, оформление отчета, устный опрос, составление презентации, составление конспекта	Типовые метод. рекомендации к практическому занятию требования к оформлению отчетов, требования к устному опросу, презентации, конспекту (пункт 3)
Междисциплинарный курс 07.02 Сертификация информационных систем	**уметь:** – разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных; **знать:** – требования к безопасности сервера базы данных;	Промежуточный	Дифференцированный зачет	**Контрольно-оценочные материалы для промежуточной аттестации (Пункт 4).**
Тема 2. Обеспечение сертификация информационных систем	знать: – основы сертификации ИС; – автоматизированные средства аудита; – восстановление базы данных: основные алгоритмы и этапы.	Текущий	Выполнение практических заданий, оформление отчета, устный опрос	Типовые метод. рекомендации к практическому занятию требования к оформлению отчетов, требования к устному опросу (пункт 3)
Междисциплинарный курс 07.02 Сертификация информационных систем	**уметь:** – разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных;	Промежуточный	Экзамен	**Контрольно-оценочные материалы для промежуточной аттестации (Пункт 4).**

	– владеть технологиями проведения сертификации программного средства; **знать:** – требования к безопасности сервера базы данных; – государственные стандарты и требования к обслуживанию баз данных.			

2 ОРГАНИЗАЦИЯ КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

Формой промежуточной аттестации по учебной дисциплине ОП.02. Архитектура аппаратных средств в соответствии с учебным планом специальности СПО 09.02.07 Информационные системы и программирование является дифференцированный зачет и экзамен (по семестрам).

Условием допуска к соответствующему промежуточному контролю является положительный результат в ходе текущего контроля в процессе изучения учебной дисциплины и выполнения всех практических занятий (лабораторных работ), предусмотренных рабочей программой. Дифференцированный зачет проводится в форме устного опроса, включающему 1 теоретический вопроса. Вопросы к экзамену охватывают наиболее значимые из тем, предусмотренных рабочей программой. Экзамен проводится в форме устного опроса, обучающегося по билету, включающему 1 теоретический вопроса и 1 практическое задание. Вопросы к экзамену охватывают наиболее значимые из тем, предусмотренных рабочей программой.

При определении уровня достижений, обучающих на экзамене, учитывается:

– знание программного материла и структуры междисциплинарного курса;

– знания, необходимые для решения типовых задач, умение выполнять предусмотренные программой задания;

– владение методологией дисциплины, умение применять теоретические знания при решении задач, обосновывать свои действия.

При определении уровня достижений, обучающих на экзамене, обращается особое внимание на следующее:

– дан полный, развернутый ответ на поставленный вопрос;
– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные признаки, причинно-следственные связи;
– знание об объекте демонстрируются на фоне понимания его в системе данной дисциплины и междисциплинарных связей;
– ответ формулируется в терминах дисциплины, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающегося;
– теоретические постулаты подтверждаются примерами из практики.

Оценка «отлично» ставится за работу, выполненную без ошибок и недочетов или имеющую не более одного недочета;

- оценка «хорошо», ставится за работу, выполненную полностью, но при наличии в ней не более одной негрубой ошибки и одного недочета или не более двух недочетов;
- оценка «удовлетворительно» ставится в том случае, если студент правильно выполнил не менее половины работы или допустил:

а) не более двух грубых ошибок;
б) не более одной грубой ошибки и одного недочета;
в) не более двух-трех негрубых ошибок;
г) не более одной негрубой ошибки и трех недочетов;
д) при отсутствии ошибок, но при наличии 4-5 недочетов;

- оценка «неудовлетворительно» ставится, когда число ошибок и недочетов превосходит норму, при которой может быть выставлена оценка «3», или если правильно выполнено менее половины работы.

Грубыми являются ошибки, свидетельствующие о том, что студент не усвоил основные понятия темы, не знает формул, последовательность выполнения задания, не умеет формулировать выводы по результатам расчетов.

Негрубыми ошибками являются неточности расчетов, пропуск или неполное написание формул, неполное отражение результатов исследования в выводе.

К недочетам относятся небрежное выполнение заданий, отдельные погрешности в формулировке ответа.

3 КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением семинаров, оцениванием контрольных заданий, проверкой конспектов лекций, выполнением индивидуальных и творческих заданий, периодическим опросом обучающихся на занятиях. Ниже приведены методические рекомендации по выполнению всех видов текущего контроля в соответствии с рабочей программой.

3.1 Методические рекомендации по подготовке презентаций

На первом слайде размещается:

- название презентации;
- автор: ФИО, группа, название учебного учреждения (соавторы указываются в алфавитном порядке);
- год.

На втором слайде указывается содержание работы, которое лучше оформить в виде гиперссылок (для интерактивности презентации).

На последнем слайде указывается список используемой литературы в соответствии с требованиями, интернет-ресурсы указываются в последнюю очередь.

Оформить слайдов	
Стиль	• необходимо соблюдать единый стиль оформления; • нужно избегать стилей, которые будут отвлекать от самой презентации; • вспомогательная информация (управляющие кнопки) не должны преобладать над основной информацией (текст, рисунки)
Фон	• для фона выбираются более холодные тона (синий или зеленый)
Использование цвета	• на одном слайде рекомендуется использовать не более трех цветов: один для фона, один для заголовков, один для текста; • для фона и текста используются контрастные цвета; • особое внимание следует обратить на цвет гиперссылок (до и после использования)
Анимационные эффекты	• нужно использовать возможности компьютерной анимации для представления информации на слайде; • не стоит злоупотреблять различными анимационными эффектами; анимационные эффекты не должны отвлекать внимание от содержания информации на слайде
Представление информации	
Содержание информации	• следует использовать короткие слова и предложения; • время глаголов должно быть везде одинаковым; • следует использовать минимум предлогов, наречий, прилагательных; • заголовки должны привлекать внимание аудитории
Расположение информации на странице	• предпочтительно горизонтальное расположение информации; • наиболее важная информация должна располагаться в центре экрана; • если на слайде располагается картинка, надпись должна располагаться под ней.
Шрифты	• для заголовков не менее 24; • для остальной информации не менее 18;

- шрифты без засечек легче читать с большого расстояния;
- нельзя смешивать разные типы шрифтов в одной презентации;
- для выделения информации следует использовать жирный шрифт, курсив или подчеркивание того же типа;
- нельзя злоупотреблять прописными буквами (они читаются хуже, чем строчные).

Способы выделения информации	Следует использовать: • рамки, границы, заливку • разные цвета шрифтов, штриховку, стрелки • рисунки, диаграммы, схемы для иллюстрации наиболее важных фактов
Объем информации	• не стоит заполнять один слайд слишком большим объемом информации: люди могут единовременно запомнить не более трех фактов, выводов, определений. • наибольшая эффективность достигается тогда, когда ключевые пункты отражаются по одному на каждом отдельном слайде.
Виды слайдов	Для обеспечения разнообразия следует использовать разные виды слайдов: с текстом, с таблицами, с диаграммами.

3.2 Требования к оформлению отчетов по практическим занятиям

Практические работы выполняются на компьютере в соответствии с выданными методическими указаниями. Результатом выполнения работы является отчет о проделанной работе, который должен быть распечатан и сложен в специальную папку на листах формата А4, которые должны быть скреплены. Первый (титульный) лист (приложение 1) должен содержать сведения об исполнителе.

Студент должен защитить практическую работу индивидуально. Подвести итог и сформулировать основные выводы. Сдать работу преподавателю (т.е. защитить её на оценку) можно на том же занятии, на котором она выполнялась. Защита практической работы осуществляется путем частичной демонстрации проделанной работы и ответов на контрольные вопросы, приведенных в конце методических указаний.

Структура отчета практической работы:

1. Цель и задачи работы. Формулируются в соответствии с метод. указаниями.
2. Ход работы. Выполнение предложенных заданий.
3. Описание выполненной работы, сопровождаемой скриншотами.
4. Выводы.

Программа практических работ по учебной дисциплине:

ТЕМА 1. ОБЕСПЕЧЕНИЕ КАЧЕСТВА ИНФОРМАЦИОННЫХ СИСТЕМ

ПЗ№1. Анализ лицензионного соглашения на использование услуг популярных интернет-сервисов.

ПЗ№2. Настройка политики безопасности.

ПЗ№3. Восстановление носителей информации.

ПЗ№4. Восстановление удаленных файлов.

ПЗ№5. Мониторинг активности портов.

ПЗ№6. Блокирование портов.

ТЕМА 2. ОБЕСПЕЧЕНИЕ СЕРТИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

ПЗ№7. Анализ современных автоматизированных средств аудита.

ПЗ№8. Брандмауэры.

ПЗ№9. Анализ качества программной продукции с точки зрения безопасности.

ПЗ№10. Анализ качества конфигурации серверного оборудования.

ПЗ№11. Анализ качества конфигурации локальных сетей.

ПЗ№12. Оформление технического задания по конфигурации серверного оборудования.

ПЗ№13. Оформление технического задания по конфигурации локальных сетей.

ПЗ№14. Проверка наличия и сроков действия сертификатов

ПЗ№15. Разработка политики безопасности корпоративной сети

ПЗ№16. Получение сертификата

ПЗ№17. Защита данных от несанкционированного доступа
ПЗ№18. Создание резервных копий базы данных
ПЗ№19. Восстановление базы данных
ПЗ№20. Анализ эффективности функционирования базы данных и развитие системы.
ПЗ№21. Анализ работы с пользователями БД.
ПЗ№22. Подготовка и поддержание системных программных средств.
ПЗ№23. Подготовка и поддержание системных программных средств.

Экспертная оценка выполнения практических работ

Оценка «5»

- выполнил работы в полном объеме с соблюдением необходимой последовательности действий;
- проводит работу в условиях, обеспечивающих получение правильных результатов и выводов;
- соблюдает правила техники безопасности;
- в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления;
- правильно выполняет анализ ошибок.

Оценка «4» ставится, если выполнены требования к оценке 5, но допущены 2-3 недочета, не более одной ошибки и одного недочета.

Оценка «3» ставится, если

- работа выполнена не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы
- в ходе проведения работы были допущены ошибки.

Оценка «2» ставится, если студент совсем не выполнил работу.

3.3 Методические рекомендации по подготовке конспекта

Конспектирование – это свертывание текста, в процессе которого не просто отбрасывается маловажная информация, но сохраняется, переосмысливается все то, что позволяет через определенный промежуток времени автору конспекта развернуть до необходимых рамок конспектируемый текст без потери информации. При этом используются сокращения слов, аббревиатуры, опорные слова, ключевые слова, формулировки отдельных положений, формулы, таблицы, схемы, позволяющие развернуть содержание конспектируемого текста.

Конспект один из разновидностей вторичных документов фактографического ряда – это краткая запись основного содержания текста с помощью тезисов.

Существует две разновидности конспектирования:

– конспектирование письменных текстов (документальных источников, учебников и т.д.);
– конспектирование устных сообщений (лекций, выступлений и т.д.).

Дословная запись как письменной, так и устной речи не относится к конспектированию.

Успешность конспекта зависит от умения структурирования материала. Важно не только научиться выделять основные понятия, но и намечать связи между ними.

Классификация видов конспектов:

1. План-конспект (создается план текста, пункты плана сопровождаются комментариями. Это могут быть цитаты или свободно изложенный текст).
2. Тематический конспект (краткое изложение темы, раскрываемой по нескольким источникам).
3. Текстуальный конспект (изложение цитат).
4. Свободный конспект (включает в себя цитаты и собственные формулировки).
5. Формализованный конспект (записи вносятся в заранее подготовленные таблицы.

Это удобно при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных объектов, явлений, процессов и т.д.).

6. Опорный конспект. Необходимо давать на этапе изучения нового материала, а потом использовать его при повторении. Опорный конспект позволяет не только обобщать, повторять необходимый теоретический материал, но и даѐт педагогу огромный выигрыш во времени при прохождении материала.

Необходимо помнить, что:

1. Основа конспекта – тезис.

2. Способ записи должен обеспечивать высокую скорость конспектирования.

3. Нужны формы записи (разборчивость написания), ориентированные на быстрое чтение.

4. Приёмы записи должны способствовать быстрому запоминанию (подчеркивание главной мысли, выделение другим цветом, схематичная запись в форме графика или таблицы).

5. Конспект – это запись смысла, а не запись текста. Важной составляющей семантического свертывания при конспектировании является перефразирование, но он требует полного понимания речи. Перефразирование – это прием записи смысла, а не текста.

6. Необходимо указывать библиографическое описание конспектируемого источника.

7. Возможно в конспекте использование цитат, которые заключаются в кавычки, при этом рекомендуется на полях указать страницу, на которой находится изречение автора.

Способы конспектирования.

Тезисы — это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

а) Линейно-последовательная запись текста.

При конспектировании линейно — последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

б) Способ «вопросов - ответов».

Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них. Одна из модификаций способа «вопросов - ответов» — таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа - решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, « мое мнение» и т.п.

в) Схема с фрагментами

Способ конспектирования, позволяющий ярче выявить структуру текста, — при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

г) Простая схема

Простая схема — способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно. Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

д) Параллельный способ

Параллельный способ конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в

левой части листа. Однако лучше использовать разные способы конспектирования для записи одного и того же материала.

е) Комбинированный конспект

Комбинированный конспект — вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки индивидуальность студента.

Общие рекомендации студентам по составлению конспекта:

1. Определите цель составления конспекта.

2. Читая изучаемый материал в электронном виде в первый раз, разделите его на основные смысловые части, выделите главные мысли, сформулируйте выводы.

3. Если составляете план - конспект, сформулируйте названия пунктов и определите информацию, которую следует включить в план-конспект для раскрытия пунктов плана.

4. Наиболее существенные положения изучаемого материала (тезисы) последовательно и кратко излагайте своими словами или приводите в виде цитат.

5. Включайте в конспект не только основные положения, но и обосновывающие их выводы, конкретные факты и примеры (без подробного описания).

6. Составляя конспект, записывайте отдельные слова сокращённо, выписывайте только ключевые слова, делайте ссылки на страницы конспектируемой работы, применяйте условные обозначения.

7. Чтобы форма конспекта отражала его содержание, располагайте абзацы «ступеньками», подобно пунктам и подпунктам плана, применяйте разнообразные способы подчеркивания, используйте карандаши и ручки разного цвета.

8. Отмечайте непонятные места, новые слова, имена, даты.

9. При конспектировании старайтесь выразить авторскую мысль своими словами. Стремитесь к тому, чтобы один абзац авторского текста был передан при конспектировании одним, максимум двумя предложениями.

Экспертная оценка составления коспекта

«Отлично» - полнота использования учебного материала. Объём конспекта – 1 тетрадная страница на один раздел или один лист формата А 4. Логика изложения (наличие схем, количество смысловых связей между понятиями). Наглядность (наличие рисунков, символов и пр.; аккуратность выполнения, читаемость конспекта. Грамотность (терминологическая и орфографическая). Отсутствие связанных предложений, только опорные сигналы – слова, словосочетания, символы. Самостоятельность при составлении.

«Хорошо» - использование учебного материала неполное. Объём конспекта – 1 тетрадная страница на один раздел или один лист формата А 4. Недостаточно логично изложено (наличие схем, количество смысловых связей между понятиями). Наглядность (наличие рисунков, символов и пр.; аккуратность выполнения, читаемость конспекта. Грамотность (терминологическая и орфографическая). Отсутствие связанных предложений, только опорные сигналы – слова, словосочетания, символы. Самостоятельность при составлении.

«Удовлетворительно» - использование учебного материала неполное. Объём конспекта – менее одной тетрадной страницы на один раздел или один лист формата А 4. Недостаточно логично изложено (наличие схем, количество смысловых связей между понятиями). Наглядность (наличие рисунков, символов, и пр.; аккуратность выполнения, читаемость конспекта. Грамотность (терминологическая и орфографическая). Отсутствие связанных предложений, только опорные сигналы – слова, словосочетания, символы. Самостоятельность при составлении. Неразборчивый почерк.

«Неудовлетворительно» - использование учебного материала неполное. Объём конспекта – менее одной тетрадной страницы на один раздел или один лист формата А 4. Отсутствуют схемы, количество смысловых связей между понятиями. Отсутствует наглядность

(наличие рисунков, символов, и пр.; аккуратность выполнения, читаемость конспекта. Допущены ошибки терминологические и орфографические. Отсутствие связанных предложений, только опорные сигналы – слова, словосочетания, символы. Несамостоятельность при составлении. Неразборчивый почерк.

3.4 Типовые задания

Устный опрос по теме «Требования безопасности к серверам баз данных. Классы защиты».

1. Что такое Сертификация?
2. Перечислите краткую характеристику требований к современным серверам баз данных.
3. Чем отличается Прикладной программный интерфейс от Универсального?
4. Назовите, с какими технологиями связан Microsoft Data Access Components (MDAC)?
5. Опишите технологию Borland Database Engine (BDE).
6. Перечислите этапы классификации АС.
7. Какие параметры определяют класс защищенности АС?
8. Сколько существует классов защищенности АС от НСД к информации?

Тестовый опрос по теме «Информационная безопасность баз данных».
Ссылка на тест https://forms.gle/aNEWfgv9DREqhFE59

1. Установить соответствие между термином и определением: а) состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно б) состояние информации, при котором изменение осуществляется только субъектами, имеющими на него право в) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право 1) конфиденциальность 2) целостность 3) доступность	2. К какому классу отнести угрозу: обнаружена уязвимость, которая нарушает конфиденциальность личной информации пользователей и нарушает целостность работы системы: а) по свойствам информации б) по компонентам информационных систем в) по способу осуществления г) по расположению источника угроз
3. К какому классу отнести угрозу: обнаружена уязвимость в работе жесткого диска, нормальная работа которого может быть нарушена с помощью грамотно настроенных звуковых волн: а) по свойствам информации б) по компонентам информационных систем в) по способу осуществления г) по расположению источника угроз	4. ... является следствием наличия уязвимых мест или уязвимостей в информационной системе (дописать текст, регистр при вводе ответа не учитывается)
5. Что является причинами возникновения уязвимостей: а) ошибки при разработке программного обеспечения б) преднамеренные изменения программного обеспечения с целью внесения уязвимостей	6. Определите характеристики Input-инъекции (инъекции в поле ввода): а) взлом традиционных СУБД б) уязвимыми являются многие веб-платформы (PHP, WordPress, Joomla, Java) в) взлом СУБД, архитектура которых отличается от классической реляционной модели

в) неправильные настройки программного обеспечения г) несанкционированное внедрение вредоносных программ д) неумышленные действия пользователей е) сбои в работе программного и аппаратного обеспечения ж) невозможность протестировать все уязвимости з) желание специалиста "сломать программу"	г) отсутствии единого, унифицированного языка запросов д) обнаружить уязвимость можно с помощью suIP.biz 1) SQL-инъекция 2) NoSQL-инъекция
7. Как называется совокупность мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на веб-приложение (написать определение, регистр при вводе ответа не учитывается, также можно использовать аббревиатуру)	8. Как называется способ атаки информационной системы, в результате которой легитимные пользователи теряют доступ к сетевым приложениям или информации (написать определение, регистр при вводе ответа не учитывается, также можно использовать аббревиатуру)
9. Как называется вид интернет-мошенничества, цель которого получить идентификационные данные пользователей: а) Фишинг б) Кликбейт в) DoS г) WAF д) Wapiti	10. Что нужно сделать для информационной безопасности при использовании общедоступного Wi-Fi? а) использовать VPN-соединение б) не передавать личные данные в) провести обновление программного обеспечения г) заклеить камеру скотчем д) провести резервное копирование ваших данных
11. Как называется принцип ИБ, который предоставляет доступ к информации и её носителям в соответствии с полномочиями пользователя? а) Простота использования информационной системы б) Контроль над всеми операциями в) Запрещено всё, что не разрешено г) Открытая архитектура ИС д) Разграничение доступа е) Минимальные привилегии ж) Достаточная стойкость з) Минимум идентичных процедур	12. Как называется принцип ИБ, который говорит о выделении пользователю наименьших прав и доступа к минимуму необходимых функциональных возможностей программ? а) Простота использования информационной системы б) Контроль над всеми операциями в) Запрещено всё, что не разрешено г) Открытая архитектура ИС д) Разграничение доступа е) Минимальные привилегии ж) Достаточная стойкость з) Минимум идентичных процедур
13. Назовите минимальное количество символов, которое рекомендовано для создания безопасного пароля (ответ ввести в строку цифрой)	

ОТВЕТЫ:

№ заданий	Варианты ответа
1	а – 3 б – 2

	в – 1
2	а
3	б, г
4	угроза
5	а, б, в, г, д, е
6	а, б - 1 в, г, д - 2
7	файрвол, WAF
8	Отказ в обслуживании (DoS)
9	а
10	а, б
11	д
12	е
13	8

Экспертная оценка выполнения тестового задания

"5" - 85% (от 17 баллов)
"4" - 65% (от 13 баллов)
"3" - 51% (от 10 баллов)
"2" - 35% (от 9 баллов и ниже)

3.5 Типовые методические рекомендации к выполнению практических заданий

Практическая работа №1.

Тема: Правовые нормы, относящиеся к информации. Анализ лицензионного соглашения на использование услуг популярных интернет-сервисов.

1. Цель работы: знать правовые нормы, относящиеся к информации, уметь провести анализ лицензионного соглашения на использование услуг популярных интернет-сервисов.

2. Оборудование, приборы, аппаратура, материалы: персональный компьютер с выходом в Интернет.

3. Краткие теоретические сведения

В конкурентной борьбе широко распространены разнообразные действия, направленные на получение (добывание, приобретение) конфиденциальной информации самыми различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки. Установлено, что 47% охраняемых сведений добывается с помощью технических средств промышленного шпионажа.

Таким образом, информационная безопасность — это состояние защищенности информации среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств.

1) ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРАВА СОБСТВЕННОСТИ

Право собственности рассматривают как совокупность отдельных прав или правомочий. В российском праве обычно выделяют правомочия владения, пользования и распоряжения.

- ***Право владения*** связано с обладанием какой-либо информацией. Под обладанием понимается в том числе и доступ к месту, где вещь находится.
- ***Право пользования*** связано с возможностью извлекать выгоды из информации.
- ***Право распоряжения*** означает возможность решать юридическую судьбу информации (возможность продать, подарить, отдать в аренду, уничтожить и т.д.).

Информация хоть и не является материальной, на неё распространяется такое право собственности, как и на материальный объект.

2) ЗАКОН ОБ АВТОРСКОМ ПРАВЕ (ГК РФ ГЛАВА 70. АВТОРСКОЕ ПРАВО)

Авторское право является институтом гражданского права, который регулирует правоотношения, связанные с использованием произведений творческой или интеллектуальной деятельности.

Закон об авторском праве РФ был принят ***9 июля 1993 года***. Защита авторских прав регулируется статьями 1252 и 1301 ГК РФ. В ст. 1255 ГК РФ говорится о том, какие права принадлежат автору.

- Право авторства;
- Право автора на имя;
- Право на неприкосновенность произведения;
- Право на обнародование произведения;
- Исключительное право на произведение.

Субъектом авторского права является ***физическое лицо, творческим трудом которого создано произведение***. Ему принадлежит весь спектр прав: Личные неимущественные и исключительные права, которые дают возможность использовать произведение в любой форме, не противоречащей закону. Автором является тот, чье имя указано на оригинале.

Объектом авторского права является произведение науки, искусства, независимо от способа его выражения.

Личные неимущественные права — вид субъективных прав, относящихся к категории нематериальных благ. Личные неимущественные права (право свободного передвижения, право выбора места пребывания и жительства, право на имя и др.) возникают у человека от рождения. Они входят в содержание правоспособности.

а) Личные неимущественные права:

- Право признаваться автором произведения;
- Право использовать или разрешать использовать свое произведение под псевдонимом;
- Право обнародовать произведение в любой форме;
- Право на неприкосновенность произведения.

Исключительное право — совокупность принадлежащих правообладателю (гражданину или юридическому лицу) прав на использование по своему усмотрению любым не противоречащим закону способом результата интеллектуальной деятельности или средства индивидуализации и на запрещение или разрешение такого использования другими лицами.

б) Исключительное право на произведение:

- Право признаваться автором произведения;
- Изготовление одного и более экземпляров произведения (воспроизведение);
- Распространение путем продажи;
- Публичный показ;
- Импорт с целью распространения;
- Прокат оригинала или экземпляра;
- Публичное исполнение;
- Сообщение в эфир;
- Сообщение по кабелю;
- Перевод и переработка произведения.

Согласно Гражданскому кодексу Российской Федерации, исключительное ***авторское право действует на протяжении всей жизни автора и еще семьдесят лет после смерти владельца.***

3) ДОКАЗАТЕЛЬСТВО АВТОРСТВА:

На данный момент, на территории Российской Федерации действует презумпция авторства, что, говоря обычным языком, представляет собой датированный факт предоставления произведения. Если настоящий автор зарегистрирует свои права на книгу, песню или музыку

позже, чем это сделает кто-либо другой, то доказать принадлежность к данной интеллектуальной собственности будет крайне сложно, хотя этот факт будет считаться нарушением авторских прав. Что может служить доказательством авторства при подаче иска в суд?

- ***черновики произведения***, датированные разработки музыки на компьютере, эскизы и пр.;
- ***нотариально заверенная регистрация*** авторских прав;
- ***документ о депонировании*** произведения;

Российская государственная библиотека осуществляет прием на депонирование необнародованных результатов интеллектуальной деятельности с выдачей авторам свидетельства о депонировании.

Депонирование предусматривает: прием, учет, регистрацию, хранение результатов интеллектуальной деятельности в электронном виде и обеспечение к ним доступа потребителей (также возможно депонирование без предоставления доступа). Под результатами интеллектуальной деятельности понимаются произведения науки, литературы, искусства, а также иные объекты, указанные в нормах Гражданского кодекса РФ.

Депонирование результатов интеллектуальной деятельности ***не влияет на возникновение, осуществление и охрану авторских прав***, однако сам факт депонирования может быть использован ***в качестве доказательства*** существования необнародованного результата интеллектуальной деятельности и ***признания авторства лица***, его создавшего.

Подписав заявление о депонировании произведения, автор предоставляет Российской государственной библиотеке на безвозмездной основе неисключительное право на размещение цифрового экземпляра депонируемого произведения в фонде депонированных произведений, с возможным в дальнейшем размещением в электронной библиотеке РГБ для предоставления к нему открытого доступа читателям.

По результатам депонирования автору выдается свидетельство о депонировании результатов интеллектуальной деятельности.

Для депонирования своего произведения автору необходимо предоставить в Российскую государственную библиотеку:

- заявление;
- экземпляр произведения в электронной форме;
- реферат в электронной форме в соответствии с ГОСТ 7.9–95;
- карточку с библиографическим описанием произведения в электронной форме в соответствии с ГОСТ 7.1–2003, ГОСТ 7.80-2000 и ГОСТ 7.51–9;
- копию паспорта (вторая, третья страницы и страница, содержащая данные о последнем месте регистрации).

Для этого автор может воспользоваться одним из удобных ему способов: электронная почта (с последующим предоставлением подлинников) или обычная почта; личное обращение в отдел или же через сайт Российской государственной библиотеки (с последующим предоставлением подлинников в отдел).

- ***нераспечатанное заказанное письмо*** с экземпляром произведения;
- ***электронный экземпляр*** произведения, записанный ***на диск с фиксированной датой***.

Стоит отметить, что во время судебных разбирательств, самым веским доказательством предъявления авторских прав будет служить документ, одобренный и заверенный нотариусом, а лишь потом, акт депонирования и другие.

4) АКТЫ НАРУШЕНИЯ АВТОРСКИХ ПРАВ:

Сейчас, проблемы и правонарушения в области авторского права растут в огромных масштабах, так как с развитием телевидения, электронной техники, а также всемирной сети – контролировать законность распространения произведений, становится крайне трудно. Что же можно оценить, как правонарушение?

- «***Пиратство***» (как видео-, так и аудио-) – создание и запись копии медиа файлов с целью ***коммерческого или некоммерческого нелегального распространения***. Что можно ожидать от подобных экземпляров произведения? Его качество может быть значительно ниже, нежели качество оригинала, но, с другой стороны, может являться точной копией.
- ***Создание программ для взлома («кряков») для лицензионных программ***. Так политика получения ключа за определенную плату в Российской Федерации не очень популярна, то «кряки» и «таблетки» приобрели огромную популярность. На интернет- порталах существуют целые комплекты с уже вложенными в них взломанными программами и ключами.
- Электронные библиотеки и ***незаконное издательство авторских книг***. На литературных интернет - порталах находятся терабайты электронных книг, которые запрещены к свободному распространению.

5) НАКАЗАНИЕ ЗА НАРУШЕНИЕ АВТОРСКИХ ПРАВ:

Данная статья рассматривает несколько видов наказаний за некоторые виды нарушений, а именно:

- За ***плагиат*** предусмотрено принудительное взимание средств размером *до двухсот тысяч рублей* или в размере заработной платы за срок до полутора лет, а также исправительные работы или *заключение под стражу до шести месяцев*
- ***За коммерческое или некоммерческое использование*** незаконных ***авторских материалов*** наказываются штрафом в размере *до двухсот тысяч рублей* или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами *на срок до двух лет*, либо лишением свободы на тот же срок.
- За проступки с ***отягощающими обстоятельствами*** срок исправительных работ увеличен до *пяти лет*, а взимаемый штраф *до пятисот тысяч рублей*

За нарушение авторских прав ответственность налагается либо добровольно по договоренности обеих сторон при досудебном урегулировании спора, либо в судебном порядке.

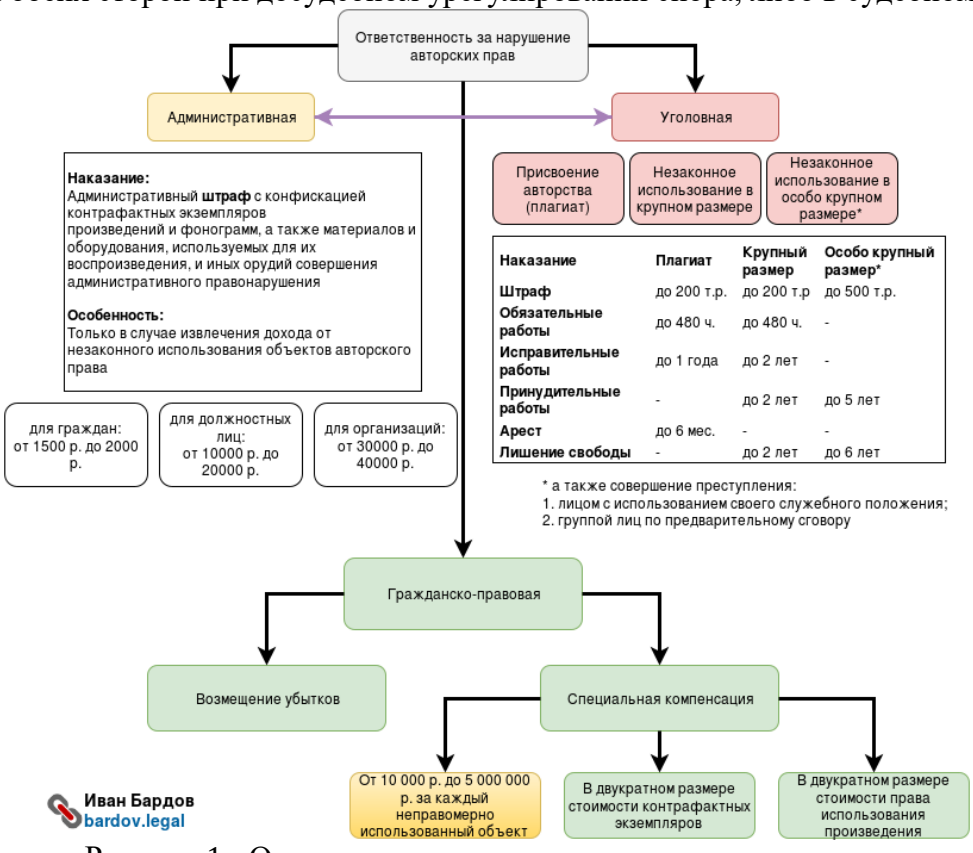

Рисунок 1 - Ответственность за нарушение авторских прав

6) ЗАКОН № 149-ФЗ «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»

Нормативный документ Российской Федерации, юридически описывающий понятия и определения в области технологии правового регулирования в сфере информации, информационных технологий, а также регулирующий отношения при осуществлении права на поиск, получение, передачу, производство и распространение информации при применении информационных технологий. Вступил в силу ***9 августа 2006.***

Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

В настоящем Федеральном законе используются следующие основные понятия:

Информация - сведения (сообщения, данные) независимо от формы их представления;

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

Доступ к информации - возможность получения информации и ее использования;

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

Электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

а) Виды информации по категории доступа:

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

– ***информацию, свободно распространяемую;***

К общедоступной информации относятся общеизвестные сведения и иная информация, *доступ* к которой *не ограничен*. Общедоступная информация *может использоваться любыми*

лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

- ***информацию, предоставляемую по соглашению лиц***, участвующих в соответствующих отношениях;
- ***информацию, которая в соответствии с федеральными законами подлежит предоставлению*** или распространению;
- ***информацию, распространение которой в Российской Федерации ограничивается*** или запрещается.

б) Не может быть ограничен доступ к:

нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

- информации ***о состоянии окружающей среды***;
- информация ***о законах различного уровян***;
- информации ***о деятельности государственных органов*** и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- информации, накапливаемой в открытых фондах ***библиотек, музеев и архивов***, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

в) Ограничение доступа к информации:

- Ограничение доступа к информации устанавливается федеральными законами ***в целях защиты основ конституционного строя, нравственности, здоровья, прав*** и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
- Обязательным является соблюдение ***конфиденциальности информации***, доступ к которой ограничен федеральными законами.
- Защита информации, составляющей ***государственную тайну***, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.
- Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим ***коммерческую тайну, служебную тайну*** и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.
- Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (***профессиональная тайна***), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.
- Информация, составляющая ***профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами*** и (или) по решению суда.
- Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

- Запрещается требовать от гражданина (физического лица) предоставления ***информации о его частной жизни***, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.
- Порядок доступа к ***персональным данным граждан*** (физических лиц) устанавливается федеральным законом о персональных данных.

10) ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (ГЛ 28 УК РФ)

Закон принят от 13.06.96 N 63-ФЗ

а) Статья 272. Неправомерный доступ к компьютерной информации

- ***Неправомерный доступ*** к охраняемой законом компьютерной информации, если это деяние ***повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации***, - наказывается штрафом в размере ***до двухсот тысяч рублей*** или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на ***срок до двух лет***, либо лишением свободы на тот же срок.
- То же деяние, ***причинившее крупный ущерб или совершенное из корыстной заинтересованности***, - наказывается ***штрафом*** в размере от ста тысяч ***до трехсот тысяч рублей*** или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на ***срок до четырех лет***, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.
- Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные ***группой лиц по предварительному сговору*** или организованной группой либо лицом с использованием своего служебного положения, - наказываются штрафом в размере ***до пятисот тысяч рублей*** или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок ***до пяти лет***, либо лишением свободы на тот же срок.
- Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли ***тяжкие последствия*** или создали угрозу их наступления, - наказываются лишением свободы на ***срок до семи лет***.

Примечания.

1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

б) Статья 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ.

Первая часть данной статьи предусматривает уголовную ответственность за создание программ для ЭВМ или их модификацию, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, а также использование таких программ или носителей с такими программами (дискеты, диски, флэш-накопители, съемные жесткие диски). (объективная сторона)

Изменение программы подразумевает под собой существенное изменение функционала программного обеспечения в сравнении с авторским исполнением, например, появление в программе дополнительных функций, утрата имеющихся либо ограничение некоторых функций.

Вредоносная программа – программа, находящаяся в электронном виде и способная осуществлять вредоносные функции (алгоритмы, процессы, воздействия).

Субъективная сторона данного преступления характеризуется прямым умыслом, то есть физическое вменяемое лицо, достигшее шестнадцатилетнего возраста, совершающее преступление, осознаёт, что создает программу – «вирус», «червь» и т.д., либо модифицирует, доводя до такого качества (таких функций) обычную программу, предвидит возможность или неизбежность наступления, при её использовании другими пользователями ЭВМ, вредных последствий и желает их наступления либо относится к ним безразлично.

Под вредоносной программой следует понимать программу, которая была создана для выполнения несанкционированных (неразрешенных) владельцем информации, ЭВМ или системы ЭВМ, определённых функций (алгоритмов, процессов).

Под такими функциями можно подразумевать:

- несанкционированное уничтожение информации;
- блокирование информации;
- изменение либо копирование информации;
- нарушение работы ЭВМ или систем ЭВМ, в частности вывод из строя антивируса.

Важно подчеркнуть, что для первой части данного преступления обязательны два признака, характеризующие способ совершения преступления и конкретное средство:

- действия не должны быть санкционированы владельцем информации (не разрешены);
- наличие самой вредоносной программы или существенные изменения в уже существующей.

Так же к компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств её защиты, относится информация со встроенным в неё вредоносными кодами («компьютерный червь», «логическая бомба», «троянский конь»).

- ***Создание, распространение или использование компьютерных программ*** либо иной компьютерной информации, заведомо ***предназначенных*** для н***есанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты*** компьютерной информации, - наказываются ограничением свободы на ***срок до четырех лет***, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок ***со штрафом в размере до двухсот тысяч рублей*** или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.
- Деяния, предусмотренные частью первой настоящей статьи, совершенные ***группой лиц по предварительному сговору*** или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на ***срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей*** или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
- Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли ***тяжкие последствия*** или создали угрозу их наступления, - наказываются лишением свободы на ***срок до семи лет***.

в) Статья 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

- ***Нарушение правил эксплуатации средств хранения, обработки или передачи*** охраняемой компьютерной ***информации*** либо информационно-телекоммуникационных сетей и оконечного оборудования, а также ***правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации***, причинившее крупный ущерб, - наказывается штрафом в размере ***до пятисот тысяч рублей*** или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы ***на срок до двух лет***, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.
- Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло ***тяжкие последствия*** или создало угрозу их наступления, - наказывается принудительными работами на ***срок до пяти лет*** либо лишением свободы на тот же срок.

Необходимо подчеркнуть, что преступление, предусмотренное частью 3 статьи 273 УК РФ одно из немногих из главы 28 УК РФ, которая имеет статус тяжкого преступления. И это неудивительно, т.к. создание, использование и распространение вредоносных программ могут нанести значительный ущерб экономическому аспекту жизни общества и даже стать причиной причинения вреда здоровью различной тяжести и смерти людей. При высоком уровне технической подготовки преступник своими действиями может серьёзно дезорганизовать работу больницы, метро, школы и т.д., а также совершить хищение денежных средств и персональных данных клиентов различных организаций.

Основанием для возбуждения уголовного дела может являться наличие элементарных «crack»-программ, которые в обход ввода лицензионного ключа продукта, предоставляют возможность использования программного обеспечения и распространяются, в основном, в комплекте с лицензионным программным обеспечением, например, с Microsoft Office.

11) ФЕДЕРАЛЬНЫЙ ЗАКОН «О ПЕРСОНАЛЬНЫХ ДАННЫХ»:

Федеральный закон РФ ***от 27 июля 2006 года № 152-ФЗ*** «О персональных данных» — федеральный закон, регулирующий деятельность по обработке (использованию) персональных данных.

Персональные данные (сокр. ПД) или личностные данные — ***сведения, относящиеся к прямо или косвенно определённому, или определяемому физическому лицу*** (субъекту персональных данных), которые могут быть предоставлены другим лицам.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Хотя концепция персональных данных довольно стара, развитие сетей связи и автоматизированного анализа данных позволило красть, централизованно собирать и массово продавать данные о человеке. Эти данные помогают выследить человека, спланировать преступление против него или постороннему выдать себя за другого. Более мирное применение персональным данным — реклама.

Персональные данные — это юридическое, а не техническое понятие, тем не менее современные технологии анализа данных позволяют отличить одного человека от другого по косвенным признакам. Персональными данными являются ***фамилии, имена и отчества, дата и место рождения, место жительства или пребывания, номера телефонов, реквизиты паспорта или иного документа, удостоверяющего личность, идентификационный номер налогоплательщика*** - физического лица, основной государственный регистрационный номер индивидуального предпринимателя, страховой номер индивидуального лицевого счета.

а) Основные положения закона:

- ***обработка персональных данных осуществляется с согласия субъекта*** персональных данных на обработку его персональных данных;
- обработка персональных данных ***необходима для достижения целей***, предусмотренных международным договором Российской Федерации или законом, ***для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;***
- обработка персональных данных ***осуществляется в связи с участием лица*** в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве ***в*** арбитражных ***судах***;
- обработка персональных данных ***необходима для исполнения полномочий федеральных органов исполнительной власти***, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
- обработка персональных данных необходима ***для исполнения договора***, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- обработка персональных данных необходима ***для защиты жизни, здоровья*** или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон "О микрофинансовой деятельности и микрофинансовых организациях", либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
- Обработка персональных данных должна осуществляться на законной и справедливой основе.
- Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
- Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- ***Обработке подлежат только персональные данные, которые отвечают целям их обработки.***
- Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
- ***При обработке персональных данных должны быть обеспечены точность персональных данных***, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
- Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

б) обязанности оператора:

- Для всех компаний, которые ведут свою деятельность на территории РФ:
    - ***Данные должны храниться на серверах, которые находятся на территории РФ***. Санкции за нарушение могут быть серьезными (речь даже не о штрафе, а о прекращении деятельности, достаточно вспомнить LinkedIn и решение суда о блокировке).
    - Необходимо провести внутреннюю работу в своей компании - ***подготовить установленные документы*** (Политику конфиденциальности и другие), провести инструктаж, подписать со стороны руководства и сотрудников.
    - ***Уведомить Роскомнадзор*** (в электронном и бумажном виде) ***о том, что вы являетесь оператором данных*** (если у вас есть сотрудники, вы храните данные соискателей, клиентов или других физических лиц — значит вы являетесь оператором данных).

- Дополнительно для тех, у кого есть сайт и на нем есть поля для ввода персональных данных (имя, телефон, почта и прочая информация, которая указывается при регистрации или заполнении форм обратной связи):
    - Разместить Политику конфиденциальности в открытом доступе.
    - Разместить Пользовательское соглашение, которое должно содержать необходимые положения о порядке обработке персональных данных.
    - Под каждой формой ввода персональных данных разместить ссылку на согласие с обработкой этих данных и ссылку на Пользовательское соглашение.

в) Содержание бланка согласия на обработку ПД:

- При необходимости согласия ***бланк согласия должен включать*** в себя ***следующие сведения***:
    - фамилию, имя, отчество, адрес, номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе;
    - наименование и адрес оператора, получающего согласие;
    - цель обработки;
    - перечень данных, на обработку которых даётся согласие;
    - перечень действий с данными, на совершение которых даётся согласие, общее описание используемых оператором способов обработки данных;
    - срок, в течение которого действует согласие, а также способ его отзыва;
    - личную подпись.

Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов этих данных о своем намерении осуществлять такую обработку. О том, что это за орган, будет сказано далее.

г) Согласие на обработку ПД не требуется:

- Такое ***уведомление не требуется***, когда данные:
    - обрабатываются в соответствии с трудовым законодательством;
    - получены в связи с заключением договора, стороной которого является физическое лицо, если его данные не распространяются и не предоставляются третьим лицам, а используются оператором исключительно для исполнения указанного договора;
    - относятся к членам общественного объединения и обрабатываются соответствующим общественным объединением, действующими в соответствии с законодательством Российской Федерации, при условии, что данные не будут распространяться или раскрываться третьим лицам;
    - сделаны самим владельцем персональных данных общедоступными;
    - включают в себя только фамилию, имя и отчество субъекта;
    - необходимы в целях однократного пропуска субъекта на территорию, на которой находится оператор, или в иных аналогичных целях;
    - включены в государственные автоматизированные информационные системы для защиты безопасности государства и общественного порядка;
    - обрабатываются без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации;
    - обрабатываются в целях транспортной безопасности.

Например, является ли интернет-магазин оператором персональных данных? — Изначально, вроде, нет, так как данные клиента используются только «в связи с заключением договора, стороной которого является субъект». Но ведь при отправке заказа почтой или транспортной компанией сведения о клиенте предоставляются третьей стороне.

д) Контроль осуществляет:

- В настоящее время ***уполномоченным органом по защите прав субъектов персональных данных назначена Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)***. Непосредственно

этим направлением занимается одно из её подразделений — Управление по защите прав субъектов персональных данных.

- Деятельность Роскомнадзор направлена на организационно-документальную сторону дела. Технические аспекты защиты персональных данных курирует Федеральная служба по техническому и экспортному контролю (ФСТЭК).
- Если в технических средствах защиты информации используется криптография (шифрование), к регулированию подключается Федеральная служба безопасности РФ (ФСБ).

е) Обязанности оператора:

- Оператор персональных данных ***обязан обеспечить их защиту от неправомерного или случайного доступа к ним***, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении них.
- Под мерами по обеспечению безопасности персональных данных при их обработке законодатель понимает следующие действия.
    - Определение угроз безопасности.
    - Применение организационных и технических мер по обеспечению безопасности.
    - Применение средств защиты информации.
    - Оценка эффективности принимаемых мер по обеспечению безопасности до ввода в эксплуатацию информационной системы.
    - Учёт съёмных носителей персональных данных.
    - Обнаружение фактов несанкционированного доступа к данным.
    - Восстановление данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
    - Установление правил доступа к обрабатываемым данным, а также обеспечение регистрации и учёта всех действий, совершаемых с ними.
    - Контроль за принимаемыми мерами по обеспечению безопасности данных и уровня защищенности информационных систем.

Этот список не является исчерпывающим, то есть законом допускаются иные действия, направленные на обеспечение безопасности персональных данных.

ж) Ответственность:

Федеральным законом "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях" от 07.02.2017 N 13-ФЗ с 1 июля 2017 года ужесточена ответственность за несоблюдение закона «О персональных данных». Обработка персональных данных без письменного согласия субъекта, когда это необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие. ***Штраф*** за невыполнения тех или иных действий, предусмотренных в законе, составит ***от 10 000 до 75 000 руб. за каждое обнаруженное нарушение.***

Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ. По статье предусмотрен штраф в размере ***до 200 тысяч рублей*** или лишение свободы на ***срок до 2 лет***.

Те же деяния, совершенные лицом ***с использованием своего служебного положения***, предусматривают штраф в размере ***от 100 тысяч до лишения свободы на срок до 4 лет***.

12) ФЕДЕРАЛЬНЫЙ ЗАКОН № 139-ФЗ ОТ 28 ИЮЛЯ 2012 ГОДА:

Федеральный закон Российской Федерации *«О внесении изменений в Федеральный закон „О защите детей от информации, причиняющей вред их здоровью и развитию“* и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет». Этот закон внёс в другие федеральные законы ряд положений, предполагающих фильтрацию интернет-сайтов по системе чёрного списка и блокировку запрещённых интернет-ресурсов.

Ряд экспертов высказывал опасения, что данный закон может использоваться для цензуры Интернета.

- Так, до внесения поправок по этому закону каждую страницу в сети Интернет с информацией, «причиняющей вред…», нужно будет ***промаркировать специальными знаками***: 6+, 12+, 16+, 18+ (старше 6 лет, старше 12 лет, старше 16 лет, старше 18 лет соответственно). По тексту ЗП № 89417-6 от 9 июля 2012 года (за два дня до принятия Думой), поправки устанавливают тексты знаков и делают исключение для сайтов, не являющихся «сетевыми изданиями», и для комментариев пользователей «сетевых изданий». Кроме того, в поправках подробно описываются процедуры экспертизы «информационной продукции».
- Также законом вносится положение, что ***доступ к сети Интернет в «местах доступных для детей» должен быть ограничен.***
- ***Создаётся информационная система Росреестр*** «Единый реестр доменных имен и (или) универсальных указателей страниц сайтов в сети Интернет и сетевых адресов сайтов в сети Интернет, ***содержащих информацию, запрещённую к распространению на территории*** Российской Федерации федеральными законами» (далее — Реестр).
- Ограничение на интернет-страницы или доменные имена, содержащие:
  После решений федеральных органов:
  - ***материалы с порнографическими изображениями несовершеннолетних*** и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;
  - информацию о местах приобретения и о методах ***изготовления и использования наркотиков***, психотропных веществ и их прекурсоров, либо о способах и местах культивирования наркосодержащих растений;
  - ***информацию о способах совершения самоубийства***, а также призывов к совершению самоубийства;
  - (добавлено ФЗ 05.04.2013 № 50-ФЗ[18]) информацию о несовершеннолетних, пострадавших в результате противоправных деяний.
  - ***любую иную информацию, запрещённую к распространению в России решениями судов***.
- ***Решение о включении в Реестр доменных*** имен, ссылок на интернет-страницы сайтов и сетевых адресов сайтов ***можно обжаловать только через суд,*** причём лишь ***в течение 3 месяцев***.
- С момента внесения доменного имени или ссылки на интернет-страницу в ***Реестр хостинг-провайдер обязан в течение суток проинформировать владельца сайта о необходимости незамедлительного удаления интернет-страницы целиком***, на которой размещается запрещённая, по мнению оператора Реестра, информация.
- ***Владелец сайта обязан в течение суток с момента*** получения от хостинг-провайдера уведомления ***удалить данную интернет-страницу целиком***. В случае отказа или бездействия владельца сайта, хостинг-провайдер обязан ограничить доступ к такому сайту в сети Интернет.
- ***В случае непринятия*** хостинг-провайдером и владельцем сайта ***данных мер, сетевой адрес сайта включается в Реестр.***
- ***Оператор связи***, оказывающий услуги по предоставлению доступа к сети Интернет, ***обязан в течение суток с момента включения сетевого адреса сайта в Реестр ограничить к нему доступ***. Тот факт, что на одном IP-адресе могут находиться несколько сайтов с разными доменными именами, законом не учитывается.

13) «ПАКЕТ ЯРОВОЙ»:

Федеральный закон от ***6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму“*** и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»

Федеральный закон от ***6 июля 2016 г. № 375-ФЗ*** «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

Большая часть поправок вступила в силу 20 июля 2016 года.

- Поправки, дающие Правительству полномочия ***обязывать операторов связи хранить записи телефонных разговоров, SMS и интернет-трафик пользователей сроком 6 месяцев***, должны были вступить в силу 1 июля 2018 года. При этом, как это следует из поправок, указанная информация должна была храниться исключительно на территории России. Однако 19 июля 2016 член Совета Федерации Антон Беляков внёс законопроект о переносе срока вступления в силу этих поправок на 2023 год.
- Второй законопроект обязывает операторов связи хранить звонки и сообщения абонентов за период, определяемый Правительством Российской Федерации (но не более, чем за 6 месяцев) в соответствии с 64-й статьей федерального закона «О связи», а ***информацию о фактах приема, передачи, доставки и обработки сообщений и звонков — 3 года***.
- Согласно проекту приказа Минкомсвязи, ***интернет-компании и сервисы должны хранить и предоставлять спецслужбам: псевдоним, дату рождения, адрес, фамилию, имя, отчество, паспортные данные, языки, которыми владеет пользователь, список его родственников, текст сообщений, аудио- и видеозаписи, адрес электронной почты, дату и время авторизации и выхода из информационного сервиса, наименование программы-клиента***.
- 12 апреля 2018 года правительство РФ подписало постановление о том, что с 1 октября 2018 года операторы связи обязаны хранить в течение 30 суток текстовые, голосовые, видео- и другие сообщения пользователей. Далее оператор обязан увеличивать объем хранения на 15 процентов в год.
- Законопроект устанавливает ***запрет на использование несертифицированных средств кодирования*** (шифрования). За нарушение этого запрета нарушителю грозит штраф в размере от 3 000 до 5 000 руб. с конфискацией средств шифрования. В Федеральной службе безопасности уточнили, что обязательная сертификация средств кодирования (шифрования) требуется только при передаче сведений, составляющих государственную тайну, поэтому ***сертификации систем мгновенного обмена сообщениями (мессенджеров), таких как Telegram, WhatsApp*** и прочих при передаче сведений ***не составляющих гостайну, не требуется***.
- Также «закон Яровой» обязывает организаторов распространения информации в интернете декодировать сообщения пользователей. По требованию ФСБ компании должны будут предоставлять ключи к зашифрованному трафику.

Уже после подписания этого закона Президентом выяснилось, что оборудования, необходимого для хранения таких гигантских объёмов данных, нет не только в России, но и во всём мире. В связи с этим Путин распорядился запустить собственное производство необходимого аппаратного обеспечения. К 1 сентября 2016 года он также поручил проанализировать возможность, сроки и затраты на организацию производства отечественного оборудования и программного обеспечения, нужного для хранения и обработки данных.

14) МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

• Организационные

Повышение квалификации персонала, контролируемые каналы распространения информации, разделение прав доступа, уничтожение ненужных копий документов, соблюдение коммерческой тайны персоналом.

• Юридические

В России действуют Закон «О правовой охране программ для ЭВМ и баз данных» и Закон «Об авторском праве и смежных правах».

Уголовный Кодекс содержит статьи:

- Ст. 272 «О неправомерном доступе к компьютерной информации»
- Ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ»
- Ст. 274 «Нарушение правил эксплуатации ЭВМ, систем ЭВМ или сети ЭВМ»

• Программно-технические.

- Защита от компьютерных вирусов
- Шифрование данных
- Резервное копирование данных
- Ограничение доступа к устройствам и файловой системе
- Контроль трафика с помощью межсетевых экранов (брандмауэров)

Рисунок 2 – Методы защиты информации

4. Задание

Задание №1. Найти в Интернет закон РФ «Об информации, информатизации и защите информации» и выделить определения понятий:

1. информация	
2. информационные технологии	
3. информационно-телекоммуникационная сеть	
4. доступ к информации	
5. конфиденциальность информации	
6. электронное сообщение	
7. документированная информация	
8. оператор информационной системы	

Задание 2. Изучив источник «Пользовательское соглашение» Яндекс ответьте на следующие вопросы:

1. По какому адресу находится страница с пользовательским соглашением Яндекс?	

2. В каких случаях Яндекс имеет право отказать пользователю в использовании своих служб?	
3. Каким образом Яндекс следит за операциями пользователей?	
4. Что подразумевается под термином «контент» в ПС?	
5. Что в ПС сказано о запрете публикации материалов, связанных с: • нарушением авторских прав и дискриминацией людей; • рассылкой спама; • изготовлением и применением оружия?	
6. Ваш почтовый ящик на Почте Яндекса будет удален, если Вы не пользовались им более ___.	
7. Поясните понятие ***логин*** для электронной почты	
8. Что такое *пароль*? Какие пароли недопустимы? Какое минимальное количество символов должны быть в пароле? Какие символы обязательны для пароля?	
9. Для чего применяется смс-копия в электронном письме?	
10. Назовите ограничение на количество писем в сутки. Что происходит, если пользователем превысил заданный предел?	

Задание 3. Изучив источник «Условия использования Google» и ответьте на следующие вопросы:

1. По какому адресу находится условиями использования Google? Укажите дату актуальной версии	
2. Укажите требуемый возраст для управления аккаунтом Google	
3. Как Google обеспечивает конфиденциальность и защиту информации?	
4. Как удалить информацию о себе из результатов поиска Google?	
5. Что в сказано о запрете публикации материалов, связанных с: • дискриминационные высказывания; • призывы к совершению противоправных или опасных действий; • террористическая деятельность; • рассылкой спама; • нарушение авторских прав?	
6. Пользуйтесь сервисом, чтобы аккаунт оставался активным. Использование подразумевает в том числе доступ к контенту сервиса или добавление нового контента по крайней мере…	
7. Что такое *пароль*? Какие пароли недопустимы? Какое минимальное количество символов должны быть в пароле? Какие символы обязательны для пароля?	
8. Список сервисов, для которых действуют Условия использования Google, а также их дополнительные условия и правила	

5. Содержание отчета

Отчет должен содержать: (при написании отчета использовать образец, выданный преподавателем).

1. Название работы.

2. Тема работы.
3. Цель работы.
4. Оборудование, приборы, аппаратура, материалы.
5. Результаты выполнения задания с подписанными скриншотами.
6. Вывод по работе.

6. Контрольные вопросы

1. Что такое информационная безопасность?
2. Сколько лет действует авторское право согласно Гражданскому кодексу Российской Федерации? Как автору можно доказать свое авторство?
3. Как вы думаете, почему преступления в сфере компьютерной информации (ГЛ 28 УК РФ) относятся к более тяжким преступлениям и караются статьей уголовного кодекса?
4. Опишите основные положения Закона «Об информации, информатизации и защите информации». Доступ к какой информации должен быть ограничен/не ограничен?
5. Как вы поняли, что такое обработка персональных данных? Приведите пример. Является ли публикация только фамилии, имени, отчества какого-либо человека без его согласия нарушением закона?
6. Что изменилось в законодательстве согласно федеральному закону № 139-ФЗ?
7. Вступил ли в полную силу «Пакет Яровой»? Почему?
8. Перечислите меры обеспечения информационной безопасности
9. Противоречит ли «Пользовательское соглашение» Яндекса Закону «Об информации, информатизации и защите информации». Почему?

3.6 Методические указания по подготовке к устному опросу

Целью устного собеседования являются обобщение и закрепление изученного курса.

Студентам предлагаются для освещения сквозные концептуальные проблемы. При подготовке следует использовать лекционный материал и учебную литературу. Для более глубокого постижения курса и более основательной подготовки рекомендуется познакомиться с указанной дополнительной литературой. Готовясь к семинару, студент должен, прежде всего, ознакомиться с общим планом семинарского занятия. Следует внимательно прочесть свой конспект лекции по изучаемой теме и рекомендуемую к теме семинара литературу. При этом важно научиться выделять в рассматриваемой проблеме самое главное и сосредотачивать на нем основное внимание при подготовке. С незнакомыми терминами и понятиями следует ознакомиться в предлагаемом глоссарии, словаре или энциклопедии.

Ответ на каждый вопрос из плана семинарского занятия должен быть доказательным и аргументированным, студенту нужно уметь отстаивать свою точку зрения. Для этого следует использовать документы, монографическую, учебную и справочную литературу. Активно участвуя в обсуждении проблем на семинарах, студенты учатся последовательно мыслить, логически рассуждать, внимательно слушать своих товарищей, принимать участие в спорах и дискуссиях.

Для успешной подготовки к устному опрос, студент должен законспектировать рекомендуемую литературу, внимательно осмыслить фактический материал и сделать выводы. Студенту надлежит хорошо подготовиться, чтобы иметь возможность грамотно и полно ответить на заданные ему вопросы, суметь сделать выводы и показать значимость данной проблемы для изучаемого курса. Студенту необходимо также дать анализ той литературы, которой он воспользовался при подготовке к устному опросу на семинарском занятии.

При подготовке, студент должен правильно оценить вопрос, который он взял для выступления к семинарскому занятию. Но для того чтобы правильно и четко ответить на поставленный вопрос, необходимо правильно уметь пользоваться учебной и дополнительной литературой.

Перечень требований к любому выступлению студента примерно таков:

- связь выступления с предшествующей темой или вопросом.
- раскрытие сущности проблемы.

- методологическое значение для научной, профессиональной и практической деятельности.

Разумеется, студент не обязан строго придерживаться такого порядка изложения, но все аспекты вопроса должны быть освещены, что обеспечит выступлению необходимую полноту и завершенность. Приводимые участником семинара примеры и факты должны быть существенными, по возможности перекликаться с профилем обучения. Выступление студента должно соответствовать требованиям логики. Четкое вычленение излагаемой проблемы, ее точная формулировка, неукоснительная последовательность аргументации именно данной проблемы, без неоправданных отступлений от нее в процессе обоснования, безусловная доказательность, непротиворечивость и полнота аргументации, правильное и содержательное использование понятий и терминов.

4 КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Теоретические вопросы к дифференцированному зачету:

1. Законодательство Российской Федерации в области защиты информации.
2. Требования безопасности к серверам баз данных.
3. Классы защиты.
4. Основные группы методов противодействия угрозам безопасности в корпоративных сетях.
5. Программные методы защиты процесса обработки и передачи информации.
6. Аппаратные методы защиты процесса обработки и передачи информации.
7. Политика безопасности.
8. Настройка политики безопасности.
9. Виды неисправностей систем хранения данных.
10. Утилиты резервного копирования.
11. Восстановление базы данных: основные алгоритмы и этапы.
12. Восстановление носителей.
13. Воссоздание утраченных файлов.
14. Полное восстановление.
15. Неполное восстановление.
16. Мониторинг активности и блокирование.

Примеры заданий для выполнения практической части к дифференцированному зачету:

1. Анализ лицензионного соглашения на использование услуг популярных интернет-сервисов: Яндекс.
2. Анализ лицензионного соглашения на использование услуг популярных интернет-сервисов: Google.
3. Составление политики конфиденциальности.
4. Настройка политики безопасности: права пользователей.
5. Настройка политики безопасности: глобальные параметры безопасности системы.
6. Настройка политики безопасности: политика обновления.
7. Настройка параметров аутентификации системы.
8. Восстановление носителей информации.
9. Резервное копирование данных.
10. Восстановление удаленных файлов.
11. Восстановление зараженных файлов.
12. Мониторинг активности портов.
13. Поиск активных портов
14. Блокирование портов.

Теоретические вопросы к экзамену:

1. Автоматизированные средства аудита. Обзор современных программных средств.
2. Брандмауэры.
3. Восстановление базы данных: основные алгоритмы и этапы.
4. Уровни качества программной продукции.
5. Требования к конфигурации серверного оборудования. Оформление требований.
6. Требования к конфигурации локальных сетей. Оформление требований.
7. Объекты информатизации, требующие обязательной сертификации программных средств и обеспечения.
8. Виды сертификатов безопасности.
9. Функции сертификатов безопасности, срок действия.
10. Проверка наличия сертификата безопасности.
11. Системы сертификации.
12. Процедура сертификации.
13. Платформы и центры сертификации.
14. Сертификат разработчика.
15. Процесс подписи и проверки кода.
16. SSL сертификат: содержание, формирование запроса.
17. SSL сертификат: проверка данных с помощью сервисов.

Примеры заданий для выполнения практической части к экзамену:

1. Анализ современных автоматизированных средств аудита.
2. Применение брандмауэров для аудита.
3. Анализ качества программной продукции с точки зрения безопасности.
4. Анализ качества конфигурации серверного оборудования.
5. Анализ качества конфигурации локальных сетей.
6. Оформление технического задания по конфигурации серверного оборудования.
7. Оформление технического задания по конфигурации локальных сетей.
8. Проверка наличия и сроков действия сертификатов
9. Разработка политики безопасности корпоративной сети
10. Процедура получение сертификата.
11. Защита данных от несанкционированного доступа
12. Создание резервных копий базы данных
13. Восстановление базы данных
14. Анализ эффективности функционирования базы данных.
15. Анализ работы с пользователями БД.
16. Подготовка системных программных средств.
17. Поддержание системных программных средств.

5 ПЕРЕЧЕНЬ ПЕЧАТНЫХ ИЗДАНИЙ, ЭЛЕКТРОННЫХ ИЗДАНИЙ (ЭЛЕКТРОННЫХ РЕСУРСОВ), ДОПОЛНИТЕЛЬНЫХ ИСТОЧНИКОВ

Основные источники:

1. Баранова, Е. К. Информационная безопасность и защита информации: учеб. пособие / Е. К. Баранова, А. В. Бабаш. -3-е изд., перераб. и доп. -Москва: РИОР: ИНФРА-М, 2017. -322 с

2. Ляпина О.П., Перлова О.Н. Стандартизация, сертификация и техническое документирование. – М.: Академия, 2018. – 208 с.;

3. Перлова О.Н. Соадминистрирование баз данных и серверов:учебник для студ. учреждений сред. проф. образования/О.Н. Перлова, О.П. Ляпина. – М.: Издательский центр «Академия», 2018 г.

4. Шишмарев В. Ю. Метрология, стандартизация, сертификация и техническое регулирование. – М.: НИЦ ИНФА-М, 2017. – 312 с.;

Дополнительные источники:

1. Технология разработки программного обеспечения: учебник для вузов / С. А. Орлов. - 4-е изд. Стандарт третьего поколения. - СПб. : Питер, 2012. - 608 с.

2. Технология разработки программного обеспечения: учебн. пособие / под ред. Гагарина Л.Г. – М.:ИД ФОРУМ, НИЦ ИНФРА-М, 2018. – 400 с.

3. ФуфаевЭ.В. Разработка и эксплуатация удаленных баз данных: учебник для студ. учреждений сред.проф. образования/ Э.В. Фуфаев, Д.Э. Фуфаев. –4-е изд., стер. –М.: Издательский центр «Академия», 2014 г.

Приложение 1 «Образец титульного листа»

Министерство образования Красноярского края
Краевое государственное бюджетное профессиональное образовательное учреждение
«Красноярский колледж радиоэлектроники и информационных технологий»

ОТЧЕТ ПО ПРАКТИЧЕСКИХ РАБОТАХ

_____
дисциплина

Студент _____ _____ _____
номер группы, зачетной книжки подпись, дата инициалы, фамилия

Преподаватель _____ _____
подпись, дата инициалы, фамилия

Красноярск 2022