ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПРАКТИКУМ.

Е.А.ГАФАРОВА

ЮЖНО-УРАЛЬСКИЙ
ГОСУДАРСТВЕННЫЙГУМАНИТАРНО-
ПЕДАГОГИЧСЕКИЙ УНИВЕРСИТЕТ

Город Челябинск

Е.А. Гафарова

Организационно-правовое обеспечение информационной безопасности

Учебное пособие

Челябинск 2019

ББК 67.4:73я73

УДК 34:001.8(021)

Г 24

Гафарова, Е.А. Организационно-правовое обеспечение информационной безопасности : учебное пособие / Е.А. Гафарова. - Челябинск : Издательство ЗАО «Библиотека А. Миллера». - 153 с.

ISBN 978-5-93162-170-8

Учебное пособие включает 10 практических работ по дисциплине «Организационно-правовое обеспечение информационной безопасности» для магистрантов направления «Управление информационной безопасности в профессиональном обучении». В пособие включены тесты для самопроверки и подробный план концепции обеспечения информационной безопасности учреждения для самостоятельной работы студентов.

Учебное пособие может быть использовано для организации практических занятий по отдельным темам у студентов- бакалавров направления «Профессиональное обучение (по отраслям)» профильной направленности «Информатика и вычислительная техника» и «Правоведение и правоохранительная деятельность».

Рецензенты: В.А. Белевитин, д.т.н., профессор

И.А. Прохорова, к.т.н., доцент

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Анализ существующих программ магистерской подготовки в области информационной безопасности показывает, что возможны различные варианты формирования профессиональных компетенций образовательной области «Информационная безопасность».

Приказом Министерства образования и науки РФ от 1 декабря 2016 г. № 1513 «Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры)» определены требования государства в этой области, в связи с чем, содержание существующих магистерских программ требует своевременного осмысления, актуализированного наполнения при условии оптимальной преемственности между ступенями высшего образования – бакалавриата и магистратуры.

Организационно-правовое обеспечение информационной безопасности является одной из базовой дисциплин в профессиональной подготовке магистров направления «Управление информационной безопасности в профессиональном обучении».

При изучении дисциплины магистранты формируют компетенции, необходимые для выполнения следующих видов деятельности:

- организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации (ФСБ РФ), Федеральной службы но техническому и экспортному контролю Российской Федерации (ФСТЭК РФ);
- организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

- разработка проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности; аудит информационной безопасности информационных систем и объектов информатизации;
- аттестация объектов информатизации по требованиям безопасности информации.

Дисциплина «Организационно-правовое обеспечение информационной безопасности» базируется на курсах «Основы информационной безопасности» и «Правоведение».

Значимость дисциплины обусловлена применением полученных знаний в дальнейшей исследовательской работе, при подготовке и защите магистерской диссертации, в будущей профессиональной деятельности.

Цель дисциплины – сформировать способность и готовность магистранта в применении нормативно-правовых актов в области информационной безопасности в учреждениях профессионального образования.

Основные задачи курса:

– сформировать систему знаний об основах организационного и правового обеспечения информационной безопасности, о содержании основных нормативных правовых актов в области обеспечения информационной безопасности и нормативных методических документов ФСБ России и ФСТЭК России в области защиты информации;

– сформировать умение организации работы по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.

- создать условия для получения опыта по разработке организационно-распорядительных документов в области информационной безопасности.

Компетенция магистранта, формируемая в результате освоения учебной дисциплины:

ПК-32 – способен и готов разрабатывать и применять новые методики повышения производительности труда, экономии ресурсов и безопасности.

Магистрант в ходе освоения учебной дисциплины должен:

знать:

- сущность и понятие информационной безопасности, характеристику её составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды угроз информационной безопасности;
- основные положения комплексного подхода к защите информации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, нормативные методические документы ФСБ и ФСТЭК РФ в данной области;

уметь:

- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

владеть

- основами работы с нормативными правовыми актами;

- основами организации обеспечения режима конфиденциальности и управления деятельностью служб защиты информации на учреждении;
- опытом разработки проектов организационно-распорядительных документов для учреждений профессионального образования.

Для формирования профессиональных компетенций магистранту необходимо предложить различные виды практических работ.

Практические занятия проводятся с целью закрепления и углубления теоретических знаний, полученных обучающимися на лекциях и в ходе самостоятельной работы.

Настоящее учебное пособие предназначено для проведения практических работ магистрантов направления «Управление информационной безопасности в профессиональном обучении».

Отдельные учебные материалы могут быть использованы для организации занятий у студентов – бакалавров направления «Профессиональное обучение (по отраслям)» профильной направленности «Информатика и вычислительная техника» и «Правоведение и правоохранительная деятельность».

ПРАКТИЧЕСКАЯ РАБОТА №1. РАБОТА СО СПРАВОЧНО-ИНФОРМАЦИОННОЙ ПРАВОВОЙ СИСТЕМОЙ «КОНСУЛЬТАНТПЛЮС»

Цель работы: ознакомиться с функционалом справочно-поисковой системой, приобрести практические навыки работы с информационной правовой системой «КонсультантПлюс»,

Методы и приемы: лабораторная работа с использованием информационно-коммуникационных технологий, выполнение упражнений, частично-поисковый метод, самостоятельная работа.

Ключевые слова: справочно-поисковая система, реквизиты нормативных актов, карточка поиска, правовой навигатор, обзор законодательства.

Краткие теоретические сведения

Справочная правовая система (СПС) «КонсультантПлюс» включает все законодательство РФ: от основополагающих документов до узкоотраслевых актов. Стартовое окно некоммерческой интернет-версии СПС представлено на рисунке 1.

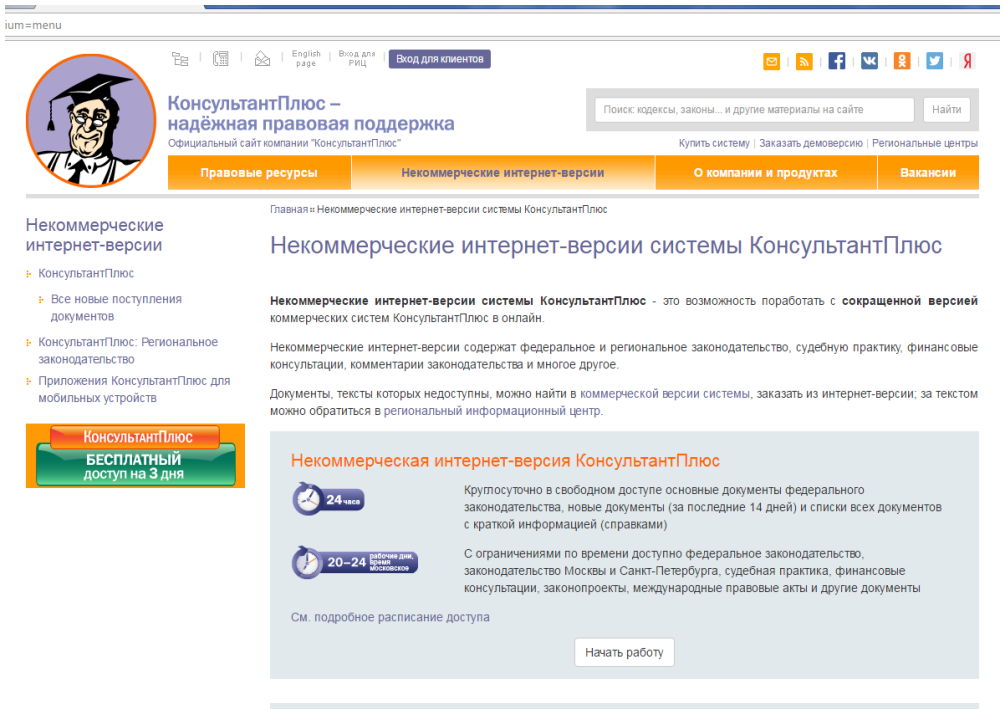


Рисунок 1. Стартовое окно СПС «КонсультантПлюс» некоммерческой интернет-версии

Некоммерческие интернет–версии СПС «КонсультантПлюс» содержат федеральное и региональное законодательство, судебную практику, финансовые консультации, комментарии законодательства, тематические обзоры.

Документы, тексты которых недоступны, можно найти в коммерческой версии системы, заказать из интернет–версии; за текстом можно обратиться в региональный информационный центр.

Для поиска необходимых документов, необходимо заполнить карточку поиска (рис.2).

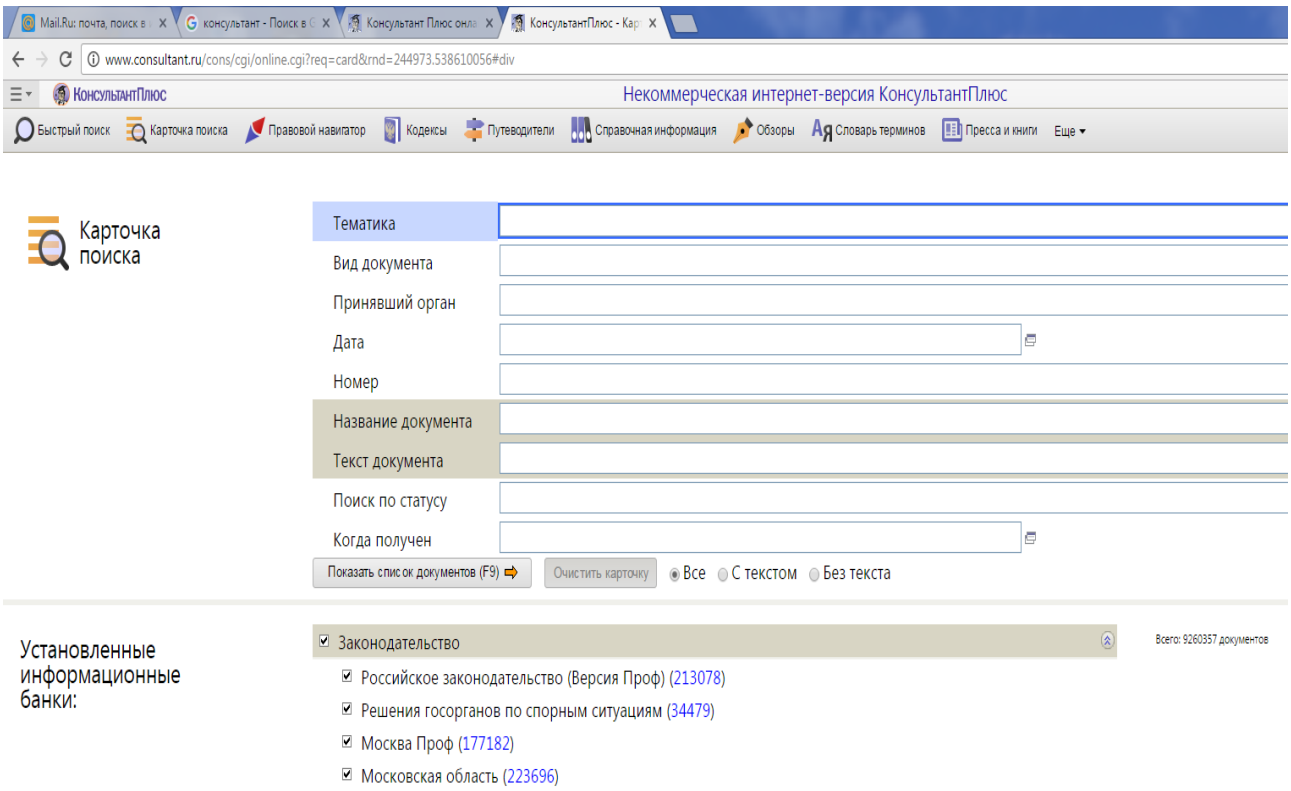


Рисунок 2. Карточка поиска некоммерческой интернет-версии КонсультантПлюс

Карточка поиска – основное средство поиска документов в базе данных системы. Система ищет документы, одновременно удовлетворяющие всем заполненным полям карточки поиска. Заполнять все поисковые поля не обязательно, достаточно заполнить лишь несколько полей.

В системе «КонсультантПлюс» предусмотрена возможность уточнять

полученные списки несколько раз по разным полям.

Работа со справочно-правовой системой «КонсультантПлюс» сводится к следующему алгоритму:

• составление запроса на поиск документа или группы документов и их поиск;

• применение процедур обработки: сортировки, фильтрации и др.;

• использование механизма гиперссылок, поиска и создания папок и закладок при работе с текстом документа;

• чтение, редактирование, печать, сохранение текста документа в файл или экспорт данных в текстовый редактор MSWord или табличный редактор MSExcel.

На рисунке 3 представлен пример диалогового окна для тематического поиска документов.

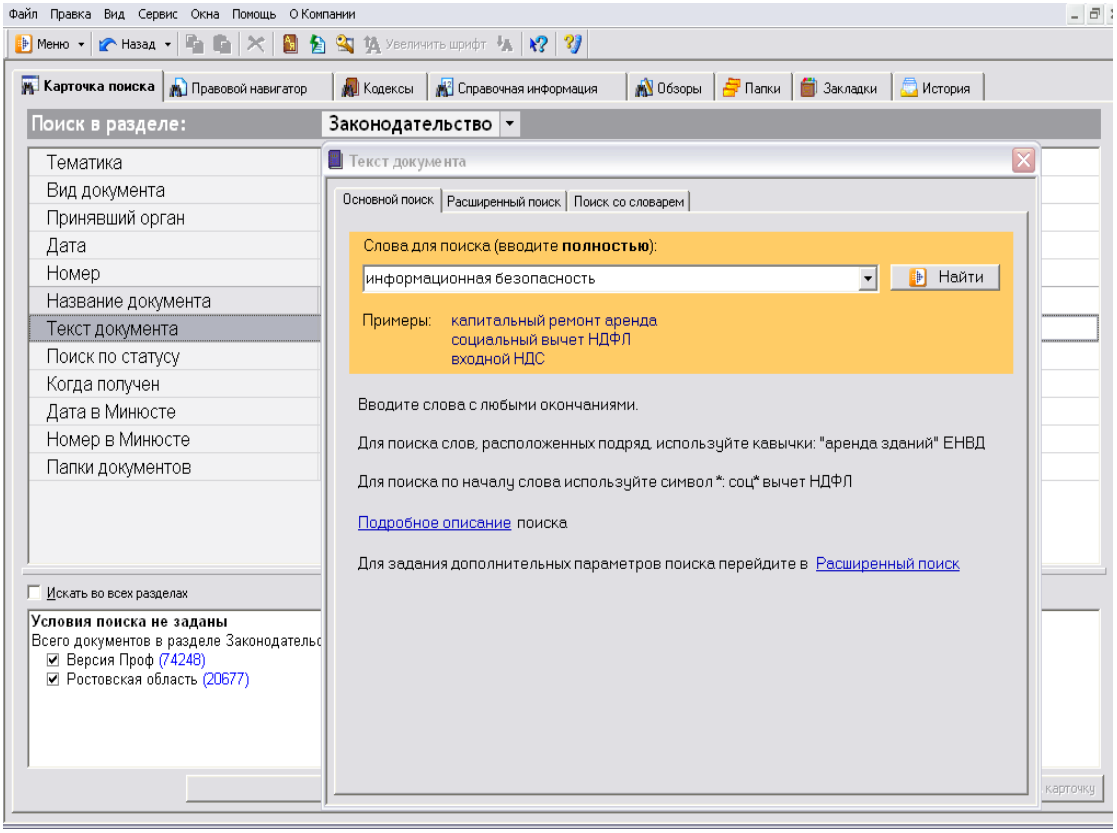


Рисунок 3. Окно поиска документа по правовому вопросу в системе «КонсультантПлюс»

Порядок выполнения работы.

1. Открыть сайт: http://www.consultant.ru, выбрать вкладку работа с некоммерческими интернет-версиями
2. Ознакомиться с краткими теоретическими сведениями
3. Ознакомиться со структурой и возможностями некоммерческой интернет-версией СПС «КонсультантПлюс»
4. Открыть в новой вкладке MSWord, начать оформление отчета по лабораторной работе: записать тему, цель.
5. Войти из стартового окна в режим «Обзоры законодательства», просмотреть информацию в разделе: Правовые новости/ Специальный выпуск, вернуться в Стартовое окно.
6. Открыть по ссылке «Новые документы» списки документов, включенных в систему за последний месяц. Сохранить скриншот списка в отчет по лабораторной работе
7. Перейти в раздел «Законодательство», знакомиться с общим построением справочно-информационной правовой системы «КонсультантПлюс»
8. Изучить поочередно все подпункты основного меню системы, зайти в карточку поиска, рассмотреть все её элементы.
9. Зайти в режим Правового навигатора, изучить особенности поиска информации по конкретному правовому вопросу; двухуровневую структуру словаря; ключевые понятия и группы ключевых понятий; различные виды сортировки списка. Выйти из Правового навигатора.
10. Выполнить упражнения, указанные в таблице 1 - найти нормативно-правовые документы, используя различные виды поиска
11. Ответить на контрольные вопросы.
12. Оформить отчет к лабораторной работе.

Таблица 1. Упражнения для поиска нормативных документов в СПС «КонсультантПлюс».

Вид поиска	**Задание**
Поиск по номеру и дате документа	Найдите Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Скопируйте реквизиты и преамбулу закона, вставьте эти данные в отчет по лабораторной работе. Найдите статью, посвященную ограниченному доступу к информации, скопируйте ее сохраните её в отчет.
Поиск по виду документа и его названию	Найдите основные документы по защите прав детей. Выделите три наиболее значимые, скопируйте реквизиты трех из них в отчет.
Поиск по правовому навигатору	Необходимо определить, чему равен минимальный размер оплаты труда (МРОТ). Найдите последний документ, которым внесены изменения в МРОТ. Вставьте его в отчет.
Поиск по принявшему органу	Найдите Приказ Генпрокуратуры РФ № 39 «О применении бланков процессуальных документов». Если документ отсутствует в некоммерческой интернет-версии, сделайте скриншот сервисного сообщения системы и вставьте его в отчет
Работа со списком документов	Сформируйте список документов о защите персональных данных. Поиск информации проводите по всем разделам справочной правовой системы. Список документов по данному вопросу сохраните в отчет.

Контрольные вопросы

1. Каковы основные разделы правовых документов в СПС «КонсультантПлюс»?
2. Что включается в иную официальную правовую информацию?
3. Перечислите основные инструменты поиска данной системы.
4. Как найти списки документов, регламентирующих конкретный правовой вопрос?
5. Из каких подразделов состоят разделы «Законодательство», «Судебная практика»?
6. В каком из разделов можно посмотреть тематические обзоры по проблемным правовым вопросам?
7. Как организована обратная связь с пользователями в данной системе?
8. Для чего применяется функция закладок в СПС «КонсультантПлюс»

Содержание отчета: тема, цель, скриншоты основных этапов работы, результаты выполненных заданий, ответы на контрольные вопросы.

Информационные источники:

1. Фомичева Т.Г. Лабораторный практикум по курсу «Компьютерные технологи и в правовой практике» Южно-Российский государственный технический университет, Новочеркасск, 2008
2. http://www.consultant.ru

ПРАКТИЧЕСКАЯ РАБОТА № 2: РАБОТА СО СПРАВОЧНО-ИНФОРМАЦИОННОЙ ПРАВОВОЙ СИСТЕМОЙ «ГАРАНТ»

Цель работы: ознакомиться с функционалом и приобрести практические навыки работы со справочной правовой системой «Гарант», формировать устойчивые навыки самостоятельной работы.

Методы и приемы: лабораторная работа с использованием информационно-коммуникационных технологий, изучение алгоритмов, выполнение упражнений, частично-поисковый метод, самостоятельная работа.

Ключевые слова: справочно-поисковая система, реквизиты нормативных актов, сервисы справочно-правовой системы, обзор законодательства.

Краткие теоретические сведения

Система производится в виде информационных блоков — баз данных, сформированных по тематическому принципу. Из информационных блоков формируется комплект, который и является конечным продуктом, предлагаемым заказчику. Еженедельное пополнение максимального комплекта составляет несколько десятков тысяч документов (включая документы судебной практики в виде онлайн-архива). Система включает все существующие виды правовой информации: акты органов власти федерального, регионального и муниципального уровня, судебную практику, международные договоры, проекты актов органов власти, формы (бухгалтерской, налоговой, статистической отчётности, бланки, типовые договоры), комментарии, словари и справочники. [википедия].

Работа со справочно-правовой системой «Гарант» начинается с организации поиска документа или списка документов.

Существуют следующие виды поиска в правовой системе «Гарант»: поиск

по реквизитам, поиск по классификатору, поиск по ситуации, поиск по источнику опубликования, поиск по словарю терминов. Вид поиска выбирается в зависимости от того, какую информацию необходимо получить и какие имеются известные реквизиты.

Искомые слова можно вводить в любой из этих форм. Система самостоятельно переведет каждое введенное слово в нормальную форму. Однако, следует учесть, что слова необходимо вводить полностью, поскольку при сокращении система не может точно определить, для какого именно слова русского языка требуется подобрать грамматические формы.

Результатом поиска нескольких слов, словосочетаний или целых фраз будет список документов, включающих словоформы всех слов запроса. Документы, полученные таким образом, по умолчанию будут отсортированы особым образом – по степени соответствия.

При открытии документа, найденного с использованием поиска по тексту, искомые слова будут отмечены цветом, а сам документ откроется в месте, которое больше всего соответствует введенному контексту.

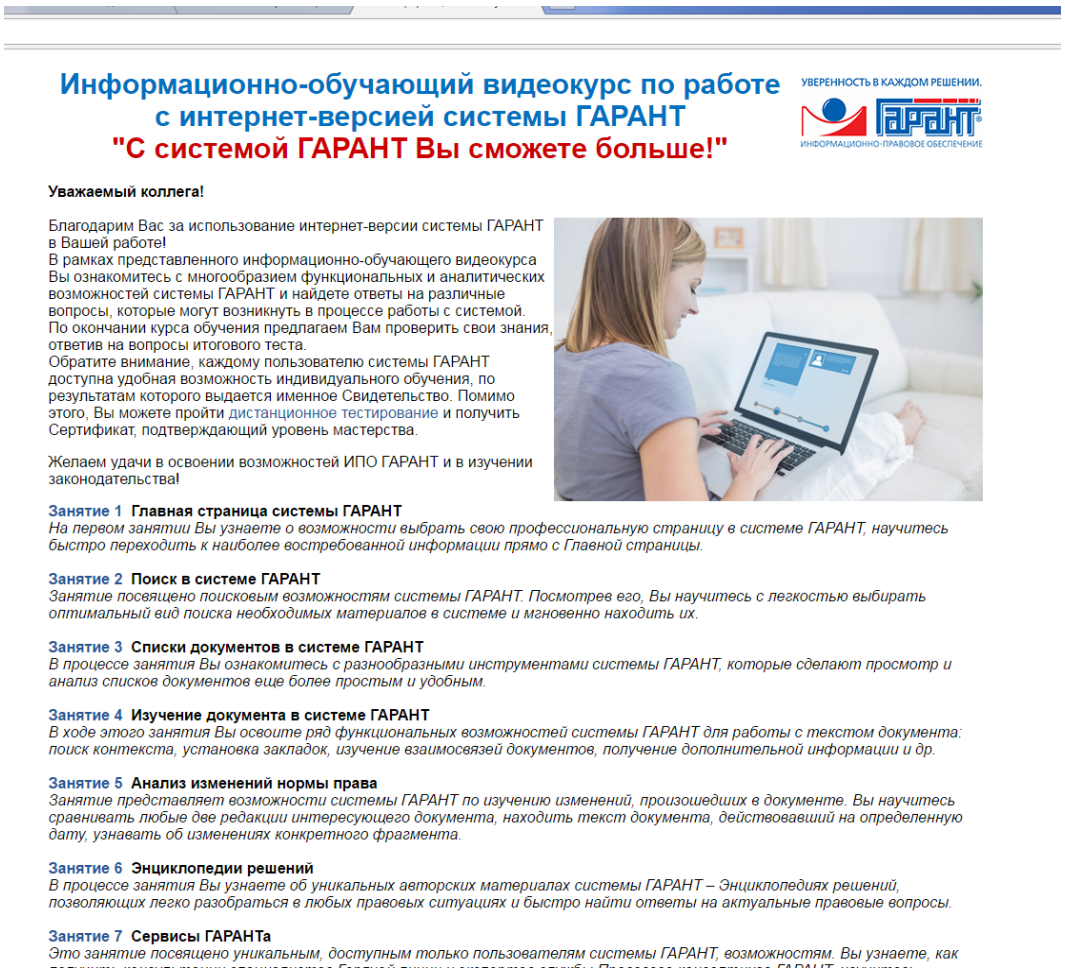
Сортировка *по степени соответствия* возможна только для списков, полученных при работе с *быстрым контекстным поиском*. Чем точнее конкретный документ соответствует содержанию запроса, тем выше его место в полученном списке.

Для получения изменений законодательства в определенной области в системе *существует индивидуальная новостная лента. Она* позволяет оперативно получить краткие тематические обзоры наиболее важных новых документов и судебных решений по интересующим вопросам[Фомичева].

Порядок выполнения работы

1. Откройте сайт http://www.garant.ru, выберите интернет-версию ГАРАНТ.
2. Изучите краткие теоретические сведения.

3. Перейдите по ссылке «Помощь в работе, возможности системы.
4. Откройте страницу Информационно-обучающий видеокурс по работе с интернет-версией системы ГАРАНТ (рис.4)



Информационно-обучающий видеокурс по работе с интернет-версией системы ГАРАНТ "С системой ГАРАНТ Вы сможете больше!"

УВЕРЕННОСТЬ В КАЖДОМ РЕШЕНИИ. ГАРАНТ ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

Уважаемый коллега!

Благодарим Вас за использование интернет-версии системы ГАРАНТ в Вашей работе!
В рамках представленного информационно-обучающего видеокурса Вы ознакомитесь с многообразием функциональных и аналитических возможностей системы ГАРАНТ и найдете ответы на различные вопросы, которые могут возникнуть в процессе работы с системой.
По окончании курса обучения предлагаем Вам проверить свои знания, ответив на вопросы итогового теста.
Обратите внимание, каждому пользователю системы ГАРАНТ доступна удобная возможность индивидуального обучения, по результатам которого выдается именное Свидетельство. Помимо этого, Вы можете пройти дистанционное тестирование и получить Сертификат, подтверждающий уровень мастерства.

Желаем удачи в освоении возможностей ИПО ГАРАНТ и в изучении законодательства!

Занятие 1 Главная страница системы ГАРАНТ
На первом занятии Вы узнаете о возможности выбрать свою профессиональную страницу в системе ГАРАНТ, научитесь быстро переходить к наиболее востребованной информации прямо с Главной страницы.

Занятие 2 Поиск в системе ГАРАНТ
Занятие посвящено поисковым возможностям системы ГАРАНТ. Посмотрев его, Вы научитесь с легкостью выбирать оптимальный вид поиска необходимых материалов в системе и мгновенно находить их.

Занятие 3 Списки документов в системе ГАРАНТ
В процессе занятия Вы ознакомитесь с разнообразными инструментами системы ГАРАНТ, которые сделают просмотр и анализ списков документов еще более простым и удобным.

Занятие 4 Изучение документа в системе ГАРАНТ
В ходе этого занятия Вы освоите ряд функциональных возможностей системы ГАРАНТ для работы с текстом документа: поиск контекста, установка закладок, изучение взаимосвязей документов, получение дополнительной информации и др.

Занятие 5 Анализ изменений нормы права
Занятие представляет возможности системы ГАРАНТ по изучению изменений, произошедших в документе. Вы научитесь сравнивать любые две редакции интересующего документа, находить текст документа, действовавший на определенную дату, узнавать об изменениях конкретного фрагмента.

Занятие 6 Энциклопедии решений
В процессе занятия Вы узнаете об уникальных авторских материалах системы ГАРАНТ – Энциклопедиях решений, позволяющих легко разобраться в любых правовых ситуациях и быстро найти ответы на актуальные правовые вопросы.

Занятие 7 Сервисы ГАРАНТа
Это занятие посвящено уникальным, доступным только пользователям системы ГАРАНТ, возможностям. Вы узнаете, как

Рисунок 4. Страница с информационно-обучающим видеокурсом по СПС «Гарант»

5. Изучить возможности СПС «Гарант» с помощью видеокурсов занятий с 1 по 7
6. Пройти итоговый тест (рис.5). Продемонстрировать результат выполненного теста преподавателю
7. Найти нормативно-правовые документы из задания для самостоятельной работы, используя возможности СПС «Гарант». Составить краткий электронный конспект
8. Ответить на контрольные ответы

9. Оформить отчет по лабораторной работе.

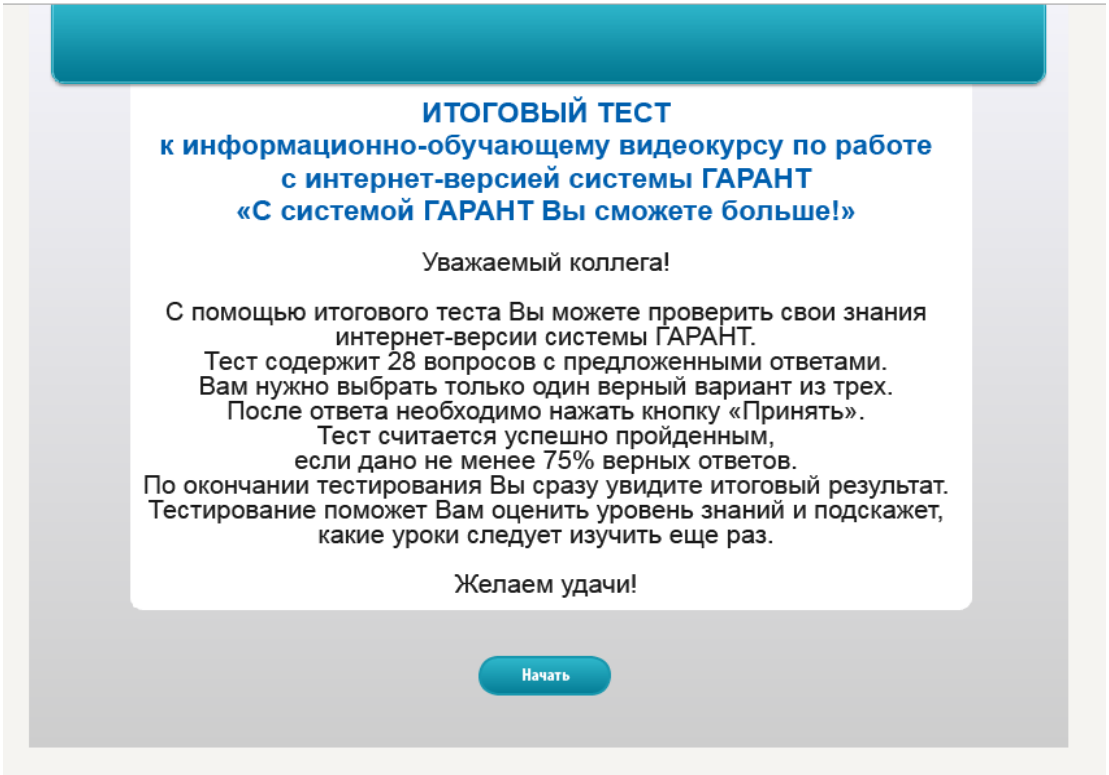


Рисунок 5.Тест для диагностики знаний по функциональным возможностям СПС «ГАРАНТ»

Задания для самостоятельной работы

Составить электронный конспект по основным правовым актам в области информационной безопасности:

- ст. ст. 23, 24, 29, 42 Конституции РФ, ст. ст. 5,7,8,9 ФЗ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (действующая редакция, 2016);
- ст.ст. 3, 4 Закона РФ от 27.12.1991 N 2124-1 (ред. от 03.07.2016) "О средствах массовой информации" (с изм. и доп., вступ. в силу с 15.07.2016),
- ст. ст. 7, 8, 9, 11 ФЗ "О персональных данных" от 27.07.2006 N 152-ФЗ (действующая редакция, 2016);

- сфера действия и принцип отнесения к гостайне ФЗ РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне";
- ст. 2 ФЗ "Об электронной подписи" от 06.04.2011 N 63-ФЗ (действующая редакция, 2016);
- ст.272, 273, 274 УК РФ.

Контрольные вопросы

1. Назовите виды поиска документов в СПС «Гарант».
2. Что такое быстрый контекстный поиск?
3. Назначение правового навигатора?
4. Какова структура единого информационного массива СПС «Гарант?»
5. Назовите элементы стартового окна СПС «Гарант?»
6. Как осуществляется переход к связанным документам?
7. Как просмотреть графические объекты?
8. Каков алгоритм работы с фильтрами в СПС «Гарант?»

Содержание отчета: Тема, цель, скриншоты основных этапов работы, электронный конспект, ответы на контрольные вопросы.

Информационные источники:

1. Фомичева Т.Г. Лабораторный практикум по курсу «Компьютерные технологи и в правовой практике» Южно-Российский государственный технический университет, Новочеркасск, 2008
2. http://www.garant.ru

ПРАКТИЧЕСКАЯ РАБОТА №3: НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

Цель: ознакомиться с нормативными правовыми актами в области информационной безопасности, проанализировать систему действующих правовых актов РФ в области информационной безопасности, формировать устойчивые навыки самостоятельной работы.

Методы и приемы: лабораторная работа с использованием информационно-коммуникационных технологий, поисковая работа, анализ источников.

Ключевые слова: информационная безопасность, правовые акты, система нормативно-правовых актов.

Порядок выполнения работы

1. Используя любой интернет-браузер, найти правовые документы из представленного перечня.
2. Вставить недостающие реквизиты в перечень нормативных актов.
3. Составить аналитическую записку - обзор по предложенному перечню правовых актов.
4. Оформить отчет по лабораторной работе.

Нормативно-правовые акты в области информационной безопасности РФ

1. Конституция Российской Федерации, принята 12 декабря ___ г.

2. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О ___ отдельных видов деятельности».

3. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об ___ подписи».

4. Федеральный закон от 28 декабря 2010 г. № ___ -ФЗ «О безопасности».

5. Федеральный закон от 27 июля ___ г. № 152-ФЗ «О персональных данных».

6. Федеральный закон от 27 июля ___ г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

7. Федеральный закон от 19 декабря ___ г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

8. Федеральный закон от 7 июля ___ г. № 126-ФЗ «О связи».

9. Федеральный закон от 27 декабря ___ г. № 184-ФЗ «О техническом регулировании».

10. Закон РФ № 195-ФЗ от 30 декабря ___ г. «Кодекс Российской Федерации об административных правонарушениях».

11. Закон РФ № 63-ФЗ от 13 июня ___ г. «Уголовный кодекс Российской Федерации».

12. Закон РФ № 5485-1 от 21 июля ___ г. «О государственной тайне».

13. ___ национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации 31 декабря 2015 г. № 683.

14. ___ информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 5 декабря 2016 г. № 646.

15. Указ Президента Российской Федерации от 12 мая 2008 г. № ___ «Вопросы системы и структуры федеральных органов исполнительной власти».

16. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и ___ контролю».

17. Указ Президента Российской Федерации от 1 ноября 2008 г. № 1576 «О совете при Президенте Российской Федерации по развитию ___ общества в Российской Федерации».

18. Указ Президента Российской Федерации от 30 мая 2005 г. № ___ «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

19. Указ Президента Российской Федерации от 17 марта 2008 г. № ___ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

20. Указ Президента Российской Федерации от 6 марта ___ г. № ___ «Об утверждении перечня сведений конфиденциального характера».

21. Концепция долгосрочного социально-экономического развития Российской Федерации на период до ___ года. Утверждена распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р.

22. Постановление Правительства Российской Федерации от 16 марта ___ г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

23. Постановление Правительства Российской Федерации № ___ от 1 ноября 2012 г. «Об утверждении требований к защите ___ данных при их обработке в информационных системах персональных данных».

24. Постановление Правительства Российской Федерации от 6 июля 2008 г. № ___ «Об утверждении требований к материальным носителям

биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

25. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № ___ «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

26. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № ___ «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

27. Постановление Правительства Российской Федерации от 21 марта 2012 г. № ___ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

28. Постановление Правительства Российской Федерации от 18 сентября 2012 г. № ___ «Об утверждении правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с федеральной службой безопасности российской федерации и федеральной службой по техническому и экспортному контролю».

29. Постановление Правительства Российской Федерации от 21 ноября 2011 г. № ___ «Об организации лицензирования отдельных видов деятельности».

30. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № ___ «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

31. Постановление Правительства Российской Федерации от 3 февраля 2012 г. № ___ «О лицензировании деятельности по технической защите конфиденциальной информации».

32. Постановление Правительства Российской Федерации от 3 марта 2012 г. № ___ «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

33. Постановление Правительства РФ от 28 ноября 2011 г. № ___ «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи».

34. Постановление Правительства РФ от 09 февраля 2012 г. № ___ «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об

установлении требований к обеспечению совместимости средств электронной подписи».

35. Постановление Правительства Российской Федерации от 26 июня 1995 г. № ___ «О сертификации средств защиты информации».

Контрольные вопросы:

1. Какой документ из перечня является высшим в иерархии правовых актов?
2. Составьте иерархическую структуру нормативно-правовых актов РФ в области информационной безопасности, используя возможности MSWord
3. В каких случаях принимается Указ Президента?
4. В составленном перечне отметьте правовые акты, регламентирующие технические условия?
5. В составленном перечне отметьте правовые акты, регламентирующие организационные условия?
6. Какие документы из представленного перечня являются следствием ассоциирования правовых актов РФ с международным законодательством?

Аналитическая записка должна содержать иерархическую структуру исследованных правовых актов, сферу действия отдельных групп документов, соотношение и согласование групп правовых актов.

Содержание отчета: Тема, цель, перечень нормативно-правовых актов с полными реквизитами, ответы на контрольные вопросы, аналитическая записка.

Информационные источники:

1. http://www.consultant.ru/
2. http://www.garant.ru/
3. http://www.e-nigma.ru/articles/

ПРАКТИЧЕСКАЯ РАБОТА №4: НОРМАТИВНЫЕ МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ.

Цель: ознакомиться с нормативными методическими документами в области защиты информации, систематизировать сведения о нормативно-методических документах, приобрести опыт самостоятельного поиска и анализа.

Методы и приемы: лабораторная работа с использованием информационно-коммуникационных технологий, поисковая работа, анализ источников.

Ключевые слова: информационная безопасность, правовые акты, система нормативно-методических документов.

Порядок выполнения работы.

5. Используя любой интернет-браузер, найти нормативно-методические документы из представленного перечня.
6. Вставить недостающие реквизиты в перечень нормативных методических документов
7. Составить аналитическую записку - обзор по предложенному перечню.
8. Оформить отчет по лабораторной работе.

Нормативно методические документы в области информационной безопасности РФ

1. «Ответ требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

2. «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по Ответ каналам». Гостехкомиссия России. - М., 2002.

3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические ___ . Госстандарт России. - М., 1995.

4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие ___ . Госстандарт России. - М., 2006.

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и ___ - М., 2006.

6. ГОСТ Р ИСО/МЭК 15408-1-___ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

7. ГОСТ Р ИСО/МЭК 15408-2-___ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Росстандарт России. - М., 2013.

8. ГОСТ Р ИСО/МЭК 15408-3-___ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

9. ГОСТ Р ИСО/МЭК ___ -2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

10. ГОСТ Р ИСО/МЭК 27001-___ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

11. ГОСТ Р ИСО/МЭК 27002-___ «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», введен в действие с 01.01.2014

12. ГОСТ Р ИСО/МЭК 27003-___ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».

13. ГОСТ Р ИСО/МЭК 27004-___ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения».

14. ГОСТ Р ИСО/МЭК 27005-___ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

15. ГОСТ Р ИСО/МЭК 27006-___ «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».

16. ГОСТ Р ИСО/МЭК 27011-___ «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002».

17. ГОСТ Р ИСО/МЭК 27031-___ «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности

информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».

18. ГОСТ Р ИСО/МЭК 27033-1-___ «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».

19. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки ___ . Защита криптографическая. Алгоритм криптографического преобразования.

20. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. ___ защита информации. Процессы формирования и проверки электронной цифровой подписи.

21. ГОСТ Р 34.10-___ . Государственный стандарт Российской Федерации. Информационная технология. ___ защита информации. Процессы формирования и проверки электронной цифровой подписи.

22. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция ___ .

23. ГОСТ Р 34.11-___ . Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция ___ .

24. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № ___ «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

25. Приказ ФСБ России от 9 февраля 2005 г. № ___ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

26. Приказ ФСБ России от 30 августа 2012 г. № ___ «Об утверждении административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

27. Приказ ___ России от 08 августа 2009 г. № 149/7/2/6-1173 «Об утверждении типового регламента проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

28. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в ___ системах персональных данных с использованием средств автоматизации».

Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.

29. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих ___ тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622.

30. Приказ ФСБ России от 27 декабря 2011 г. № ___ «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

31. Приказ ФСБ России от 27 декабря 2011 г. № ___ «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

32. Приказ ФСБ России от ___ июля ___ г. № ___ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

33. Приказ ___ России от 20 марта 2012 г. № ___ «Об утверждении требований к средствам антивирусной защиты».

34. Приказ ___ России от 6 декабря 2011 г. № ___ «Об утверждении требований к системам обнаружения вторжений».

35. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по ___ персональных данных».

36. Приказ Минкомсвязи России от 29 сентября 2011 г. № 242 «Об утверждении порядка передачи реестров квалифицированных сертификатов ключей проверки ___ подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования ___ подписи в случае прекращения деятельности аккредитованного удостоверяющего центра».

37. Приказ Минкомсвязи России от 23 ноября 2011 г. № ___ «Об утверждении Административного регламента предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по организации ведения единого государственного реестра сертификатов ключей подписей удостоверяющих центров, обеспечению доступа к нему и к реестру сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, физических лиц и организаций».

38. Приказ Минкомсвязи России от 27 октября 2011 г. № ___ «Об утверждении Положения о Департаменте государственной политики в области создания и развития электронного правительства Министерства связи и массовых коммуникаций Российской Федерации».

39. Приказ Минкомсвязи России от 05 октября 2011 г. № ___ «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».

40. Приказ Минкомсвязи России от 23 ноября 2011 г. № ___ «Об аккредитации удостоверяющих центров».

41. Приказ Минкомсвязи России от 13 апреля 2012 г. № ___ «Об обеспечении осуществления Министерством связи и массовых коммуникаций РФ функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров».

42. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть ___ . Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия ___ возможностей». - М., 1999.

43. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. ___ и определения». - М, 1992.

44. Руководящий документ Гостехкомиссии России «___ защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». - М., 1992.

45. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от ___ доступа к информации. Классификация автоматизированных систем и требования по защите информации». - М, 1992.

46. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от ___ доступа к информации. Показатели защищенности от несанкционированного доступа к информации». -М., 1992.

47. Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в ___ системах и средствах вычислительной техники». - М., 1992.

48. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. ___ экраны. Защита от несанкционированного

доступа к информации. Показатели защищенности от несанкционированного доступа к информации». - М., 1997.

49. «Базовая модель угроз безопасности персональных данных при их обработке в ___ системах персональных данных». ФСТЭК России. - М., ___ .

50. «Методика определения ___ угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России. - М., 2008.

51. Приказ ФСТЭК России от 18 февраля ___ г. № ___ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

52. Приказ ФСТЭК России от 11 февраля ___ г. № ___ «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

53. Приказ ФСТЭК России от 14 марта ___ г. № ___ «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

54. Приказ ___ России от 12 июля 2012 г. № 83 «Об утверждении административного регламента федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».

55. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2011 г. № ___ «Об утверждении административного регламента проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных».

Контрольные вопросы

1. В составленном перечне отметьте правовые документы, регламентирующие технические условия?
2. В составленном перечне отметьте правовые документы, регламентирующие организационные условия?
3. Какие документы из представленного перечня являются следствием ассоциирования правовых актов РФ с международным законодательством?
4. Составьте классификацию исследованных документов по органу, принявшему тот или иной документ. Признак принадлежности к классу отметьте в перечне специальным значком.
5. Какова доля документов, регламентирующих организацию работ по защите персональных данных?
6. Какова доля документов, регламентирующих организацию работ по обороту средств технической защиты?

Аналитическая записка должна содержать иерархическую структуру исследованных правовых актов, сферу действия отдельных групп документов, соотношение и согласование групп правовых документов, принадлежность к государственному органу.

Содержание отчета: Тема, цель, перечень нормативно-правовых документов с полными реквизитами, ответы на контрольные вопросы, аналитическая записка.

Информационные источники:

1. http://www.consultant.ru/
2. http://www.garant.ru/
3. http://www.e-nigma.ru/articles/
4. http://fstec.ru/
5. http://www.iso27000.ru/zakonodatelstvo/normativnye-dokumenty-fstek-rossii

ПРАКТИЧЕСКАЯ РАБОТА №5: ПОНЯТИЙНЫЙ АППАРАТ НАПРАВЛЕНИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Цель: изучить понятийный аппарат направления «Информационная безопасность», получить опыт анализа и нормативных актов, формировать устойчивые навыки самостоятельной работы.

Методы и приемы: изучение теоретических источников, частично-поисковая работа, анализ, формулирование понятий.

Ключевые слова: информационная безопасность, персональные данные, информационная система, информация, коммерческая тайна, государственная тайна, информационно-коммуникационные технологии, защита информации.

Порядок выполнения работы

1. Сопоставить предложенный перечень понятий с определениями, приведенными ниже.
2. Результат сопоставления оформить в виде пар чисел, где арабская цифра – ключевое понятие, а римская цифра – его определение
3. Составить отчет по практической работе.

Часть 1.

1. **Вирус (компьютерный, программный)**
2. **Информационная система общего пользования**
3. **Документированная информация**
4. **Аутентификация отправителя данных**
5. **Государственная тайна**
6. **Информационная система**

7. **Автоматизированная обработка персональных данных**
8. **Блокирование персональных данных**
9. **Автоматизированная система**
10. **Информация**
11. **Гриф секретности**
12. **Вредоносная программа**
13. **Доступ к информации**
14. **Информационно-телекоммуникационная сеть**
15. **Вспомогательные технические средства и системы**
16. **Защищаемая информация.**
17. **Безопасность персональных данных**

I. программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

II. возможность получения информации и ее использования

III. технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

IV. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации

V. реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него

VI. сведения (сообщения, данные) независимо от формы их представления

VII. временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)

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

IX. подтверждение того, что отправитель полученных данных соответствует заявленному

X. состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных

XI. технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных

XII. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

XIII. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

XIV. обработка персональных данных с помощью средств вычислительной техники

XV. система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций

XVI. исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения

XVII. информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Часть 2

1. **Ключ проверки электронной подписи**
2. **Межсетевой экран**
3. **Несанкционированный доступ**
4. **Коммерческая тайна**
5. **Информационные технологии**
6. **Идентификация**
7. **Источник безопасности персональных данных**
8. **Ключ электронной подписи**
9. **Конфиденциальность**
10. **Информационная система персональных данных**
11. **Контролируемая зона**
12. **Корпоративная информационная система**
13. **Накопитель информации**
14. **Контрагент**
15. **Нарушитель безопасности персональных данных**
16. **Конрагент**
17. **Недекларированные возможности**

I. уникальная последовательность символов, предназначенная для создания электронной подписи

II. устройство, предназначенное для записи и (или) чтения информации на носитель информации. Устройство конструктивно может содержать в себе неотчуждаемый носитель информации, либо может быть предназначено для использования сменных носителей информации. Накопители подразделяются на встроенные (в конструктиве системного блока) и внешние (подсоединяемые через порт). Встроенные накопители подразделяются на съемные и несъемные

III. информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц

IV. физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке (в том числе техническими средствами) в информационных системах персональных данных

V. функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации

VI. процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов

VII. присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

VIII. уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи)

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

X. обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания

XI. совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

XII. пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание сторонних лиц, а также транспортных, технических и иных материальных средств

XIII. субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации

XIV. сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию

XV. доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных

XVI. режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

XVII. локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в

информационную систему персональных данных и (или) выходящей из информационной системы.

Часть 3

1. **Распространение информации**
2. **Побочные электромагнитные излучения и наводки**
3. **Правила разграничения доступа**
4. **Оператор**
5. **Пользователь ИСПДн**
6. **Обезличивание персональных данных**
7. **Предоставление информации**
8. **Оператор**
9. **Перехват информации**
10. **Обладатель информации**
11. **Носитель информации**
12. **Технические средства ИСПДн**
13. **Оператор ИС**
14. **Программная закладка**
15. **Персональные данные**
16. **Программное (программно-математическое воздействие)**
17. **Ресурс информационной системы**

I. действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

II. именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы

III. действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

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

V. несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ

VI. любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

VII. физический объект, предназначенный для хранения информации

VIII. электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания

IX. код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожать информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства

X. действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц

XI. лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования

XII. неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов

XIII. государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

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

XV. средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации)

XVI. совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

XVII. действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Часть 4

1. **Технический канал утечки информации**
2. **Целостность информации**
3. **Уполномоченное оператором лицо**

4. **Электронный документ**

5. **Электронное сообщение**

6. **Разглашение информации, составляющей коммерческую тайну**

7. **Сайт в сети Интернет**

8. **Уничтожение персональных данных**

9. **Утечка информации по техническим каналам**

10. **Субъект доступа**

11. **Электронная подпись**

12. **Средства вычислительной техники**

13. **Система защиты персональных данных**

14. **Трансграничная передача персональных данных**

15. **Удостоверяющий центр**

16. **Угрозы безопасности персональных данных.**

I. совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных

II. неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

III. действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору

IV. комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в ИСПДн

V. информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

VI. 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

VII. информация, переданная или полученная пользователем информационно-телекоммуникационной сети

VIII. способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения)

IX. лицо или процесс, действия которого регламентируются правилами разграничения доступа

X. документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

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

XII. совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по

сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет"

XIII. юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом

XIV. лицо, которому на основании договора оператор поручает обработку персональных данных

XV. совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем

XVI. совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Содержание отчета: Тема, цель, ответы по тематическим частям в виде пар чисел, где арабская цифра – ключевое понятие, а римская цифра – его определение.

Информационные источники

1. Чубукова С.Г. Организационное и правовое обеспечение информационной безопасности. Учебник и практикум. Серия: Профессиональное образование. ISBN: 9785991676076, Юрайт, 2016
2. http://www.e-nigma.ru/articles/
3. http://fstec.ru/

ПРАКТИЧЕСКАЯ РАБОТА №6: РЕГЛАМЕНТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Цель: ознакомиться с классификацией и регламентами автоматизированных систем (АС) различного назначения, получить знания применимости регламентов для конкретных АС, формировать устойчивые навыки самостоятельной работы.

Методы и приемы: изучение теоретических источников, формулирование определений, частично-поисковая работа, анализ, семинарское занятие.

Ключевые слова: автоматизированные системы (АС), регламенты АС, объекты информатизации, информационная безопасность, персональные данные, информационная система, государственные информационные системы информация, информационно-коммуникационные технологии, защита информации, ФСТЭК РФ, ФАПСИ РФ, ФСБ.

Порядок выполнения работы

1. Найти определения АС в соответствии с классификацией, принятой в действующей системе правовых актов и нормативно-методических документов.
2. Вставить определения вместо пропусков.
3. Отметить нормативные документы, регламентирующие функционирование конкретной АС в предлагаемом перечне нормативных документов.
4. Проверить правильность выполнения заданий путем совместного обсуждения и проверки.

5. Оценить участие каждого из обучающегося в практической работе и семинаре по образцу таблицы 2.

система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами)

Отметьте в списке 12 нормативных документов, которые относятся к данному объекту информатизации

1. 149-ФЗ от 27 июля 2006 г.
2. Указ Президента РФ от 17 марта 2008 г. № 351
3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
4. Пост. Правительства РФ № 512 от 6 июля 2008 г.
5. Пост. Правительства РФ № 687 от 15 сентября 2008 г.
6. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
7. СТР-К
8. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
9. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
10. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в

информационных системах общего пользования»
11. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
12. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999
13. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Термины и определения», 1992
14. РД Гостехкомиссии «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», 1992
15. РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992
16. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992
17. РД Гостехкомиссии «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», 1992
18. РД Гостехкомиссии «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к

информации», 1997
19. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
20. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
21. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
22. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны)

Отметьте в списке 4 нормативных документа, которые относятся к данному объекту информатизации

1. 149-ФЗ от 27 июля 2006 г.
2. Указ Президента РФ от 17 марта 2008 г. № 351
3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
4. Пост. Правительства РФ № 512 от 6 июля 2008 г.
5. Пост. Правительства РФ № 687 от 15 сентября 2008 г.
6. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
7. СТР-К
8. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
9. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
10. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
11. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
12. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999
13. РД Гостехкомиссии «Защита от несанкционированного доступа к

информации. Термины и определения», 1992
14. РД Гостехкомиссии «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», 1992
15. РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992
16. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992
17. РД Гостехкомиссии «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», 1992
18. РД Гостехкомиссии «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1997

автоматизированные системы управления, обеспечивающие контроль и управление технологическим и (или) производственным оборудованием (исполнительными устройствами) и реализованными на нем технологическими и (или) производственными процессами (в том числе системы диспетчерского управления, системы сбора (передачи) данных, системы, построенные на основе программируемых логических

контроллеров, распределенные системы управления, системы управления станками с числовым программным управлением).

Отметьте в списке 6 нормативных документов, которые относятся к данному объекту информатизации

1. 152-ФЗ от 27 июля 2006 г.
2. 98-ФЗ от 29 июля 2004 г.
3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
4. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
5. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
6. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
7. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999
8. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992
9. РД Гостехкомиссии «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1997

10. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
11. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
12. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
13. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

информационно-управляющая или информационно-коммуникационная система, которая осуществляет управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

Отметьте в списке 6 нормативных документов, которые относятся к данному объекту информатизации

1. 152-ФЗ от 27 июля 2006 г.
2. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
3. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
4. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
5. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
6. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
7. РД Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999
8. РД Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992
9. РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992
10. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры
11. Методика определения актуальных угроз безопасности информации

в ключевых системах информационной инфраструктуры
12. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
13. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры.
14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008.
15. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
16. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
17. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
18. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
19. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья

людей и для окружающей природной среды»

_____

совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Отметьте в списке 11 нормативных документов, которые относятся к данному объекту информатизации

1. 152-ФЗ от 27 июля 2006 г.
2. 149-ФЗ от 27 июля 2006 г.
3. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
4. Пост. Правительства РФ № 512 от 6 июля 2008 г.
5. Пост. Правительства РФ № 687от 15 сентября 2008 г.
6. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
7. Пост. Правительства РФ № 211 от 21 марта 2012 г.
8. Пост. Правительства РФ № 953 от 24 ноября 2009 г.
9. СТР-К
10. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
11. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
12. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в

информационных системах общего пользования»
13. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
14. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры
15. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры
16. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
17. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
18. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
19. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
20. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
21. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
22. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей

государственную тайну, содержащейся в государственных информационных системах»
23. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

федеральные информационные системы и региональные информационные системы, созданные на основании соответственно Федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

Отметьте в списке 6 нормативных документов, которые относятся к данному объекту информатизации

1. 149-ФЗ от 27 июля 2006 г.
2. 98-ФЗ от 29 июля 2004 г.
3. Указ Президента РФ от 17 марта 2008 г. № 351
4. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
5. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
6. СТР-К
7. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»

8. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»
9. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
10. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры
11. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры
12. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
13. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
15. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006
16. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008
17. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

18. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
19. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

федеральные государственные информационные системы, созданные или используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательных для размещения в информационно-телекоммуникационной сети Интернет, определяемые Правительством Российской Федерации.

Отметьте в списке 2 нормативных документа, которые относятся к данному объекту информатизации

1. 98-ФЗ от 29 июля 2004 г.
2. Пост. Правительства РФ № 1119 от 1 ноября 2012 г.
3. Пост. Правительства РФ № 1233 от 3 ноября 1994 г.
4. Пост. Правительства РФ № 211 от 21 марта 2012 г.

5. Пост. Правительства РФ № 953 от 24 ноября 2009 г.

6. Приказ ФСТЭК и ФСБ России № 416/489 от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008

8. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России, 2006

9. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008

10. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

11. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

12. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Таблица 2 Образец чек-листа для взаимного оценивания

Ф.И.О.	Степень участия: правильность выполнения, активность в обсуждении и приведении аргументов, баллы от 1 до 5
…	

Информационные источники:

1. Чубукова С.Г. Организационное и правовое обеспечение информационной безопасности. Учебник и практикум. Серия: Профессиональное образование. ISBN: 9785991676076, Юрайт, 2016
2. http://www.e-nigma.ru/articles/
3. http://fstec.ru/

ПРАКТИЧЕСКАЯ РАБОТА №7: РЕАЛИЗАЦИЯ МОДЕЛИ ПОЛИТИКИ БЕЗОПАСНОСТИ

Цель: ознакомиться с моделями управления доступом, научиться составлять матрицу доступа и иерархию ролей для учреждения профессионального учреждения для целей реализации политики безопасности, получить опыт принятия мотивированного решения.

Методы и приемы: изучение теоретических источников, контент-анализ сайтов образовательных учреждений, моделирование (политики безопасности), структурное программирование, кейс-метод.

Ключевые слова: политика безопасности, матрица доступа, ролевое управление доступом, мандатное управление доступом, объектно-ориентированный подход в ролевом управлении доступом, наследование ролей, инкапсуляция ролей

Краткие теоретические сведения

Под политикой безопасности понимают набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации.

Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.

Политика безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа: дискретное (дискреционное, избирательное) управление доступом; мандатное (полномочное) управление доступом.

Избирательное (или дискреционное) управление доступом характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек объект – субъект – тип доступа). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.

Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка – субъекту.

На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту.

Матрица доступа является самым простым подходом к моделированию систем управления доступом. С ростом организации, увеличивается опасность хищения информации, в том числе сотрудниками, возрастают финансовые и репутационные риски, это приводит к ужесточению политик и систем контроля. Любые избыточные права доступа сотрудников ведут к увеличению риска утечки информации, в связи с чем, происходит ужесточение политики ИБ, так как увеличиваются риски утечки информации.

Избирательная политика безопасности широко применяется в автоматизированных системах коммерческого сектора, так как её реализация соответствует требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость.

Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Полномочное (или мандатное)

управление доступом характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя [5]. Полномочное управление доступом подразумевает, что:

1) все субъекты и объекты системы однозначно идентифицированы;

2) каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;

3) каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

Чем важнее объект, тем выше его метка конфиденциальности, поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.

При выборе и реализации политики безопасности в автоматизированной системе проводится анализ угроз и рисков для информации и информационного обмена и определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей. Фрагмент матрицы доступа представлен в таблице 3.

Таблица 3 Пример матрицы доступа

Объект / Субъект	Файл_1	Файл_2	CD-RW	Дисковод
Администратор	Полные права	Полные права	Полные права	Полные права
Гость	Запрет	Чтение	Чтение	Запрет
Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Запрет

Ролевое управление доступом

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования, так как число связей в них пропорционально произведению количества пользователей на количество объектов, и тогда в этом случае принимаются решения в объектно-ориентированном стиле, способные эту сложность понизить. Таким решением является **ролевое управление доступом**.

Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (см. рис. 6).Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число

администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно. Ролевое управление доступом оперирует следующими основными понятиями: **пользователь** (человек, интеллектуальный автономный агент и т.п.); **сеанс работы пользователя; роль** (обычно определяется в соответствии с организационной структурой); **объект** (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД); **операция** (зависит от объекта; для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными); **право доступа** (разрешение выполнять определенные операции над определенными объектами).

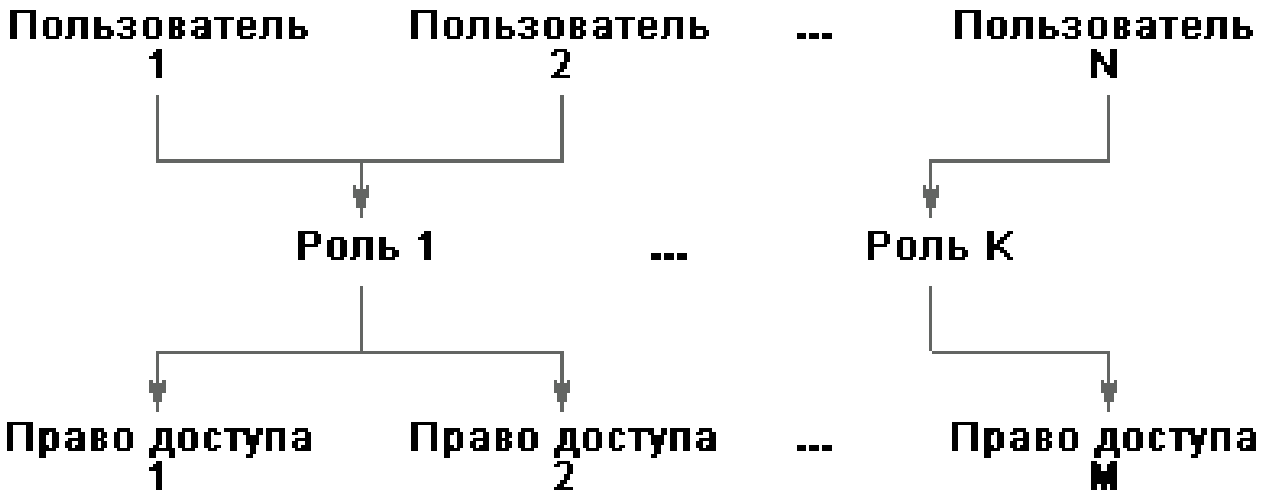


Рисунок 6. Схема ролевого управления доступом

Ролям приписываются пользователи и права доступа, то есть реализуется отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многим пользователям; один пользователь может быть приписан нескольким ролям. Во время сеанса раб0оты пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов. Между ролями

может быть определено отношение частичного порядка, называемое наследованием. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1.

Очевидно, что **наследование ролей** соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям – объекты (экземпляры) классов. Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить формирование **иерархии ролей**, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), до роли "руководитель".

При формировании иерархии ролей учитывается принципом **минимизации привилегий**, то есть каждой роли разрешено только то, что необходимо для выполнения служебных обязанностей.

Порядок выполнение работы:

1. Изучить теоретические сведения
2. Найти сайт образовательного учреждения
3. Смоделировать политику безопасности образовательного учреждения и составить матрицу доступа для образовательного учреждения.
4. Составить иерархию ролей для данного образовательного учреждения с описанием ролей сотрудников. При описании должен быть реализован принцип минимизации привилегий.
5. Ответить на контрольные вопросы. Оформить отчет.

Контрольные вопросы

1. Что понимается под политикой безопасности?
2. В чем заключается модель дискреционной политики безопасности?
3. В чем заключается модель мандатной политики безопасности?
4. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
5. Как соотносятся матрица доступа и ролевой доступ?
6. В каких случаях целесообразно использовать ролевой доступ?
7. В чем состоит принцип минимизации привилегий?

Содержание отчета: Тема, цель, матрица доступа учреждения, ролевой доступ, ответы на контрольные вопросы.

Информационные источники:

1. Галатенко В.А. Идентификация и аутентификация, управление доступом [Электронный ресурс]: http://citforum.ru/security/articles/galatenko/- (дата обращения - 01.03.2017)
2. https://www.anti-malware.ru/node/13626#part4

ПРАКТИЧЕСКАЯ РАБОТА №8: ПОСТРОЕНИЕ ЧАСТНОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ.

Цель: ознакомиться с содержанием и структурой частной модели угроз безопасности в информационной системе персональных данных (ИСПДн), получить опыт создания частной модели угроз безопасности для учреждения, имеющего информационную систему обработки персональных данных.

Методы и приемы: изучение теоретических источников, анализ, работа по шаблону, проектный кейс-метод, частично-поисковая работа, самостоятельная работа.

Ключевые слова: частная модель угроз, персональные данные, информационная система, модель нарушителя, угрозы утечки информации, технические каналы утечки информации, защищенность информационной системы, вероятность реализации угроз, корпоративная сеть, несанкционированный доступ.

Порядок выполнения работы

1. Изучить исходные условия существующей ИСПДн
2. Копировать шаблон частной модели угроз
3. Заполнить шаблон частной модели угроз по исходным условиям информационной систем обработки персональным данным.
4. Защитить свой проект частной модели угроз ИСПДн.

Исходные условия ИСПДн «Кадры»

Организация: ЗАО «Солнышко».

Директор: Иванов Иван Иванович.

Заместитель директора: Петрова Тамара Васильевна.

Начальник отдела кадров: Южина Мария Ивановна.

Сотрудники отдела кадров: Сидорова Александра Павловна,

Копылова Юлия Фёдоровна.

Состав ИСПДн:

1. Персональные данные сотрудников организации:

- фамилия, имя, отчество
- дата и место рождения
- пол
- сведения об образовании
- сведения о предыдущем месте работы
- семейное положение
- адреса регистрации и фактического проживания
- номера контактных телефонов
- индивидуальный номер налогоплательщика
- номер страхового свидетельства пенсионного страхования
- номер полиса обязательного медицинского страхования
- данные водительского удостоверения

В информационной системе одновременно обрабатываются данные 777 субъектов персональных данных (сотрудников) в пределах Организации.

2. Три автоматизированных рабочих места (АРМ) пользователей, сетевой принтер, сервер, коммутационное оборудование.

Топология: АРМ и сервер составляют сегмент корпоративной вычислительной сети (см. схему – рис. 7).

Корпоративная сеть: Организации не имеет подключения к сетям связи общего пользования и сетям международного информационного обмена.

В состав каждого АРМ входят два жёстких диска, на первом установлена операционная система, прикладное программное обеспечение и общедоступная справочная информация, на втором - информация, составляющая персональные данные сотрудников Организации.

Комплект АРМ №1-3: Системный блок № XXXXXXX01-03, Монитор Samsung N710 – серийный номер YYYYYYY01-03, клавиатура Genius серийный номер ZZZZZZZZ01-03, графический манипулятор (мышь) Genius серийный номер WWWW01-03,

В состав сервера входят три жестких диска, на первом установлена операционная система, прикладное программное обеспечение, второй и третий объединены в RAID массив, в котором хранится информация, составляющая персональные данные сотрудников Организации.

Комплект сервера: Системный блок № XXXXXXX04, Монитор Samsung N710 – серийный номер YYYYYYY04, клавиатура Genius серийный номер ZZZZZZZZ04, графический манипулятор Genius серийный номер WWWW04.

Сервер и коммуникационное оборудование установлены в типовой стойке.

Сетевой принтер HP LaserJet P2015 серийный номер SSSSSSSSS.

3. Технология обработки персональных данных:

Обработка персональных данных сотрудников включает весь перечень действий.

К работе на АРМ допущены сотрудники отдела кадров и заместитель директора.

Полный доступ ко всей информации на АРМ и сервере имеют заместитель директора и начальник отдела кадров.

Сотрудники отдела кадров имеют полный доступ только к каталогу «Личные дела», размещённой на диске №2 своего АРМ, и только на чтение информации из каталога «Личные дела» на сервере.

Системный администратор сегмента сети не имеет доступа к информации, составляющей персональные данные. Имеет права на инсталляцию, настройку программного обеспечения, программных (программно-аппаратных) средств защиты сервера и АРМ № 1-3. Режим работы - одновременный.

Расположение: Отдельный кабинет по адресу: РФ, г. Отрадный, ул. Веселая,, дом 6, офис 25.

Помещение офиса оборудовано охранной сигнализацией и в нерабочее время сдается под охрану.

Доступ в помещение ограничен распорядительными актами Организации и автоматизированной системой контроля и управления доступа.

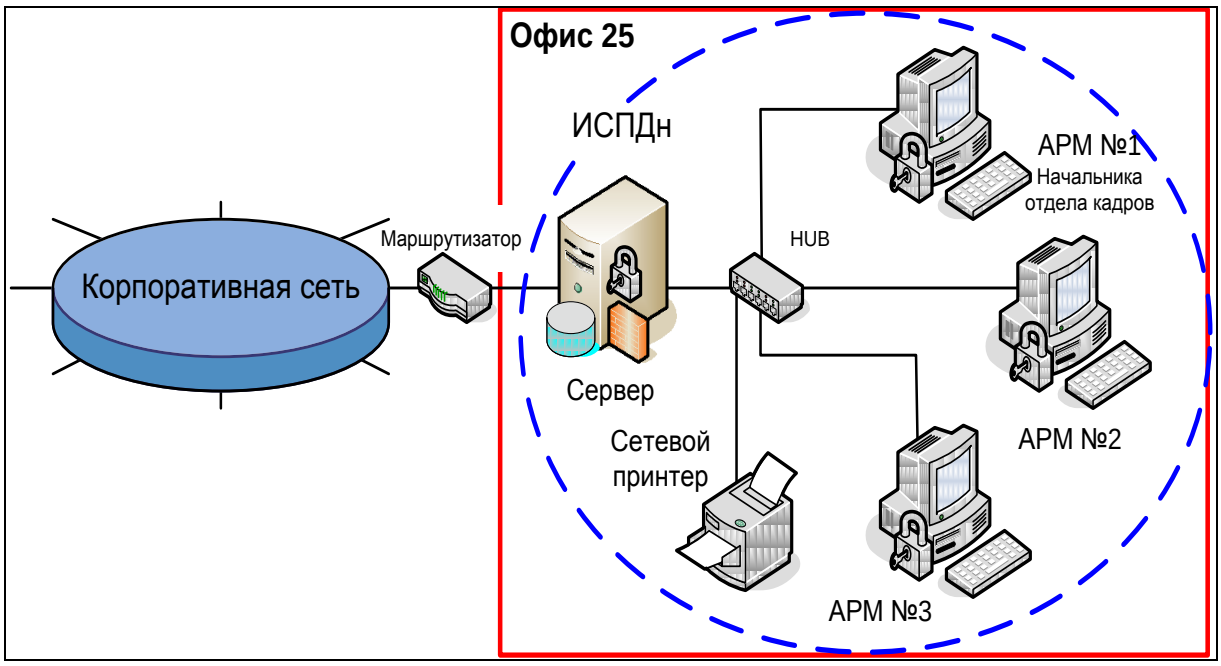


Рисунок 7. Схема корпоративной сети

УТВЕРЖДАЮ

_____

_____

(должность руководителя

организации)

_____

_____

(подпись)

«_____» _____ 201 ____г.

Частная модель угроз

безопасности персональных данных

при их обработке в ИСПДн

_____

(наименование ИСПДн)

СОГЛАСОВАНО

_____

___

«____» _____

201___ г

СОГЛАСОВАНО

_____

___

«____» _____

201___ г.

2017

Сокращения, условные обозначения

Термины и определения

Введение.

Современная система обеспечения информационной безопасности должна строиться на основе комплексирования разнообразных мер защиты и должна опираться на современные методы прогнозирования, анализа и моделирования возможных угроз безопасности информации и последствий их реализации.

Результаты моделирования предназначены для выбора адекватных оптимальных методов парирования угроз.

На стадии моделирования проведено изучение и анализ существующей обстановки и выявлены актуальные угрозы безопасности ПДн в составе ИСПДн

Модель угроз построена в соответствии с

1. Описание ИСПДн

1.1. Описание условий создания и использования ПДн

1.2. Описание форм представления ПДн

1.3. Описание структуры ИСПДн

1.4. Описание характеристик безопасности

2. Описание подхода к моделированию угроз безопасности ПДн.

Модель угроз безопасности ПДн в составе ИСПДн разработана на основе методических документов ФСТЭК:

На основе «Базовой модели угроз безопасности ПДн при их обработке в ИСПДн» проведена классификация угроз безопасности ПДн в составе ИСПДн и составлен перечень угроз безопасности ПДн в составе ИСПДн.

На основе составленного перечня угроз безопасности ПДн в составе ИСПДн с помощью «Методики определения актуальных угроз безопасности ПДн при их обработке в ИСПДн» построена модель угроз безопасности ПДн в составе ИСПДн и выявлены актуальные угрозы.

3. Классификация угроз безопасности персональных данных в ИСПДн

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угроз.

К характеристикам ИСПДн, обуславливающим возникновение УБПДн, можно отнести:

_____

_____

_____

ИСПДн представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности.

Основными элементами ИСПДн являются:

Основными **элементами канала реализации** УБПДн являются:

Носители ПДн могут содержать информацию, представленную в следующих видах:

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн угрозы классифицируются в соответствии со следующими признаками:

Реализация одной из УБПДн перечисленных классов или их совокупности может привести к следующим **типам последствий** для субъектов ПДн:

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и

приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн и описываются следующим образом:

Угрозы, связанные с НСД, представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

3.1. Общее описание угроз безопасности ПДн, обрабатываемых в ИСПДн

При обработке ПДн в ИСПДн возможна реализация следующих видов УБПДн:

3.2. Угрозы утечки информации по техническим каналам.

Основными элементами угроз утечки информации по техническим каналам являются:

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

Возникновение угроз утечки акустической (речевой) информации, содержащаяся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

3.3. Угрозы несанкционированного доступа.

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в

том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) ПДн, и включают в себя:

4. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн.

При обработке ПДн в ИСПДн, возможна реализация следующих видов УБПДн:

4.1. Угрозы утечки информации по техническим каналам.

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

4.1.1. Угрозы утечки акустической (речевой) информации.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, обусловлено наличием функций голосового

ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Утечка акустической (речевой) информации может быть осуществлена:

_____

_____

_____

В ИСПДн не реализованы функции голосового ввода ПДн в ИСПДн. Акустические средства воспроизведения ПДн в ИСПДн не предусмотрены.

Рассмотрение угроз утечки акустической (речевой) информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

4.1.2. Угрозы утечки видовой информации.

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Утечка видовой информации может быть осуществлена:

_____

_____

_____

В ИСПДн отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от

них, соответственно отсутствует возможность непосредственного наблюдения посторонними лицами ПДн.

Рассмотрение угроз утечки видовой информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

4.1.3. Угрозы утечки информации по каналам ПЭМИН.

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Рассмотрение угроз безопасности ПДн, связанных с перехватом ПЭМИН в ИСПДн, избыточно, так как носители ПДн (технические средства ИСПДн, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин) находятся в пределах контролируемой зоны. Утечка ПДн по каналам ПЭМИН – маловероятна из-за несоответствия стоимости средств съема информации и полученной в результате регистрации ПЭМИН информации, а защита ПДн от данного вида угроз – экономически нецелесообразна.

4.2. Угрозы НСД к ПДн, обрабатываемым в ИСПДн.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы

непосредственно в ИСПДн. Кроме этого, источниками угроз НСД к информации в ИСПДн могут быть аппаратные закладки и отчуждаемые носители вредоносных программ.

В ИСПДн возможны:

5. Общая характеристика источников угроз НСД.

Источниками угроз НСД в ИСПДн могут быть:

Нарушители:

Внутренние потенциальные нарушители подразделяются на **восемь категорий** в зависимости от способа доступа и полномочий доступа к ПДн (Таблица 4)

Таблица 4 Категории нарушителей

Категория нарушителя	**Способ доступа и полномочия**

Носитель вредоносной программы.

Носителем вредоносной программыможет быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

_____

_____

_____

_____

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

1. пакеты передаваемых по компьютерной сети сообщений;
2. файлы (текстовые, графические, исполняемые и т.д.).

Аппаратная закладка.

В ИСПДн имеется опасность применения аппаратных средств, предназначенных для регистрации вводимой с клавиатуры информации, например:

_____

_____

_____

В ИСПДн отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от них, соответственно отсутствует возможность установки аппаратных закладок посторонними лицами.

Существование данного источника угроз маловероятно также из-за несоответствия стоимости аппаратных закладок, сложности их скрытой установки и полученной в результате информации.

5.1. Общая характеристика уязвимостей ИСПДн.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данным.

Причины возникновения уязвимостей:

_____

_____

_____

К основным группам уязвимостей ИСПДн, относятся:

Характеристика уязвимостей системного ПО.

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем. При этом возможны уязвимости:

Уязвимости в микропрограммах и в средствах операционной системы, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Характеристика уязвимостей прикладного ПО.

К прикладному программному обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – это

Специальные прикладные программы – это

Уязвимости прикладного программного обеспечения могут представлять собой:

5.3. Характеристика угроз непосредственного доступа в операционную среду ИСПДн.

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к ПДн связаны с доступом:

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн:

Угрозы, реализуемые в ходе загрузки операционной системы

Угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем

Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ.Большая часть таких угроз – это угрозы внедрения вредоносных программ.

5.4. Общая характеристика УБПДн, реализуемых с использованием протоколов межсетевого взаимодействия.

Классификация угроз, реализуемых по сети, приведена в Таблице 5. В ее основу положено семь первичных признаков классификации.

Таблица 5 Описание угроз

№ п/п	Признак классификации	Тип угрозы	Описание

С учетом проведенной классификации можно выделить _____угроз, реализуемых с использованием протоколов межсетевого взаимодействия:

Анализ сетевого трафика.

Сканирование сети.

Угроза выявления пароля.

Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.

Навязывание ложного маршрута сети.

Внедрение ложного объекта сети.

Отказ в обслуживании.

Удаленный запуск приложений.

5..5. Общая характеристика угроз программно-математических воздействий.

Программно-математическое воздействие- это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИС, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИС с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИС.

Основными видами вредоносных программ являются:

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

5.6. Общая характеристика нетрадиционных информационных каналов.

Нетрадиционный информационный канал – это_____

Для формирования нетрадиционных каналов могут использоваться методы:

Методы компьютерной стеганографии предназначены для скрытия факта передачи сообщения путем встраивания скрываемой информации во внешне безобидные данные (текстовые, графические, аудио- или видеофайлы) и включают в себя **две группы методов**, основанных:

Нетрадиционные информационные каналы могут быть сформированы на различных уровнях функционирования ИСПДн:

5.7. Общая характеристика результатов несанкционированного или случайного доступа.

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

Нарушению конфиденциальности (копирование, неправомерное распространение), которое может быть осуществлено в случае утечки информации за счет:

Нарушению целостности (уничтожение, изменение) за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

Нарушение целостности информации в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы.

Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:

Нарушению доступности (блокирование) путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:

8. Определение уровня исходной защищенности ИСПДн

Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1).

Таблица 6 Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению			
2. По наличию соединения с сетями общего пользования:			
3. По встроенным (легальным) операциям с записями баз персональных данных:			
4. По разграничению доступа к персональным данным:			
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
6. По уровню обобщения (обезличивания) персональных данных:			
7.По объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			

В соответствии с Таблицей Описание угроз, _____ % характеристик ИСПДн соответствуют уровню не ниже "_____", следовательно,Y_1= _____ .

ИСПДн имеет _____ степень исходной защищенности.

9. Определение вероятности реализации угроз в ИСПДн

Под вероятностью реализации угрозы поднимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализации конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вероятность (Y_2) определяется по 4 вербальным градациям этого показателя:

Таблица 7 Вероятность реализации угроз (вербальный показатель)

Градация	**Описание**	**Вероятность (Y2)**

Оценка вероятности реализации угрозы безопасности различными категориями нарушителей приведена в следующей таблице

Таблица8 Вероятность реализации угроз (вероятностный показатель)

Угроза безопасности ПДн	Вероятность реализации угрозы нарушителем категории Кn

По итогам оценки уровня исходной защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы (Таблица 9). Коэффициент реализуемости угрозы рассчитывается по формуле: $Y = (Y_1+Y_2)/20$.

Таблица 9 Коэффициент реализуемости угрозы

Угроза безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы

1.1. Оценка опасности угроз ИСПДн

Оценка опасности производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет 3 значения:

низкая опасность – ……;

средняя опасность – ……;

высокая опасность – ……..

Оценка опасности с учетом приведенных критерием представлена в таблице 10.

Таблица 10 Оценка опасности

Угроза безопасности ПДн	Опасность угроз

1.2. Перечень актуальных УБПДн в ИСПДн

Правила, отнесения угроз к актуальным приведены в Таблице 11.

Таблица 11 Актуальность угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	неактуальная	актуальная
Средняя	Неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

В соответствии с правилами отнесения угроз безопасности к актуальным, для ИСПДн существуют следующие актуальные угрозы.

Таблица 12 Актуальные угрозы ИСПДн

Угроза безопасности ПДн	Опасность угроз

Таким образом, актуальными угрозами безопасности ПДн в ИСПДн являются:

_____

_____

_____

_____

Заключение

В настоящем документе проведена классификация УБПДн в ИСПДн, дано общее описание УБПДн и построена Модель угроз. В соответствии с требованиями методических документов ФСТЭК России, выявлены актуальные угрозы безопасности ПДн в ИСПДн, на основе которых в дальнейшем должны быть разработаны Требования по обеспечению безопасности ПДн в ИСПДн.

Построенная Модель угроз безопасности ПДн в ИСПДн применима к существующему состоянию ИСПДн при условии соблюдения основных (базовых) исходных данных:

- технические средства ИСПДн находятся в пределах контролируемой зоны;
- ИСПДн физически отделена от сетей общего пользования;
- отсутствует возможность неконтролируемого пребывания посторонних лиц в служебных помещениях ИСПДн и др.

В случае несоблюдения и/или изменения вышеуказанных условий Модель угроз безопасности ПДн в ИСПДн должна быть подвергнута пересмотру.

Информационные источники:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

3. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России.

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

ПРАКТИЧЕСКАЯ РАБОТА № 9 ПРАВОВЫЕ ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

Цель: научиться применять правовые акты в реальных ситуациях при организации защиты информации в учреждениях и на предприятиях, получить опыт разрешения правовых споров в области информационной безопасности, формировать законопослушность.

Методы и приемы: анализ, решение задач, проблемное обучение, мозговой штурм, семинар, кейс-метод.

Ключевые слова: государственная тайна, коммерческая тайна, персональные данные, защита информации, авторское право, интеллектуальная собственность, охранный документ, программа ЭВМ, база данных.

Порядок выполнения работы

1. Прочитать задачу, найти правовое обоснование и разрешить противоречивую правовую ситуацию.
2. Обсудить найденное решение, обосновать свою позицию аргументами и положениям правовых актов.
3. Решить задачи для самостоятельной работы по индивидуальному заданию

Раздел 1: Государственная тайна.

Задача 1.

Гражданин Иванов, служил в качестве члена научно-исследовательской группы института "Прогресс".

Иванов дал интервью для журнала «Метрополитен», в котором оценил радиационную обстановку в регионе с целью продемонстрировать суть его технической разработки по определению интенсивности излучения.

Интервью с Ивановым была опубликована и стала общедоступной, и научным руководством Института "Прогресс".

Администрация института подала заявление на Иванова о возбуждении уголовного дела по признакам преступлений, предусмотренных ст. 147 и ст. 183 Уголовного кодекса.

Защитнику Иванова стало известно, что Иванов воспользовался для разработки своего технического устройства сведениями, составляющими коммерческую тайну.

Будет ли Иванов привлечен к уголовной ответственности? Как ему избежать уголовной ответственности?

Задача 2

Репортер взял интервью у высокопоставленного чиновника Министерства экономического развития. В интервью были указаны сведения о стратегических запасах золота, платины и серебра. В отношении репортера и чиновника было возбуждено уголовное дело за распространение информации, составляющих государственную тайну.

Что нужно предпринять журналисту и чиновнику, чтобы избежать уголовной ответственности по ст. 283 УК РФ?

Задача 3

Инженер Михайлов, который был гражданином Российской Федерации и инженер Скрипко, который был гражданином Украины, провели совместной научно-исследовательской работу, разработали новую технологию по виртуализации доменов. Оба соавтора имели доступ к сведениям,

составляющим государственную тайну. При рассмотрении заявки федеральным органом исполнительной власти по интеллектуальной собственности было установлено, что в новой технологии использованы сведения, составляющие государственную тайну. Какой орган имеет право рассматривать заявки на секретные изобретения, если они относится к техническим средствам в области разведывательной деятельности?

Может ли в Российской Федерации быть выдан патент на секретное изобретение?

Задача 4

Химический комбинат г. Дубоссарск осуществил сброс производственных отходов в реку. Городские власти, получив от санэпидемслужбы города соответствующую информацию, не оповестили граждан об опасности. В результате купающиеся в реке получили ожоги.

Имеется ли вина городской администрации? Приведите правовые нормы, обосновывающие вашу позицию.

Задача 5

Российский научно-исследовательский институт «Квант» являлся разработчиком и создателем информационной базы данных об испытаниях авиационно-космической техники. Институт получил разрешение Правительства РФ и соответственно своего министерства о направлении соответствующей информации о характеристиках авиационной аппаратуры в аналогичную научную организацию, находящуюся на территории Белоруссии.

Однако представитель ФАПСИ, через которого предполагалось обеспечить передачу этой информации, обратил внимание дирекции института на конфиденциальный характер передаваемых сведений и, ссылаясь на этот факт, отказал НИИ в выделении каналов и средств для передачи информации.

Институт «Квант» обжаловал решение представителя ФАПСИ в Правительство РФ. Оцените ситуацию с точки зрения действующего законодательства [12].

Раздел 2: Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна

Задача 6

Общественная организация «За здоровье нации» обратилась к администрации Аргаяшской птицефабрики с заявлением о предоставлении информации о технике безопасности на предприятии: уровне ПДК в воздухе производственных помещений, уровне травматизма на производстве и выплате компенсаций по здоровьесбережению. Руководство предприятия отказалось удовлетворить просьбу общественной организации, мотивируя свое отказное решение тем, что указанные данные являются конфиденциальной информацией.

Дайте разъяснения по существу сложившейся ситуации, приведите правовые нормы в обоснование своих доводов.

Задача 7

Сотрудники частной нотариальной конторы «Дело» на одном из своих совещаний приняли решение — создать собственный тайный архив, в котором собирать наиболее интересную частную информацию о всех своих клиентах и по мере необходимости использовать ее в своей повседневной деятельности.

На следующий день был назначен руководитель архива и два эксперта и они начали собирать через своих коллег нужные сведения и данные о клиентах. Однако о факте создания тайного архива в нотариальной конторе «Дело» стало известно одному из клиентов, и он пожаловался на нотариусов в прокуратуру.

Нарушила ли в этом случае контора законодательство? [11]

Задача 8

Используя электронную сеть «Межсвязь», главный специалист коммерческого банка «Кубыш» Кусочкин в течение двух недель передавал с магнитных носителей информацию в департамент ценных бумаг ЦБ РФ.

При этом он однажды рассказал о содержании направленных в ЦБ сообщений своему другу – юристу Министерства связи Савенко. Савенко, зная, что его товарищи из адвокатской фирмы «Прокруст» готовят иск против «Кубыш», немедленно переправил им полученную информацию. Адвокаты по достоинству оценили полученные сведения, использовали их при подготовке иска и в итоге – выиграли дело у банка. Узнав об этом, председатель правления коммерческого банка «Кубыш» Кубышкин уволил Кусочкина с работы за разглашение коммерческой тайны. Кусочкин не согласился с решением Кубышкина и обжаловал его действия в суде.

Проанализируйте ситуацию с точки зрения норм информационного права и квалифицируйте действия Кусочкина, Савенко и Кубышкина [13].

Задача 9

Журналисты провели расследование совместно с общественной организацией «Маяк» и выявили повышенный уровень радиоизлучения в деревне Дербишево, находящейся на расстоянии 60 км от химкобината «Маяк». Об этом было рассказано в газете «За правое дело». Имеются ли в действиях журналистов признаки злоупотребления правом?

Оцените эту ситуацию с точки зрения законодательства о средствах массовой информации. Какие меры здесь необходимо принять к нарушителям?

Раздел 3: . Интеллектуальная собственность. Авторское право.

Задача 10

Лех Я.В. обратился в суд с иском к ООО «Гранада» о взыскании компенсации за нарушение исключительного права на произведение, компенсации морального вреда, возложении обязанности по удалению произведения с сайта.

В обоснование иска указал, что общество разместило на своем сайте литературно-художественный публицистический очерк (документальный рассказ), посвященный дню защиты Земли, автором которого он является Лех. Разрешение на публикацию очерка на сайте ответчика он не давал. Путем размещения на сайте указанного очерка было нарушено его авторское неимущественное право. Представитель ответчика факт размещения произведения истца на сайте не отрицала, исковые требования признала в части компенсации за нарушение ответчиком авторского права истца, при этом ссылалась на завышенный размер компенсации, заявленный истцом. В части компенсации морального вреда иск не признала, ссылаясь на то, что неимущественные права истца ответчиком не нарушены.

Отмечает, что «незаконно использованный» ответчиком очерк по количеству строк более чем в два раза превышает написанный им рассказ, авторские права на который были приобретены московским продюсером за 1000 долларов. При этом над очерком он работал около 4 месяцев, а рассказ написан за 1 день. Как разрешитъ этот спор с позиции норм информационного права?

Задача 11

Смирнов П.Б. обратился в суд с иском к Новиковой Е.О. о защите авторских прав. Свои требования истец мотивирует тем, что на странице

интернет-сайта ответчика неправомерно использована фотография, автором которой является истец, без его согласия на воспроизведение и доведение до всеобщего сведения, без заключения с истцом авторского лицензионного договора, без указания и ссылок на источник и автора произведения, что является нарушением ст. 1229, 1265, 1270, 1300 Гражданского кодекса Российской Федерации (далее по тексту ГК РФ). Ответчиком допущено искажение фотографии в частности: кадрирование, обрезка изображения, наложение на фотографию надписи изменение цветового фона изображения. Истец просил взыскать с Новиковой Е.О. денежную компенсацию за нарушение авторских исключительных прав на фотографию (произведение), компенсацию морального вреда за использование фотографии без указания авторства, судебные расходы по обеспечению доказательств нотариусом и расходы по оплате услуг представителя.

Ответчик вину в неправомерном размещении в сети Интернет фотографии не признала, пояснила, что фотографию удалила, ее размещение носило некоммерческий характер. Считает заявленные истцом суммы к взысканию завышенными. Оцените ситуацию с позиции правовых норм. Какое решение должен принять суд?

Задача 12

Организация «Новые технологии», занимающаяся формированием информационных ресурсов, начала разработку новой программы для государственных информационных систем. Для обеспечения защиты информационных ресурсов в этой системе был использован криптографический алгоритм «Криптт» компании «Джомолунгма» . Правомерно ли использование этого криптоалгоритма в разрабатываемой программе? Если да, то при каких условиях?

Задача 13

ООО «Холдинг-М» в лице Москвина осуществляло предоставление возмездных Интернет услуг с применением 2-х электронных терминалов «Инфоинтсэйл», на жестких дисках которых установлены и использовались для работы терминала два экземпляра программы для ЭВМ «Microsoft Windows XP Professional», обладателем авторских и смежных прав на которую является «Корпорация Microsoft».

Вышеуказанные экземпляры ЭВМ являются контрафактными по следующими признакам: отсутствуют документы, подтверждающие приобретение копии программы «Microsoft Windows XP Professional»; в корпусе системного блока не имеется сертификата подлинности программы (СОА) с наименованием и уникальным буквенно-цифровым ключом программного продукта; отсутствует соглашение с правообладателем об участии в программе корпоративного лицензирования, тем самым ООО «Холдинг-М» использовало с целью получения прибыли программу для ЭВМ «Microsoft Windows XP Professional». Представитель ООО «Холдинг-М» Москвин пояснял, что документов, подтверждающих приобретение обществом операционной «Windows XP» у него не имеется.

Оцените ситуацию с точки зрения авторского права.

Раздел 4 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Задача 14

Оператор ПК Абдуллин, согласно своим должностным обязанностям, приеме электронных носителей с материалами обязан был проверять их на

наличие вирусов. Пытаясь завершить работу как можно скорее, Абдуллин проигнорировал проверку на антивирусном программном обеспечении.

В результате попадания вируса в компьютерную систему был испорчен готовый к печати оригинал-макет выпуска газеты. Редакция понесла убытки, был нанесен репутационный вред изданию.

Оцените действия Абдуллина с точки зрения действующего законодательства.

Задача 15

Разработчик программного обеспечения Стив несколько лет работал в акционерном обществе "Галатея". В трудовом договоре не было указано на явно имущественные права на созданные программы в процессе трудовой деятельности программиста.

Во время работы Стив разработал эффективную систему автоматизации учета товаров на предприятии. Увидев, что его программа дает значительный экономический эффект, Стив потребовал от руководства доплату к ежемесячному окладу. Руководство рассмотрело вопрос по оплате и отказалось осуществлять доплату, вместо этого они приняли на работу еще одного программиста. Стив, в надежде, что он не сможет прийти к соглашению с компаниями, модифицировал свою программу, в результате чего она перестала функционировать.

Оцените сложившуюся ситуацию с точки зрения действующего законодательства. Как квалифицировать действия Стива?

Задача 16

Программисту Иванову было поручено создать базу данных по финансовым и нематериальным активам предприятия. В целях быстрейшего Иванов, стремясь выполнить свою работу как можно быстрее, проигнорировал

требования антивирусной защиты. В результате база данных и программная оболочка были повреждены, предприятию пришлось закупать новое программное обеспечение. На программиста было наложено административное взыскание штраф, с чем он не согласился и обжаловал действия администрации

Имеются ли здесь нарушения законодательства об информации, информатизации, защите информации и трудового права?

Раздел 5 Неправомерный доступ к информации.

Задача 17

Адвокат Хорошавин, работая в юридической фирме «Лига А» в качестве помощника генерального директора, получил несанкционированный доступ к программам других людей и постоянно использовал их. Более того, часть информации, полученной в базах данных, адвокат Хорошавин продал заинтересованным людям. В то же время, из-за несанкционированного проникновения помощника генерального директора в вышеупомянутые программы, в них начали появляться сбои, после чего владельцы источников информации, чтобы найти причину сбоя программного обеспечения провели экспертизу и установили причину сбоев. Владельцы программ и баз данных потребовали строгого наказания Хорошавина. Оцените сложившуюся ситуацию с точки зрения действующего законодательства.

Задача 18

Сельский почтальон по просьбе своей дочери подслушивал телефонные разговоры ее мужа. Он постоянно вскрывал письма и рассказывал об их содержании своей дочери, жалея ее, ведь она могла остаться одна и воспитывать двоих детей, если муж уйдет от нее к другой женщине.

Имеются ли нарушения законодательства?

Задачи для самостоятельного решения

1. Сотрудник завода Чернов попросил у знакомого бухгалтера дистрибутив на установку программы 1С. В процессе развертывания дистрибутива, Черновым была допущена серьезная ошибка и дистрибутив оказался испорченным. Не мудрствуя лукаво, Чернов решил вернуть другой дистрибутив, взятый в коммерческой фирме у другого знакомого бухгалтера. Оцените действия Чернова.

2. Разработчик программного обеспечения Шариков использовал часть алгоритма своего знакомого Кошечкина, уехавшего некоторое время назад в Европу. Шариков зарегистрировал программу в установленном порядке и получил охранный документ. Кошечкин узнал о коммерческом использовании Шариковым программного продукта и подал на него в суд. Необходимо классифицировать действия Шарикова и Кошечкина. Будет ли удовлетворен иск?

3. Петровский получил на телефон сообщение, в котором был прислан единоразовый пароль для входа в личный кабинет банковских транзакций его подруги Ивановской. Однажды Ивановская просила его телефон для проведения транзакций и, по-видимому, «привязала» номер к личному профилю интернет-банка. Петровский помнил номер карты Ивановской и, воспользовавшись единоразовым паролем, перевел часть денежных средств с банковской карты Ивановской на свой расчетный счет. Оцените действия Петровского и Ивановской с точки зрения информационной безопасности и норм права.

4. Гавриков, обладая специальными познаниями в области работы с электронными вычислительными машинами (далее - ЭВМ) и компьютерными программами, используя принадлежащую ему ЭВМ, имеющую подключение к сети Интернет, приобрел путем копирования с сайта «Fishki» компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной информации. Впоследствии посредством

принадлежащего ему компьютерного оборудования, а также находящихся в его пользовании хостинговых сервисов с доменными именами использовал указанные вредоносные компьютерные программы для заражения 50 ЭВМ пользователей сети Интернет и построения из них контролируемой сети. Построив контролируемую сеть, Гавриков без ведома и согласия пользователей скопировал хранящуюся в памяти зараженных ЭВМ компьютерную информацию, содержащую сведения о логинах и паролях авторизации пользователей на различных Интернет-ресурсах. Данную информацию Гавриков планировал использовать в личных целях. Оцените действия Гаврикова, приведите правовые нормы в обосновании своих доводов.

5. Анисимов работал и занимал различные должности в отделе технической поддержки UNIX Общества с ограниченной ответственностью (далее ООО) «Приват Трейд». С Анисимовым было заключено соглашение о конфиденциальности для работников ООО «Приват Трейд», согласно которого конфиденциальной информацией является техническая, технологическая, коммерческая (финансовая), организационная или иная используемая в коммерческой деятельности информация, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности неограниченному кругу третьих лиц, и к которой нет свободного доступа на законном основании.

В период с 2015 по 2016 годы Анисимов, находясь на своем рабочем месте, используя средства авторизации (логин и пароль), предоставленные ООО «Приват Трейд», и имея, в силу исполняемых обязанностей, доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, скопировал на USB – носитель информацию из базы данных ООО «Приват Трэйд», а именно: не менее 40.000 записей, содержащих не прошедших проверку имен, фамилий, никнеймов (имена, которые используется при регистрации на интернет сайтах), а так же адресов электронной почты. После чего Анисимов передал вышеуказанную

информацию Мусалову, который не был осведомлен о том, что полученная им информация охраняется внутренними документами ООО «Приват Трэйд».

Оцените действия Анисимова и Мусалова с правовых позиций действующего законодательства.

6. Закрытое акционерное общество «1С АКЦИОНЕРНОЕ ОБЩЕСТВО» (далее – ЗАО «1С») обратилось в Арбитражный суд Костромской области с иском к обществу с ограниченной ответственностью «Арктур» (далее – ООО «Арктур») о взыскании компенсации за незаконное использование результатов интеллектуальной деятельности в размере 90 000 руб. Исковые требования мотивированы тем, что в ходе обыска сотрудниками ОРЧ БЭП при УВД Костромской области были изъяты два системных блока и ноутбук, при осмотре выявлено, что на жестких дисках установлены компьютерные программы для ведения учета хозяйственной деятельности «1С: Предприятие 7.7. Комплексная поставка (сетевая версия)» и «1С: Предприятие 7.7. ПРОФ Комплексная поставка», имеющие признаки контрафактности. Согласно заключению эксперта от 28.04.2008 на жестких дисках, представленных на экспертизу системных блоков обнаружена информационная база с учетными данными ООО «Арктур», созданная с использованием программы «1С: Предприятие 7.7. Комплексная поставка (сетевая версия)». Запуск предположительно контрафактной программы «1С: Предприятие 7.7. Комплексная поставка (сетевая версия)» без аппаратного HASP-ключа защиты, вопреки штатного режима регламентируемого разработчиком был возможен вследствие модификации исполняемого файла. Оцените исход правого спора, приведите правовые нормы в подтверждение своей позиции.

7. Должностное лицо - индивидуальный предприниматель Сидорова не представила в установленный срок в государственный орган - Управление Федеральной службы государственной регистрации, кадастра и картографии сведения о состоянии использованных в процессе индивидуальной

деятельности геодезических пунктов. Имеется ли в действиях Сидоровой правонарушение?

8. В адрес Общества с ограниченной ответственностью «Мираторг», для подтверждения финансово-хозяйственных взаимоотношений выставлено требование об истребовании документов (информации) при проведении мероприятий налогового контроля в отношении Говоровой Н.Н. Конкурсный управляющий Общества с ограниченной ответственностью «Мираторг» (далее также - Общество) Хацевич А.А. сообщил, что требование не получал, несмотря на то, требование в адрес Общества было направлено заказным письмом по юридическому адресу организации и почтовому адресу организации и по адресу конкурсного управляющего. Истребуемые документы (информация) для проведения встречной проверки должны быть представлены в пятидневный срок со дня получения требования. Ходатайства о продлении срока предоставления документов (информации) в соответствии с п.5 ст.93.1 Налогового кодекса Российской Федерации в налоговый орган от обязанного представить соответствующие сведения лица не поступало. Имеется ли в действиях конкурсного управляющего правонарушение? Обоснуйте ответ правовыми нормами.

9. Заместителем генерального директора ОАО «УТК» по юридической и кадровой работе Громовой было направлено обращение в адрес министра строительства, жилищно-коммунального и дорожного хозяйства Республики Коми и Председателя Государственного Совета Республики Коми, содержащего, в числе прочего, информацию о проводимой работе по подготовке наградных листов для поощрения благодарностью Главы Республики Коми работников ОАО «УТК» - генерального директора Гаврилова и первого заместителя генерального директора - финансового директора Миронова. В соответствии с должностной инструкции Громова обязалась выполнять требования действующего законодательства РФ, приказов, инструкций, положений и иных нормативных актов по обеспечению

сохранности конфиденциальной информации, не разглашать и не передавать конфиденциальные сведения, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных обязанностей (договорных) обязанностей. Администрация ОАО «УТК» наложила на Громову административное взыскание за разглашение персональных данных работников, на что Громова не согласилась и обратилась в суд с иском по трудовому спору. Оцените исход правого спора, приведите правовые нормы в подтверждение своей позиции.

10. Руководитель отдела технических разработок ФАПСИ Куликов дал интервью журналу "Горизонты", отметив положительный опыт организации деятельности ФАПСИ в современных условиях. Интервью получило широкий резонанс среди читателей журнала, и редакция журнала выплатила гонорар Куликову. Руководству ФАПСИ стало известно об интервью Куликова и ему был объявлен выговор за выступление без разрешения руководства. Куликов расценил данное наказание как нарушение ч.1 ст. 29 Конституции РФ. Как можно расценить спор с точки зрения действующего законодательства?

11. Программист Якупов и адвокат Гришин создали компьютерную программу, для экспертной оценки подлинности рукописных текстов. Якупов и Гришин подали заявку в патентное ведомство России на выдачу патента на полезную модель. Патентное ведомство отклонило их заявку, указав, что программы для компьютеров не признаются патентоспособными изобретениями. Разработчики не согласились с данным отказом и обратились в суд. Необходимо дать разрешение данной спорной ситуации.

12. На совещании юридических и физических лиц, работающих в области информатики и телекоммуникаций, заместитель руководителя Торгово-промышленной палаты Российской Федерации Кошель в резкой форме покритиковал те организации, которые копируют и используют программные и технические средства информатики без разрешения собственника и допускают иные нарушения этических норм. А буквально на следующий день это выступление Кошеля было без сокращений опубликовано в «Вестях» и

обиженные организации потребовали от руководителя Торгово-промышленной палаты снятия с должности выступавшего за нарушение норм Национального кодекса деятельности в области информатики и телекоммуникаций. Необходимо определить, как должен быть разрешен этот спор.

13. На пленарном заседании торгово-промышленной палаты, посвященном взаимодействию в области развития сферы телекоммуникаций в регионе, вице-президент палаты Голенищев подверг резкой критике руководителей тех организаций, которые только «имитируют деятельность». Большой фрагмент стенограммы встречи был опубликован в областной газете. Обиженные руководители телекоммуникационных предприятий потребовали публикации опровержения в газете, а также снятия с должности вице-президента Голенищева за нарушение им норм «Положения об этике», принятом в Торгово-промышленной палате в качестве локального акта внутреннего распорядка. Вам нужно определить, как нужно решить спор.

14. Программист Войнович и его приятель техник-связист Саламатов обратились в Министерство связи с просьбой выделить им интернет-коммуникации для консалтинговой деятельности зарубежным партнерам. В удовлетворении заявления им было отказано. Войнович и Саламатов обратились за защитой прав предпринимателей в прокуратуру. Необходимо определить нарушен ли в этом случае порядок выделения ведомственных сетей связи юридическим и физическим лицам и как должен поступить прокурор города.

15. Гражданка Никанорова заподозрила своего мужа в измене и, установила специальную программу ему на телефон, пока он спал. Также она приобрела диктофонное устройство с дистанционным управлением, выполненное в виде дизайнерской зажигалки. Проанализировав детализацию звонков, полученную с помощью установленного программного обеспечения и диктофонные записи, гражданка Никанорова убедилась в правоте своих подозрений относительно неверности супруга, после чего подала на развод.

Супруг гражданки Никаноровой написал заявление о преступлении, совершенной его женой. Признаки какого преступного деяния были описаны в заявлении супруга? Укажите правовые нормы.

16. Писательница Левит получила большой гонорар за изданные в Китае ее книги по личностному развитию. Гонорар был перечислен на ее индивидуальный расчетный счет в «Уралоптобанк». Левит планировала использовать большую часть этих денежных средств на содержание приюта для животных «Спаси меня» известного зоозащитника Даллакяна, поэтому не подала налоговую декларацию о доходах. Налоговая инспекция запросила сведения о доходах Левит в «Уралоптбанк», банк сначала ответил отказом, а потом все-таки предоставил эти сведения, на основании которых налоговый инспектор выставил Левит предписание в виде штрафа и пени за неуплаченный налог на доходы. Разгневанная писательница подала на суд и налоговую инспекцию в суд. Как вы думаете, какое решение примет суд? Обоснуйте правовыми нормами свою позицию.

17. Заядлый охотник Михайлов купил на рынке бинокль повышенной видимости для использования его на охоте. Его приятель Дремов увидев такой бинокль, попросил его на некоторое время у Михайлова с целью подглядывания за своей женой, которая в соседнем квартале работала няней у состоятельных бизнесменов. Оцените действия Михайлова и Дремова с точки зрения действующего законодательства.

18. Начальником управления образования городского округа города Котельнича Червяковой в адрес руководителей образовательных учреждений направлено письмо с требованием о предоставлении в управление образования городского округа города Котельнича сведений об оплате ими и их подчиненными транспортного, земельного налога, налога на имущество. Указанные сведения представлены руководителями образовательных учреждений в управление образования городского округа города Котельнича и в последующем были переданы начальником управления образования

городского округа города Котельнича Червяковой в администрацию города Котельнича. Должностными обязанностями Червяковой не предусмотрено осуществление сбора, хранения, использования и распространения персональных данных руководителей и работников образовательных учреждений г. Котельнича, не связанных с осуществлением ими трудовой деятельности в образовательных учреждениях. Оцените ситуацию с точки зрения действующего законодательства.

19. Сотрудник рекрутингового агентства Жорин проводил отбор претендентов на должность личного помощника руководителя крупного промышленного предприятия. За хорошее выполнение этой работы ему была обещана персональная выплата от руководителя. Требования к будущему личному помощнику были следующие: высшее образование, модельная внешность, разговорный английский, кроме того девушка не должна быть замужем. Желая получить обещанную выплату Жорин в свободное от работы время съездил по адресам потенциальных претенденток и узнал от соседей их семейный статус. Как вы думаете имеет ли место нарушение законодательства?

Информационные источники:

1. http://www.garant.ru
2. http://www.consultant.ru
3. https://rospravosudie.com

ПРИМЕНЕНИЕ ИНВЕРСИОННОГО МЕТОДА ДЛЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ.

Цель: ознакомиться с инверсионным анализом ТРИЗ (теории решения изобретательских задач), научиться использовать инверсионный анализ для решения задач информационной безопасности, мотивировать обучающихся к расширению методологических оснований для будущей профессиональной деятельности.

Методы и приемы: работа по алгоритму, анализ, синтез, инвертирование, мозговой штурм, самостоятельная работа, решение задач.

Порядок выполнения работы

1. Изучить теоретические сведения, при необходимости обратиться к интернет-источникам

2. Изучить учебную задачу

3. Применить инверсионный метод для самостоятельного решения задач информационной безопасности.

Краткие теоретические сведения.

Инверсионный метод (Диверсионный анализ) — это один из разделов ТРИЗ (теории решения изобретательских задач – основоположник Альтшуллер Г.С.), направленный на выявление и предотвращение вредных явлений в системах различного генезиса — технических, информационных, организационных [1].

Суть метода состоит в инвертировании проблемной ситуации при выявлении технических противоречий в системе, то есть в создании системной диверсии.

Метод позволяет выявить явные и скрытые причины возможных отказов, уязвимостей, рисков, иных вредных явлений в системе, тем самым появляется возможность спрогнозировать и предотвратить проявление проблем такого рода, предусмотрев соответствующие меры при разработке или модификации системы. Таким образом, метод применяется:

• для поиска причин вредных явлений;

• для прогнозирования возможных вредных явлений.

Применительно к информационной системе, реализованной посредством информационно-коммуникационных технологий, задача состоит в ее «взломе» и несанкционированном доступе к информации.

Как правило, инверсионный метод реализуется через последовательные стадии:

1. Инвертирование задачи.

2. Формулирование «диверсионных гипотез».

3. Выявление «диверсионных ресурсов».

4. Тестирование «диверсионных гипотез».

В более сложных ситуациях может быть использован более широкий набор инструментов анализа [3].

Рассмотрим алгоритм решения учебной задачи с применением инверсионного метода и возможные схемы решений.

Учебная задача «Об электронной оболочке»: Необходимо определить перечень уязвимостей электронной оболочки личных профилей профессорско-преподавательского состава (далее - ППС) вуза, предложить меры по устранению потенциальных угроз.

Согласно ГОСТ Р 56545-2015 «уязвимость» – это недостаток (слабость) программного (программно-технического) средства или ИС в целом, который (которая) может быть использована для реализации угроз безопасности информации.

Информационная система – это совокупность содержащейся в базах данных (далее по тексту – БД) информации и обеспечивающих ее обработку информационных технологий и технических средств.

Стадия 1: Инвертирование задачи.

Переформулируем задачу в виде: «Как взломать электронную оболочку личных профилей ППС и получить доступ к конфиденциальной информации?»

Стадия 2: Формулирование диверсионных гипотез.

В вузе принят негласный шаблон составления логина профиля из фамилии и инициалов имени и отчества преподавателя. Таким образом, логин можно составить, исходя из сведений о фамилии, имени и отчества, данные сведения являются открытыми и доступны на сайте университета.

После определения логина, остается подобрать пароль.

Несложно просто подсмотреть пароль, либо при выполнении каких-либо работ попросить интересующего нас преподавателя войти в его профиль, ссылаясь на неработающий свой или какие-то неполадки системы. Этот способ допустим, если «добытчик» пароля является сотрудником и в силу своего должностного положения может осуществить описанную последовательность действий.

Если такая мера неосуществима, пароль можно вычислить, пользуясь специальным программным обеспечением. При известном логине, вычислительных ресурсов только «взлома» пароля требуется немного.

Существует множество программ, две наиболее популярные - advnced archive Password Recovery и Visaul Zip Password Recovery Processor.

Кроме вышеперечисленных способов

можно попытаться подобрать пароль с клавиатуры, используя известную информацию о человеке – день рождения, имя любимого питомца, и т.д.

Таким образом, предложены три диверсионные гипотезы для решения данной задачи.

Стадия 3: выявление диверсионных ресурсов.

На этой стадии необходимо составить список ресурсов, которые способствуют реализации диверсионных гипотез.

Перечень диверсионных ресурсов может быть таким:

- наличие шаблона составления логина;
- низкий уровень дисциплины ППС в области информационной безопасности;
- незнание и/или несоблюдение элементарных правил сохранения своих идентификаторов и аутентификаторов;
- малая обеспеченность компьютерной техникой рабочих мест ППС, когда за одним персональным компьютером закреплено несколько сотрудников.

Стадия 4: тестирование диверсионных гипотез - определение процедуры тестирования и проведение тестов.

Процедура тестирования состоит в экспериментальной проверке «взлома» электронной оболочки личных профилей ППС, то есть реализации выдвинутых гипотез на стадии 2.

Проверкой установлено, что логины были определены по шаблону «фамилия+инициалы». Среднее время определения логинов – 10 минут.

Подбор паролей с помощью программного обеспечения к трем профилям осуществлен в среднем в течение 30 минут, таким образом, тестирование подтвердило правоту диверсионных гипотез и наличие уязвимостей в описанной информационной системе.

При подведении итогов решения учебной задачи были предложены следующие способы усиления информационной защиты электронной оболочки:

- рекомендация замены логина и пароля пользователя после первого входа и активации профиля;
- разработка инструкции для сотрудников о необходимости сохранения аутентификаторов и идентификаторов;
- регулярный инструктаж сотрудников по соблюдению правил обеспечения информационной безопасности системы.

Задачи для самостоятельного решения.

a. **Задача «О защите интеллектуальной собственности свободными лицензиями».** Определить уязвимости для нарушения авторского права при распространении интеллектуальных продуктов в правовом поле свободных лицензий. Для определенности рассмотретьсемейства Common Public License, Cretive Commons Zero, Cretive Commons ttribution, GNU Generl Public License.

b. **Задача «О применении нейросетей для выявления террористических угроз».** В США потратили миллиарды долларов на разработку искусственного интеллекта, способного заменить человеческие ресурсы (проект ELINT- electronic intelligence) в разведке путем прослушивания и анализа разговоров по телефонам и анализа контента информационных ресурсов, используемых потенциальными террористами.

Когда проект ELINT был готов, президент Джимми Картер отозвал всех американских агентов с Ближнего Востока. С тех пор Соединенные Штаты не задержали ни одного крупного террориста. С помощью инверсионного анализа определите причину неудач.

c. **Задача «О проведении банковских транзакций».** Платежи физических лиц в настоящее время все чаще производятся с помощью смартфонов через личный профиль интернет-банка. Подтверждение платежей физическим лицом происходит через одноразовые пароли, высылаемые на привязанный номер мобильного оператора смс-сообщением. Определить уязвимости данной системы, используя методы инверсионного анализа.

d. **Задача «Защиты персональных данных».** С помощью инверсионного анализа определить уязвимости автоматизированной информационной системы (АИС) обработки персональных данных учреждения профессионального образования. Исходные данные АИС определить самостоятельно, используя сайт образовательного учреждения.

e. **Задача «О системе «Платон».** Используя инверсионный анализ, определите уязвимости системы «Платон» взимания платы с большегрузных автомобилей. Предложите меры для эффективного функционирования данной системы.

f. **Задача «Сетевой город».** В настоящее время в общеобразовательных школах введена система «Сетевой город». Определить уязвимости и способы защиты данной учебной системы.

g. **Задача «О стратегической космической онлайн игре EVE Online».** Взлом профиля противника в названной командной он-лайн игре дает множество игровых преимуществ, от перераспределения ресурсов, в том числе и реальных денежных средств, до тактического преимущества на отдельном этапе этой массовой многопользовательской он-лайн игры. Определите уязвимости профиля, используя инверсионный анализ и знание особенностей семиуровневой модели OSI.

h. **Задача «О сопровождении в социальной сети ВКонтакте».** Исследователи неоднократно поднимали вопрос о потенциальной угрозе национальной безопасности России, реализованной в социальных сетях. Экстремистские группы социальных сетей представляют реальную угрозу национальной безопасности страны, вовлекая до миллиона молодых граждан России, пропагандируя идеи политического экстремизма, национального и гендерного превосходства и неравенства. Подобных групп в социальных сетях немало и, если какие-то из них блокируются техническими службами по заявлениям неравнодушных пользователей, то на их месте появляется множество других с таким же опасным контентом. Используя инверсионный анализ, предложите меры по защите подрастающего поколения от негативного информационного воздействия экстремистских групп на примере социальной сети «ВКонтакте».

Информационные источники:

1. Абрамов О.Ю. Диверсионный анализ Технических Систем на переходном этапе развития - [Электронный ресурс] // URL: http://triz-summit.ru/file.php/id/f5015/nme/TRIZ- (дата обращения: 15.02.2017)
2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.
3. Буслов Д.И., Холкин И.Н. Как, используя диверсионный анализ ТРИЗ, найти критическую уязвимость, грозящую безопасности SP Hn // Математика и информационные технологии в нефтегазовом комплексе. 2015. №2. URL: http://cyberlenink.ru/rticle/n/kk-ispolzuy-diversionnyy-nliz-triz-nyti-kriticheskuyu-uyzvimost-grozyschuyu-bezopsnosti-sp-hn (дата обращения: 11.04.2017).
4. Вишнепольски С. Как выявлять причины вреда и устранять риски. Инверсионный метод риск-анализа. iBooks Edition. Mx E-Publishing, 2013. 131 с.

ПРИЛОЖЕНИЕ 1

КОМПЕТЕНЦИЯ МАГИСТРАНТА НАПРАВЛЕНИЯ «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТСИ В ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАНИИ», ФОРМИРУЕМАЯ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ «ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Таблица 11 Планируемые результаты обучения

Компетенция (содержание и обозначение в соответствии с ФГОС ВО и ОПОП)	**Результаты обучения в соответствии с ФГОС ВО и профессиональным (ми) стандартом(ами)**	**Конкретизация трудовых функций в рамках изучаемой дисциплины/модуля**
1	**2**	**3**
ПК-25 способность и готовность планировать и организовывать мероприятия для профессионального развития профессионально-педагогических работников профессиональных образовательных организаций, организаций дополнительного профессионального	**Знать:** З.1.Основные законодательные акты, регламентирующие образовательную деятельность З.2.Основные законодательные акты в области информационной безопасности 3.3.Функциональную структуру государственной системы обеспечения информационной безопасности	**Создание педагогических условий для развития группы (курса) обучающихся по программам высшего образования (ВО) – код D/01.6** **Трудовые знания:** Порядок обеспечения, нормативно-правовые основания и меры гражданско-правовой, административной, уголовной и дисциплинарной ответственности за жизнь и здоровье студентов, находящихся под руководством педагогического работника в организации, осуществляющей образовательную

образования		деятельность, и вне организации
	Уметь: У.1. Структурировать и оптимизировать информационные потоки учреждения У.2. Определять и использовать правовое основание для решения управленческих и организационных задач учреждения	**Трудовые умения:** Использовать средства формирования и развития организационной культуры группы (курса) **Трудовые умения:** Содействовать формированию лидерских качеств, правовых, культурных и нравственных ценностей студентов, системы общекультурных компетенций.
	Действовать (Владеть): Д.1. (В.1.) Разрабатывать концепцию и политику информационной безопасности конкретного учреждения, составлять частную модель угроз, определять политику безопасности учреждения	**Трудовые действия**: Организационно-педагогическая поддержка общественной, научной, творческой и предпринимательской активности студентов.
1	**2**	**3**

ПРИЛОЖЕНИЕ 2

ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

ТЕСТ 1

1. К каким мерам защиты относится политика безопасности?

а) к административным;

б) к законодательным;

в) к программно-техническим;

г) к процедурным.

2. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?

а) CL;

б) списки полномочий субъектов;

в) атрибутные схемы.

3. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?

а) целостность;

б) апеллируемость;

в) доступность;

г) конфиденциальность;

д) аутентичность.

4. К основным принципам построения системы защиты АИС относятся:

а) открытость;

б) взаимозаменяемость подсистем защиты;

в) минимизация привилегий;

г) комплексность;

5. Диспетчер доступа...

а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;

б) ... использует атрибутные схемы для представления матрицы доступа;

в) ... выступает посредником при всех обращениях субъектов к объектам;

г) ... фиксирует информацию о попытках доступа в системном журнале;

6. Какие предположения включает неформальная модель нарушителя?

а) о возможностях нарушителя;

б) о категориях лиц, к которым может принадлежать нарушитель;

в) о привычках нарушителя;

г) о предыдущих атаках, осуществленных нарушителем;

д) об уровне знаний нарушителя.

7. Что представляет собой доктрина информационной безопасности РФ?

а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;

б) федеральный закон, регулирующий правоотношения в области информационной безопасности;

в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;

г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

8. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?

а) политика безопасности верхнего уровня;

б) политика безопасности среднего уровня;

в) политика безопасности нижнего уровня;

г) принцип минимизации привилегий;

д) защита поддерживающей инфраструктуры.

9. Чтобы подписать сообщение электронной цифровой подписью, используются:

а) открытый ключ отправителя;

б) открытый ключ получателя;

в) закрытый ключ отправителя;

г) закрытый ключ получателя.

10. Какова последовательность подписания сообщений с помощью ЭЦП?

а) вычисляется хэш, затем хэш зашифровывается;

б) сообщение зашифровывается, после чего результат хэшируется;

в) при подписании сообщение зашифровывается, при проверке вычисляется хэш;

г) вычисляется хэш исходного сообщения, после чего оно зашифровывается.

11. В чем заключается такое свойство функции хэширования H как стойкость к коллизиям первого рода?

а) Для любого хэша h должно быть практически невозможно вычислить или подобрать такое x, что $H(x) = h$.

б) Должно быть практически невозможно вычислить или подобрать любую пару различных сообщений x и y для которых H(x) = H(y);

в) Длина хэша должна быть фиксированной независимо от длины входного сообщения;

Ключ к тесту: 1а, 2б, 3а, 4б, 5в, 6б, 7б, 8а, 9в, 10в, 11а.

ТЕСТ 2

1. **Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это....**

1. информационная война
2. информационное оружие
3. информационное превосходство

2. **Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.**

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

3. **Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена**

1. конфиденциальность
2. целостность
3. доступность

4. аутентичность
5. апеллируемость

4. **Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано**

1. надежность
2. точность
3. контролируемость
4. устойчивость
5. доступность

5. **Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.**

1. принцип системности
2. принцип комплексности
3. принцип непрерывной защиты
4. принцип разумной достаточности
5. принцип гибкости системы

6. **В классификацию вирусов по способу заражения входят**

1. опасные
2. файловые
3. резидентные
4. загрузочные
5. файлово -загрузочные
6. нерезидентные

7. **Комплекс превентивных мер по защите конфиденциальных данных и**

информационных процессов на предприятии это...

1. комплексное обеспечение И Б
2. безопасность АС
3. угроза И Б
4. атака на АС
5. политика безопасности

8. **Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:**

1. компаньон - вирусами
2. черви
3. паразитические
4. студенческие
5. призраки
6. стеле-вирусы

9. **К видам системы обнаружения атак относятся :**

1. системы, обнаружения атаки на ОС
2. системы, обнаружения атаки на конкретные приложения
3. системы, обнаружения атаки на удаленных БД
4. все варианты верны

10. **Автоматизированная система должна обеспечивать**

1. надежность
2. доступность
3. целостность
4. контролируемость

11. **Основными компонентами парольной системы являются**

1. интерфейс администратора
2. хранимая копия пароля
3. база данных учетных записей
4. все варианты верны

12. **Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ....**

1. идентификатор пользователя
2. пароль пользователя
3. учетная запись пользователя
4. парольная система

13. **К принципам информационной безопасности относятся**

1. скрытость
2. масштабность
3. системность
4. законность
5. открытости алгоритмов

14. **К вирусам, изменяющим среду обитания относятся:**

1. черви
2. студенческие
3. полиморфные
4. спутники

15. **Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это...**

1. Защита информации
2. Компьютерная безопасность

3. Защищенность информации
4. Безопасность данных

16. **Система физической безопасности включает в себя следующие подсистемы:**

1. оценка обстановки
2. скрытность
3. строительные препятствия
4. аварийная и пожарная сигнализация

17. **Какие степени сложности устройства Вам известны**

1. упрощенные
2. простые
3. сложные
4. оптические
5. встроенные

18. **К механическим системам защиты относятся:**

1. проволока
2. стена
3. сигнализация

19. **Какие компоненты входят в комплекс защиты охраняемых объектов:**

1. датчики
2. телевизионная система
3. лес

20. **К выполняемой функции защиты относится:**

1. внешняя защита
2. внутренняя защита

3. все варианты верны

21. **Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных**:

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

22. **Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:**

1. информационная война
2. информационное оружие
3. информационное превосходство

23. **Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:**

1. государственная тайна
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

24. **Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:**

1. конфиденциальность
2. целостность
3. доступность

4. аутентичность
5. апеллируемость

25. **Гарантия точного и полного выполнения команд в АС:**

1. надежность
2. точность
3. контролируемость
4. устойчивость
5. доступность

26. **Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:**

1. принцип системности
2. принцип комплексности
3. принцип непрерывности
4. принцип разумной достаточности
5. принцип гибкости системы

27. **Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:**

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. атака на автоматизированную систему
5. политика безопасности

28. **Особенностями информационного оружия являются:**

1. системность
2. открытость

3. универсальность
4. скрытность

29. **К функциям информационной безопасности относятся:**

1. выявление источников внутренних и внешних угроз
2. страхование информационных ресурсов
3. защита государственных информационных ресурсов
4. подготовка специалистов по обеспечению информационной безопасности
5. все ответы верны

30. **К типам угроз безопасности парольных систем относятся**

1. словарная атака
2. тотальный перебор
3. атака на основе психологии
4. разглашение параметров учетной записи
5. все варианты ответа верны

31. **К вирусам не изменяющим среду обитания относятся:**

1. черви
2. студенческие
3. полиморфные
4. спутники

32. **Хранение паролей может осуществляться**

1. в виде сверток
2. в открытом виде
3. в закрытом виде
4. в зашифрованном виде
5. все варианты ответа верны

33. **Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:**

1. ревизором
2. иммунизатором
3. сканером
4. доктора и фаги.

34. **Указать недостатки, имеющиеся у антивирусной программы ревизор**:

1. неспособность поймать вирус в момент его появления в системе
2. небольшая скорость поиска вирусов
3. невозможность определить вирус в новых файлах (в электронной почте, на дискете)
4. все варианты верны

35. **В соответствии с особенностями алгоритма вирусы можно разделить на два класса:**

1. Вирусы, изменяющие среду обитания, но не распространяющиеся
2. Вирусы, изменяющие среду обитания при распространении
3. Вирусы, не изменяющие среду обитания при распространении
4. Вирусы, не изменяющие среду обитания и не способные к распространению в дальнейшем

36. **К достоинствам технических средств защиты относятся:**

1. регулярный контроль
2. создание комплексных систем защиты
3. степень сложности устройства
4. Все варианты верны

37. **К тщательно контролируемым зонам относятся:**

1. рабочее место администратора
2. архив
3. рабочее место пользователя
4. все варианты верны

38. **К системам оповещения относятся:**

1. инфракрасные датчики
2. электрические датчики
3. электромеханические датчики
4. электрохимические датчики

39. **К оборонительным системам защиты относятся:**

1. проволочные ограждения
2. звуковые установки
3. дачики
4. покрышки

40. **К национальным интересам РФ в информационной сфере относятся:**

1.Реализация конституционных прав на доступ к информации

2. Защита информации, обеспечивающей личную безопасность

3. Защита независимости, суверенитета, государственной и территориальной целостности

4. Политическая экономическая и социальная стабильность

5. Сохранение и оздоровлении окружающей среды

Ключ к тесту: 1-1, 2-4, 3-1, 4-1, 5-5, 6-3,6, 7-1, 8-2, 9-4, 10-2,3, 11-1,3, 12-2, 13-3,4,5 14-3,15-1, 16-1,3,4, 17-2,3, 18-1,24, 19-1,2, 20-3,21-2, 22-2, 23-2, 24-2, 25-2,26-4, 27-5, 28-3,4, 29-5, 30-5, 31-1, 32-1,2,4 33-3, 34-4, 35-2,3, 36-2, 37-4, 38-1,2, 39-1,2, 40-1.

ПРИЛОЖЕНИЕ 3

СОДЕРЖАНИЕ КОНЦЕПЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ

- Общие положения
- Описание объекта защиты
    - Назначение и основные функции информационной системы
    - Группы задач, решаемых в информационной системе
    - Классификация пользователей системы
    - Организационная структура обслуживающего персонала
    - Структура и состав комплекса программно-технических средств
    - Корпоративная сеть предприятия
        - Серверы
        - Рабочие станции
        - Линии связи и активное сетевое оборудование
        - Виды информационных ресурсов, хранимых и обрабатываемых в системе
        - Структура информационных потоков
            - Внутренние информационные потоки
            - Внешние информационные потоки
        - Характеристика каналов взаимодействия с другими системами и точек входа
- Основные факторы, влияющие на информационную безопасность предприятия
- Основные принципы обеспечения информационной безопасности
- Организация работ по защите информации
- Меры обеспечения информационной безопасности
    - Меры обеспечения информационной безопасности организационного уровня

    - Требования к подсистеме предотвращения утечки информации по техническим каналам
- Технические требования к смежным подсистемам
    - Требования к структурированной кабельной системе
    - Требования по физической защите
- Ответственность сотрудников за нарушение безопасности
- Механизм реализации концепции

Информационный источник:

http://securitypolicy.ru - (Дата обращения: 08.04.2017).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Стандарты

ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования .

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические ___ . Госстандарт России. - М., 1995.

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. - М., 2006.

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие требования. Госстандарт России. - М., 2006.

ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». – М.: Стандартинформ, 2015.

Используемая литература

5. Абрамов О.Ю. Диверсионный анализ Технических Систем на переходном этапе развития - [Электронный ресурс] // URL: http://triz-summit.ru/file.php/id/f5015/nme/TRIZ- (дата обращения: 15.02.2017)
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.
7. Буслов Д.И., Холкин И.Н. Как, используя диверсионный анализ ТРИЗ, найти критическую уязвимость, грозящую безопасности SP Hn // Математика и информационные технологии в нефтегазовом комплексе. 2015. №2. URL: http://cyberlenink.ru/rticle/n/kk-ispolzuy-diversionnyy-nliz-triz-nyti-kriticheskuyu-uyzvimost-grozyschuyu-bezopsnosti-sp-hn (дата обращения: 11.04.2017).
8. Вишнепольски С. Как выявлять причины вреда и устранять риски. Инверсионный метод риск-анализа. iBooks Edition. Mx E-Publishing, 2013. 131 с.
9. Галатенко В.А. Идентификация и аутентификация, управление доступом [Электронный ресурс]: http://citforum.ru/security/articles/galatenko/- (дата обращения - 01.03.2017)
10. Гафарова Е.А., Азарова Е.А., Гафаров В.Ф, Гафаров М.Ф. Применение инверсионного метода для выявления уязвимостей информационной системы в обучении магистрантов. //Информационные технологии в экономике, образовании и бизнеса. Саратов: Издательство «ЦПМ Бизнес», 2017, с.22-28, ISBN 978-5-9909175-3-8
11. Гафарова Е.А., Гафаров М.Ф. О необходимости педагогического сопровождения в социальной сети «ВКонтакте».// Личность, семья и

общество: вопросы педагогики и психологии: сб. ст. по матер. LXVII междунар. науч.-практ. конф. № 8(65). – Новосибирск: СибАК, 2016. – С. 19-23.

12. Гафарова Е.А.О возможности использования открытых лицензий для защиты интеллектуальных прав создателей научных и образовательных ресурсов.//Сб. материалов II-ой международной научно-практической конференции. 2016 Издательство: Научно-издательский центр "Империя" (Москва), с.46-49
13. Гафарова Е.А. К вопросу обеспечения информационно-психологической безопасности подрастающего поколения в условиях интенсификации воздействия интернет-источников.// Научная дискуссия: инновации в современном мире: сб. ст. по материалам LVI Международной научно-практической конференции «Научная дискуссия: инновации в современном мире». – № 12(55). – М., Изд. «Интернаука», 2016. – С. 115-118.
14. Гафарова Е.А., Синицын Ф.В. К вопросу проектирвоания онтологий предметной области при подготовке магистров по направлению информационная безопасность.// Инновационные технологии в подготовке современных профессиональных кадров: Опыт, проблемы. Сборник научных трудов. 2016, Челябинский филиал РАНХиГС, 56-59 с.
15. Грицай Л.А. Информационная война в социальных сетях как угроза национальной безопасности России // Современные научные исследования и инновации. 2014. № 10 – [Электронный ресурс] – URL: http://web.snuk.ru/issues/2014/10/38607 (Дата обращения: 24.05.2016).
16. Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности: Учебное пособие. - СПб.: НИУ ИТМО, 2013. - 148 с.

17. Коноваленко С. А., Королев И. Д. Выявление уязвимостей информационных систем. // Инновации в науке: сб. ст. по матер. LXI междунар. науч.-практ. конф. № 9(58). – Новосибирск: СибАК, 2016. – С. 12-20.
18. Мезенов А.С., Гафарова Е.А. О реализации конституционного права граждан на доступ к информации в условиях интенсификации сетевого взаимодействия.//Сборник научных трудов конференции «Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы», 2016, Издательство: Челябинский филиал РАНХиГС, с.94-99
19. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.
20. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России.
21. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / А. А. Стрельцов [и д р.]; под ред. А. А. Стрельцова. — М .: Издательский центр «Академия», 2008. — 256 с. ISBN 978-5-7695-4240-4
22. Приказ Министерства образования и науки РФ от 1 декабря 2016 г. № 1513 “Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры)”- [Электронный ресурс] // URL: http://www.grnt.ru/products/ipo/prime/doc/71471182/#ixzz4WszFeZNc – (дата обращения 15.02.2017)
23. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

24. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении доктрины информационной безопасности Российской Федерации” [Электронный ресурс] /– URL: http://www.grnt.ru/hotlw/federl/1036728/ - (Дата обращения: 08.04.2017).
25. Фомичева Т.Г. Лабораторный практикум по курсу «Компьютерные технологи и в правовой практике» Южно-Российский государственный технический университет, УДК 004.9:34 (076.5) ББК 67.0 Ф 76Новочеркасск 2008
26. Чубукова С.Г. Организационное и правовое обеспечение информационной безопасности. Учебник и практикум. ISBN: 9785991676076 Год издания: 2016. Серия: Профессиональное образование. Издательство: Юрайт.
27. Шиллер В.В., Шелудков Н.Н. Российские социальные сети как потенциальная угроза национальной безопасности России (на примере сайтов «Одноклассники» и «Вконтакте») // Вестник КемГУ. 2013. № 3 (55). URL: http://cyberlenink.ru/rticle/n/rossiyskie-sotsilnye-seti-kk-potentsi... (Дата обращения: 21.07.2016).
28. Kpln S., Visnepolschi S., Zlotin B., Zusmn . New tools for filure & risk nlysis.n Introduction to nticiptory Filure Determintion (FD) nd The Theory of Scenrio Structuring. Idetion Interntionl Inc., 1999.

Электронные ресурсы.

[Электронный ресурс] // URL: https://www.anti-malware.ru/node/13626#part4- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: http://www.e-nigm.ru/rticles/- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: http://www.iso27000.ru/zkonodtelstvo/normtivnye-dokumenty-fstek-rossii- (Дата обращения: 22.02.2017)

[Электронный ресурс] // URL: http://www.intuit.ru - (Дата обращения: 22.02.2017)
[Электронный ресурс] // URL: http://www.garant.ru/- (Дата обращения: 22.02.2017)
[Электронный ресурс] // URL: http://www.consultant.ru/- (Дата обращения: 22.02.2017)
[Электронный ресурс] // URL: https://rospravosudie.com- (Дата обращения: 22.02.2017)
[Электронный ресурс] // URL: httpps://www.scienceforum.ru- (Дата обращения: 22.02.2017)
[Электронный ресурс] // URL: http://securitypolicy.ru - (Дата обращения: 08.04.2017).
[Электронный ресурс] // URL: http://fstec.ru/- (Дата обращения: 22.02.2017)
[Электронный ресурс] // URL: https://ru.wikipedi.org - (Дата обращения: 22.02.2017)

Учебное издание

Елена Аркадьевна Гафарова

Организационное-правовое обеспечение информационно й безопасности

Учебное пособие

Издательство ЗАО «Библиотека А.Миллера»

454091, г. Челябинск. Ул. Свободы, 159

Подписано в печать 14.04.2019 Формат 60х90/16из.

Объем 4,1 уч.- изд. л. Тираж 100 экз.

Заказ 374

Отпечатано с готового оригинал-макета

в типографии ЮУРГГПУ

454080, г. Челябинск, пр. Ленина, 69