МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Шуйский филиал ИвГУ

Кафедра математики, информатики и методики обучения

ОДОБРЕНО:

Руководитель ОП

_____ А.С. Зинченко
(подпись)

«25» февраля 2025 г.

Рабочая программа дисциплины
МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Уровень высшего образования:	бакалавриат
Квалификация выпускника:	бакалавр
Направление подготовки:	44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль) образовательной программы:	Математика; Информатика и VR-технологии

Шуя

1. Цели освоения дисциплины: содействовать становлению профессиональной компетентности бдящего педагога через формирование у студентов системы знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации в образовательных учреждениях.

2. Место дисциплины в структуре ОП

Дисциплина «Методы и средства защиты информации» является обязательной для изучения, относится к обязательной части блока дисциплин Б1, входит в предметно-педагогический модуль.

Успешное освоение данной дисциплины будет способствовать готовности обучающихся к прохождению производственной практики, научно-исследовательской работы (предметно-методический модуль), производственной практики, педагогической (комплексной) практики (предметно-методический модуль), подготовке к сдаче и сдаче государственного экзамена, выполнению и защите выпускной квалификационной работы.

Студент, приступающий к изучению данной дисциплины, должен:

Знать:

– базовые понятия информатики;

– возможности и ограничения актуальных информационных технологий.

Уметь:

– достигать поставленной цели с использованием заданного множества информационных средств;

– распознавать типовые отклонения в функционировании компьютерной системы в процессе её целенаправленного применения.

Владеть:

– способами осмысления и критического анализа информации;

– навыками совершенствования и развития своего когнитивного потенциала.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

3.1. Компетенции, формированию которых способствует данная дисциплина

При реализации дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

а) универсальные компетенции (УК) и индикаторы их достижения:

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Код и наименование индикатора достижения универсальной компетенции
Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении	УК.8.1. Оценивает факторы риска, умеет обеспечивать личную безопасность и безопасность окружающих в повседневной жизни и в профессиональной деятельности, а также при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов. УК.8.2. Формирует культуру безопасного и ответственного поведе-

	чрезвычайных ситуаций и военных конфликтов	ния в повседневной жизни и в профессиональной деятельности, а также использует методы защиты в чрезвычайных ситуациях и военных конфликтах.

б) общепрофессиональные компетенции (ОПК) и индикаторы их достижения:

Наименование категории (группы) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Код и наименование индикатора достижения общепрофессиональной компетенции
Правовые и этические основы профессиональной деятельности	ОПК-1. Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики.	ОПК-1.1. Понимает и объясняет сущность приоритетных направлений развития образовательной системы Российской Федерации, законов и иных нормативно- правовых актов, регламентирующих образовательную деятельность в Российской Федерации, нормативных документов по вопросам обучения и воспитания детей и молодежи, федеральных государственных образовательных стандартов дошкольного, начального общего, основного общего, среднего общего, среднего профессионального образования, профессионального обучения, законодательства о правах ребенка, трудового законодательства. ОПК-1.2. Применяет в своей деятельности основные нормативно-правовые акты в сфере образования и нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности.
Научные основы педагогической деятельности	ОПК-8. Способен осуществлять педагогическую деятельность на основе специальных научных знаний	ОПК-8.1. Применяет методы анализа педагогической ситуации, профессиональной рефлексии на основе специальных научных знаний. ОПК-8.2. Проектирует и осуществляет учебно-воспитательный процесс с опорой на знания основных закономерностей возрастного развития когнитивной и личностной сфер обучающихся, научно-

		обоснованных закономерностей организации образовательного процесса, научных основ преподаваемых предметов, их истории и места в мировой культуре и науке. ОПК-8.3. Осуществляет мониторинг и отбор программ профессионального и личностного развития.

в) профессиональные компетенции (ПК) и индикаторы их достижения:

Код и наименование профессиональной компетенции выпускника	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)
Тип задач профессиональной деятельности: педагогический		
ПК-5. Способен определять собственную позицию относительно дискуссионных проблем предметной области (в соответствии с профилем и уровнем обучения)	ПК-5.1. Проявляет мировоззренческую рефлексию при анализе проблем и тенденций в области Математики и Информатики. ПК-5.2. Проявляет способность аргументированно, логические верно и ясно выражать свою позицию по обсуждаемым дискуссионным проблемам в сочетании с готовностью к конструктивному диалогу и толерантному восприятию иных точек зрения. ПК-5.3. Выделяет концептуальную основу дискуссий в области Математики и Информатики, соотносит с нею свои мировоззренческие установки, гражданскую позицию и социальную мотивацию.	01.001 Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель)

3.2. Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения формируемых компетенций

В результате освоения дисциплины обучающийся должен:

Знать:

– современные угрозы, опасности и риски в киберпространстве (УК-8 (индикаторы – 1, 2);
– нормативно-правовые и организационные основы деятельности образовательных организаций (ОПК-1 (индикаторы – 1, 2);
– научные основы преподаваемого предмета, его историю и место в мировой культуре и науке (конкретизируются применительно к изучаемой учебной дисциплине) (ОПК-8 (индикаторы – 1, 2, 3).

Уметь:

– выстраивать алгоритм безопасного поведения в киберпространстве (УК-8 (индикаторы – 1, 2);
– использовать здоровьесберегающие технологии в организации образовательного пространства (УК-8 (индикаторы – 1, 2);
– анализировать и практически использовать нормативно-правовые акты в области образования (ОПК-1 (индикаторы – 1, 2);
– соотносить основные этапы развития предметной области с ее актуальными задачами, методами и концептуальными подходами, тенденциями и перспективами ее современного развития (ОПК-8 (индикаторы – 1, 2, 3);

– работать с математической и технической литературой(ПК-5 (индикаторы – 1, 2, 3).

Владеть:

– приемами организации без-опасной и комфортной образовательной среды (УК-8 (индикаторы – 1, 2);

– способами, методами и приемами поиска, анализа и оценки правовой информации, необходимой для постановки и решения профессиональных задач (ОПК-1 (индикаторы – 1, 2);

– способами решения проблем правового обеспечения профессиональной деятельности в современных условиях (ОПК-1 (индикаторы – 1, 2) ;

– научными основами преподаваемого предмета (конкретизируются применительно к изучаемой учебной дисциплине) (ОПК-8 (индикаторы – 1, 2, 3).

4. Объём и содержание дисциплины

Очная форма обучения

Объём дисциплины составляет 6 зачётных единиц (162 часа)

Контактная работа 64,83 час.

Самостоятельная работа 97,17 час.

Виды учебных занятий и формы промежуточной аттестации	8 сем.		9 сем.	
	Контактная работа с преподавателем	Самостоятельная работа обучающегося	Контактная работа с преподавателем	Самостоятельная работа обучающегося
Лекции	10,5	31,5	13,5	40,5
Практические занятия	12		27	
Групповые консультации перед экзаменом	-	-	1,5	-
Экзамен	-	-	0,33	25,17
Всего	22,5	31,5	42,33	65,67

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и объемом учебных занятий

Очная форма обучения

№ п/п	Раздел (тема) дисциплины	Семестр	Виды учебных занятий, включая самостоятельную работу обучающихся и объем (в часах)				Формы текущего контроля успеваемости Формы промежуточной аттестации
			Занятия лекционного типа	Занятия семинарского типа		Самостоятельная работа обучающегося	
				Лаб.	Пр.		
1.	Основное содержание и	8	6		6	10,5	Тестирование,

	понятийный аппарат проблемной области «информационная безопасность и защита информации»						практическое задание, проектное задание
2.	Законодательные меры защиты информации и государственная деятельность по обеспечению информационной безопасности	8	4,5		6	12	Тестирование, практическое задание, проектное задание
3.	Процедуры управления информационной безопасностью; лицензирование, сертификация и аттестация субъектов и объектов защиты информации	9	5,5		9	15	Тестирование, практическое задание, проектное задание
4.	Административно-организационные способы обеспечения информационной безопасности	9	4		9	15	Тестирование, практическое задание, проектное задание
5.	Технические средства и методы защиты информации	9	4		9	10,5	Тестирование, практическое задание, проектное задание
ИТОГО			24		39	72	Экзамен

4.2. Развернутое описание содержания учебного материала по разделам (темам)

Тема 1. Основное содержание и понятийный аппарат проблемной области «информационная безопасность и защита информации»

Дуализм понятий «информационная безопасность» и «защита информации»; составляющие информационной безопасности; свойства информации, определяющие состояние её защищенности; конфиденциальность, целостность и доступность; актуальные понятия состояний и процессов защиты информации; системный подход в защите информации; входы, выходы и содержание системы защиты информации; комплексный подход к обеспечению информационной безопасности; приоритеты защиты информации.

Тема 2. Законодательные меры защиты информации и государственная деятельность по обеспечению информационной безопасности

Место и роль законодательных мер обеспечения информационной безопасности в интегральном комплексе процедур защиты информации; понятия ограничительных и созидательных законодательных мер обеспечения информационной безопасности; Доктрина информационной безопасности РФ; иерархическая модель построения российского законодательства в области защиты информации; субъекты-источники законодательных документов, их взаимосвязи и иерархия; понятие юридической силы документов; действующее российское законодательство в области защиты информации; Конституция РФ, Федеральные законы, Распоряжения и Указы Президента РФ, Постановления Правительства РФ, Уголовный и Административный кодексы РФ, подзаконные акты, документы уровня

организации; органы государственной власти РФ, осуществляющие деятельность по защите информации; обзор законодательных мер обеспечения информационной безопасности в зарубежных государствах.

Тема 3. Процедуры управления информационной безопасностью; лицензирование, сертификация и аттестация субъектов и объектов защиты информации

Необходимость формирования верификационного комплекса субъектов и объектов защиты информации; составляющие процедуры верификации; законодательная база лицензирования, сертификации и аттестации; лицензирование субъектов процесса обеспечения информационной безопасности; понятия лицензируемой деятельности, соискателя лицензии, лицензиата, лицензионных требований (условий); лицензирующие органы РФ; Государственный Реестр лицензий; процедура лицензирования деятельности по защите информации; государственные контроль и надзор за исполнением лицензионных требований в период действия лицензии; сертификация средств защиты информации; система сертификации как иерархическая структура, её участники и взаимосвязи между ними в процессе сертификации; Сертификат соответствия; Государственный Реестр сертифицированных средств защиты информации; аттестация объектов информатизации по требованиям безопасности информации; система аттестации как иерархическая структура, её участники и взаимосвязи между ними в ходе аттестации; Государственный Реестр органов по аттестации; Аттестат соответствия.

Тема 4. Административно-организационные способы обеспечения информационной безопасности

Правовая и документальная основы административно-организационных мер по обеспечению информационной безопасности; внутренние угрозы информационной безопасности и пути противодействия им с применением административно-организационных мер; должностные обязанности персонала, отвечающего за информационную безопасность организации; разграничение доступа; физическое и логическое препятствование несанкционированному доступу к защищаемым информационным системам и объектам обеспечивающей инфраструктуры.

Тема 5. Технические средства и методы защиты информации

Аппаратные, программные и комплексные средства защиты информации, их возможности, ограничения и перспективы совершенствования; российская и зарубежные классификации технических средств защиты информации; критерии эффективности технических средств и методов обеспечения информационной безопасности; аргументированный выбор оптимальных целесообразных средств защиты информации применительно к конкретной информационной среде / системе; влияние технических средств защиты информации на функционирование информационных систем, проблематика совместимости; технические каналы утечки информации – выявление и противодействие; свободные, условно-бесплатные и коммерческие программные продукты, обеспечивающие информационную безопасность.

5. Образовательные технологии, в том числе перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

В соответствии с требованиями ФГОС ВО по направлению подготовки «Педагогическое образование» в программе данного курса предусмотрено использование в учебном процессе активных форм проведения занятий и организации самостоятельной работы. Поскольку дисциплина ориентирована на формирование знаний, умений и навыков в области освоения информационных технологий, то в процессе её освоения эффективны

такие технологии личностно-ориентированного обучения, как проектная, технология малогрупповой работы. В реализации образовательного процесса взаимно дополняются аудиторные и сетевые внеаудиторные формы образовательного взаимодействия, используются элементы дистанционного педагогического сопровождения учебной деятельности. На аудиторных занятиях развиваются и контролируются результаты, достигаемые обучающимися в индивидуальной и малогрупповой образовательной деятельности и в сетевой среде. Обучение организуется с опорой на электронный УМК и дополнительные информационные ресурсы.

Для выполнения индивидуальных заданий студенты используют электронный каталог библиотеки, электронные ресурсы электронных библиотечных систем «Университетская книга» (Режим доступа: www.biblioclub.ru), ЭБС Шуйского филиала ИвГУ на платформе «Руконт».

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: мультимедиа-технологии; интерактивные информационные технологии.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся при освоении учебной дисциплины «Методы и средства защиты информации» предполагает выполнение тематических исследований, направленных на формирование понимания студентом раскрываемой темы на основании сочетания целенаправленного поиска информации в различных традиционных и онлайн-ресурсах, критического анализа информационного массива и самостоятельных выбора, апробации и изучения аппаратных и/или программных средств, функционал которых задействуется в решении исследуемых задач. Предполагается обязательное исполнение обучающимся 2 тематических исследований и, по желанию студента, – произвольного количества дополнительных исследований, согласуемых обучающимся с преподавателем на основании успешности освоения учебной дисциплины.

Полностью весь методический материал по обеспечению самостоятельной работы студентов приводится в Приложении 1 к настоящей программе. Доступ к методическим материалам осуществляется через сайт Шуйского филиала ИвГУ, в том числе через ЭБС Шуйского филиала ИвГУ на платформе «Руконт».

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине

Использование балльно-рейтинговой системы оценивания достижений позволяет анализировать и своевременно корректировать индивидуальную динамику формирования компетенций бакалавра.

Текущая аттестация осуществляется с использованием накопительного рейтингового оценивания. В качестве оценочных средств для текущего контроля успеваемости используются:

1) отчеты по практическим заданиям (9 работ с трудоёмкостью 2 аудиторных часа по 4 балла, 1 лабораторная работа с трудоёмкостью 6 аудиторных часов 12 баллов, максимально 48 баллов); тематика и содержание лабораторных работ приведены в Приложении 1.
2) тестовые задания (6 тестов по 4 балла, максимально 24 балла);
3) тематические исследования (2 обязательные темы по 6 баллов; дополнительные темы (по желанию студента и по согласованию с преподавателем) по 4 балла, но суммарно не более 8 баллов; всего за обязательные и дополнительные темы максимально 20 баллов);

4) посещаемость занятий студентами (до 8 баллов).

Таким образом, максимальная сумма баллов, достигаемая студентом в ходе обучения в течение семестра, составляет 100 баллов.

Промежуточная аттестация студентов по курсу «Методы и средства защиты информации» предполагает экзамен, который проводится в форме собеседования преподавателя с обучаемым по изученным темам, выбираемым преподавателем на основании анализа успешности освоения учебного материала.

Общая накопительная оценка складывается из баллов текущей успеваемости в семестре по учебной дисциплине и баллов, полученных студентами на экзамене.

Оценка на экзамене выставляется по следующей шкале:

Шкала оценки результатов по дисциплине «Методы и средства защиты информации» при рейтинговой системе оценивания

Повышенный уровень	Базовый уровень	Пороговый уровень	Ниже порогового уровня
отлично	хорошо	удовлетворительно	неудовлетворительно
85-100 баллов	71-84 балла	61-70 баллов	менее 61 балла

8. Учебно-методическое и информационное обеспечение дисциплины

Учебная и учебно-методическая литература:

– ***основная литература:***

1. Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 186 с. : ил., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93356. – Библиогр. в кн. – ISBN 978-5-9765-1271-9. – Текст : электронный.
2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 255 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=276557. – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный.
3. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.

– ***дополнительная литература:***

1. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 257 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428605. – Текст : электронный.
2. Гашков, С. Б. Криптографические методы защиты информации : учебное пособие для студентов вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - Москва : Академия, 2010. - 304 с.
3. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие: [16+] / А. М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный

университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480636. – Библиогр.: с. 213. – Текст : электронный.

4. Информационная безопасность : учебно-методические материалы для проведения практических занятий / А.А. Михайлов, Г.Д. Хубулов .— Шуя : ФГБОУ ВПО "ШГПУ", 2010 .— 60 с. — URL: https://rucont.ru/efd/175338
5. Канивец, Е. К. Информационные технологии в профессиональной деятельности. Курс лекций : учебное пособие / Е. К. Канивец. – Оренбург : Оренбургский государственный университет, 2015. – 108 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=439012. – Библиогр. в кн. – ISBN 978-5-7410-1192-8. – Текст : электронный.
6. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 222 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=458204. – Библиогр.: с. 214-215. – Текст : электронный.
7. Петров, С. В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.
8. Прохорова, О. В. Информационная безопасность и защита информации : учебник : [16+] / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=438331. – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.
9. Расторгуев, С. П. Основы информационной безопасности : учебное пособие для студентов высших учебных заведений / С. П. Расторгуев. - Москва : Академия, 2007. - 192 с.
10. Системы защиты информации в ведущих зарубежных странах : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, М. В. Рудановский, Г. В. Кондрашин ; науч. ред. В. И. Аверченков. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 224 с. : ил., схем. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93351. – Библиогр.: с. 192-193. – ISBN 978-5-9765-1274-0. – Текст : электронный.

Интернет-ресурсы:

1. Обзоры, аналитика, тестирование компьютерных систем и информационной техники www.ixbt.com

2. Компьютерра-Онлайн www.computerra.ru

Современные профессиональные базы данных и информационно-справочные системы:

1. ЭБС «Университетская библиотека онлайн» - http://biblioclub.ru/;
2. Коллекция Шуйского филиала ИвГУ на национальном цифровом ресурсе «Руконт» - https://www.rucont.ru/;
3. Консультант Плюс http://www.consultant.ru/
4. Портал общероссийской системы оценки качества образования. -

http://www.osoko.edu.ru/;

5. Методическое хранилище Ивановского института развития образования.- http://www.iroio.ru/;

6. Словари и энциклопедии на Академике. - https://dic.academic.ru/.

Программное обеспечение:

В процессе изучения дисциплины используются офисные пакеты Microsoft Office, Open Office, программа для просмотра и чтения файлов PDF Adobe Acrobat Reader DC, программа для воспроизведения флэш-анимации в браузерах Adobe Flash Player, вэб-обозреватели GoogleChrome, Opera, Антивирус Касперского, 1С университет, Google-диск: https://drive.google.com; Google-документы: https://docs.google.com.

9. Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного типа, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории.
2. Учебная аудитория для проведения занятий семинарского типа, укомплектованная специализированной мебелью и техническими средствами обучения.
3. Учебная аудитория для проведения групповых и индивидуальных консультаций, укомплектованная специализированной мебелью и техническими средствами обучения.
4. Учебная аудитория для проведения текущего контроля и промежуточной аттестации, укомплектованная специализированной мебелью и техническими средствами обучения.
5. Помещение для самостоятельной работы, оснащенное специализированной мебелью, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.
6. Учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации: презентации, видео-ролики.

Автор рабочей программы дисциплины: В.В. Иванов, доцент кафедры математики, информатики и методики обучения, кандидат технических наук, доцент.

Программа рассмотрена на заседании кафедры математики, информатики и методики обучения «19» февраля 2025 г., протокол № 8

Программа обновлена
протокол заседания кафедры № __от «___» _____ 20__ г.
Согласовано:
Руководитель ОП_____ А.С. Зинченко
(подпись)

Программа обновлена
протокол заседания кафедры № __от «___» _____ 20__ г.
Согласовано:
Руководитель ОП _____ А.С. Зинченко
(подпись)

Программа обновлена
протокол заседания кафедры № __от «___» _____ 20__ г.
Согласовано:
Руководитель ОП _____ А.С. Зинченко
(подпись)

Приложение 1

Методические указания для обучающихся по освоению дисциплины

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Практическая работа №1 «Системы обеспечения безопасности: основные понятия и инструментарий формальных описаний» (2 аудиторных часа)

Контрольные вопросы для изучения:

1) Сходство и различие понятий «информационная безопасность» и «защита информации».

2) Термины «угроза», «атака», «злоумышленник», «источник(и) угроз(ы)», «окно опасности» применительно к проблемной области «информационная безопасность / защита информации».

3) Определения законодательных, морально-этических, организационных, физических и технических мер безопасности.

4) Системный подход в защите информации как эффективный инструмент обеспечения информационной безопасности.

Практические задания:

1) Изучить пример системы безопасности – уличный перекресток

Термин	Содержание
Угроза	поток транспорта, пересекающего наш маршрут
Атака	проезд на красный сигнал светофора
Злоумышленник	водитель-нарушитель
Источники угрозы	все водители на поперечной улице
Окно опасности	период пересечения перекрёстка
Меры безопасности	Содержание
Законодательные	ПДД, Административный кодекс РФ
Морально-этические	культура поведения, "не убий!" и проч.
Организационные	надзор сотрудников ГИБДД, регулировка движения
Физические	шлагбаумы, турникеты, подъемные препятствия
Технические	видеокамеры, интеллектуальные системы контроля трафика

Придумать свой пример системы безопасности и описать его вышеприведенным образом.

2) Рассмотреть систему безопасности, придуманную Вами при выполнении задания №1, в понятиях системного подхода:

а) Что является входами Вашей системы?

б) Что является её наполнением (содержанием)?

в) Каковы выходы вашей системы?

3) Описать 2 примера работы Вашей системы безопасности:

а) Полное предотвращение ущерба.

б) Минимизация ущерба при невозможности его предотвращения.

Представить отчет по выполненным заданиям в виде файла оптимального формата, отправленного на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер лабораторной работы (сквозная нумерация по учебной дисциплине), например: *ФТЭС3-1_ГеоргиевГГ_лаб01*

Практическая работа №2 «Российское законодательство в области информационной безопасности» (2 аудиторных часа)

Контрольные вопросы для изучения:

1) Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2018).

2) Доктрина информационной безопасности РФ (редакция 2016 г.).

Целесообразно использовать правовую online-систему «Консультант» www.consultant.ru

Практические задания:

1) В статье 2 Федерального закона 149-ФЗ определить терминологический аппарат данного закона и выделить подмножество понятий, имеющих отношение к защите информации.

2) В статье 3 Федерального закона 149-ФЗ выделить принципы правового регулирования отношений в области информационной безопасности.

3) В статье 16 Федерального закона 149-ФЗ найти ответы на вопросы:

а) В РФ разрешено применять любые средства защиты информации?

б) Кто и как может запретить нам защищать свою информацию так, как нам этого хочется?

в) Какие неправомерные действия призвана блокировать защита информации?

г) Где должны находиться базы данных со сведениями о россиянах?

д) Для каких целей защищается общедоступная (публичная) информация? или же такая информация не нуждается в защите?

е) Кто несёт ответственность за своевременное обнаружение несанкционированного доступа к защищаемой информации?

ж) А кто отвечает за защиту государственных информационных систем?

4) На основании изучения изменений и дополнений к Федеральному закону 149-ФЗ сформируйте свое мнение о тенденциях изменения ФЗ-149 в текущем году:

а) Закон стал менее или более эффективным? в чём конкретно?

б) Больше свободы или больше порядка?

в) Кто «главнее»" - граждане или государство? бизнес или политика?

5) Изучите Доктрину информационной безопасности РФ и оцените её влияние на информационные процессы:

а) Деятельность российских государственных органов по конкретной реализации положений Доктрины (принятие законов, подзаконных актов, программ, организация новых структур, кадровые назначения и проч.).

б) Реакция СМИ и бизнес-сообщества (положительные или отрицательные оценки Доктрины, желание или, наоборот, нежелание участвовать в её реализации).

Представить отчет по выполненным заданиям в виде файла оптимального формата, отправленного на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер лабораторной работы (сквозная нумерация по учебной дисциплине), например: *ФТЭС3-1_ГеоргиевГГ_лаб01*

Практическая работа №3 «Государственные органы Российской Федерации, в компетенции которых входят защита информации и обеспечение информационной безопасности» (2 аудиторных часа)

Контрольные вопросы для изучения:

1) Комитет Государственной думы по безопасности и противодействию коррупции.

2) Совет безопасности России (СБ России).

3) Служба внешней разведки Российской Федерации (СВР России).

4) Министерство обороны Российской Федерации (Минобороны России).

5) Министерство внутренних дел Российской Федерации (МВД России).
6) Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор РФ).
7) Федеральная служба безопасности (ФСБ России).
8) Федеральная служба по техническому и экспортному контролю (ФСТЭК России).
Практические задания:
1) Для каждой вышеназванной организации определить:
а) Дата создания.
б) Вышестоящий государственный орган и/или должностное лицо.
в) Действующий руководитель.
г) Количество сотрудников (ориентировочно).
д) Годовой бюджет.
е) Официальный сайт.
ж) Декларируемые задачи в области защиты информации.
з) Конкретные действия в области защиты информации в последние годы (2...3 действия)
2) Для ФСБ и ФСТЭК дополнительно определить:
и) Предшествующие организации, функции которых в настоящее время исполняет действующая служба.
к) Создание действующей службы - документ о создании (вид, №, дата).
л) Документ, регулирующий деятельность службы (Положение, Устав и проч.).
м) Научно-исследовательские структуры в области защиты информации, подчиненные службе.
Представить отчет по выполненным заданиям в виде файла оптимального формата, отправленного на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер лабораторной работы (сквозная нумерация по учебной дисциплине), например: *ФТЭС3-1_ГеоргиевГГ_лаб01*

Практическая работа №4 «Лицензирование деятельности по защите информации» (2 аудиторных часа)
Контрольные вопросы для изучения:
1) Основные понятия: лицензия, лицензируемые виды деятельности, соискатель лицензии, лицензиат.
2) Законодательная основа лицензирования в современной России.
3) Лицензионные требования и условия применительно к видам деятельности по обеспечению информационной безопасности.
4) Лицензирующие органы, процедуры их взаимодействия с соискателями лицензий и лицензиатами; нормативные сроки; реестр лицензий.
Практические задания:
1) Составить перечень видов деятельности, требующих для исполнения лицензии по современному законодательству РФ (5…7 направлений).
2) Определить, какие органы исполнительной власти выдают лицензии на право осуществления образовательной деятельности? а какие – на право владения огнестрельным оружием?
3) Разработать план-график действий для гипотетической организации – соискателя лицензии на осуществление одного из видов лицензируемой деятельности в области защиты информации. Сопоставить ориентировочные затраты денежных и материальных ресурсов, продолжительность и кадровое обеспечение отдельных этапов лицензирования.
Представить отчет по выполненным заданиям в виде файла оптимального формата,

отправленного на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер лабораторной работы (сквозная нумерация по учебной дисциплине), например: *ФТЭС3-1_ГеоргиевГГ_лаб01*

Практическая работа №5 «Сертификация средств защиты информации» (2 аудиторных часа)

Контрольные вопросы для изучения:

1) Основные понятия: сертификация, сертификат соответствия, система сертификации (сертифицирующих органов).
2) Законодательная основа осуществления сертификации средств защиты информации в современной России.
3) Федеральные органы сертификации, профильные органы сертификации, испытательные лаборатории, разработчики / производители / продавцы – процедуры их взаимодействия и нормативные сроки отдельных этапов сертификации.
4) Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00.

Практические задания:

1) Изучить ознакомительный материал «Примерный перечень действий по сертификации средств защиты информации», представленный в Приложении 3.
2) Подготовить FAQ по сертификации на основании изученного материала, включающий развёрнутые и адаптированные ответы на следующие вопросы:
а) Кто выступает инициатором сертификации?
б) Может ли сертификация проводится в плановом порядке (по заранее утвержденному графику)?
в) Куда направляется Заявка на проведение сертификации?
г) Может ли Заявитель выбирать исполнителя сертификационных испытаний?
д) Кто оплачивает расходы на проведение сертификации?
е) Каков максимальный срок получения Решения по Заявке на сертификацию?
ж) Кому направляются экземпляры Решения?
з) Что входит в комплект документов при заключении Договора между Заявителем и Испытательной Лабораторией?
и) На основании чего Испытательная лаборатория устанавливает стоимость сертификационных испытаний?
к) Кто составляет программу сертификационных испытаний?
л) Кто настраивает оборудование (например, испытательный стенд) для сертификационных испытаний?
м) Может ли Заявитель оперативно (в ходе испытаний) вносить улучшения в конструкцию и/или комплектацию сертифицируемой продукции?
н) Какие документы составляются по результатам сертификационных испытаний?
о) Кому направляются результаты испытаний?
п) Кто исполняет экспертизу результатов испытаний и какие документы появляются «на выходе» этого процесса?
р) Кто принимает решение о выдаче сертификата соответствия?
3) Изучить Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (доступен на официальном сайте ФСТЭК) и определить:
а) Сколько всего сертификатов внесено в Госреестр в настоящее время?
б) Когда были выданы первый и последний (на данный момент) сертификаты? какие объекты были сертифицированы первым и последним?

в) Какие антивирусные средства сертифицированы? отдаётся ли предпочтение какому-то конкретному разработчику антивирусов?
г) Какие продукты корпорации Microsoft получили сертификаты?
д) Какая из испытательных лабораторий является чемпионом по количеству обследованных объектов сертификации?
Представить отчет по выполненным заданиям в виде файла оптимального формата, отправленного на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер лабораторной работы (сквозная нумерация по учебной дисциплине), например: *ФТЭС3-1_ГеоргиевГГ_лаб01*

Практическая работа №6 «Аттестация объектов информатизации» (2 аудиторных часа)
Контрольные вопросы для изучения:
1) Основные понятия: аттестация, аттестат соответствия, система аттестации (органов по аттестации).
2) Законодательная основа осуществления аттестации объектов информатизации в современной России.
3) Федеральные органы аттестации, профильные органы сертификации, испытательные центры / лаборатории, заявители – процедуры их взаимодействия и нормативные сроки отдельных этапов аттестации.
4) Государственный реестр «Перечень органов по аттестации N РОСС RU.0001.01БИ00»
Практические задания:
1) Изучить Госреестр «Перечень органов по аттестации N РОСС RU.0001.01БИ00» (доступен на официальном сайте ФСТЭК) и определить:
а) В каких организационно-правовых формах представлены органы по аттестации?
б) Есть ли среди органов по аттестации высшие учебные заведения? Если есть - приведите несколько примеров.
в) Какая организация получила аттестат первой? а какая - последней (на данный момент)?
г) Какая организация имеет аттестат наиболее продолжительный срок?
д) Есть ли действующие орган(ы) по аттестации в Ивановской области? Если есть, то сколько их? Если нет, то где находятся ближайшие органы в соседних регионах?
2) Разработать план-график действий для гипотетической организации-разработчика информационной системы (информационного объекта), подлежащих аттестации перед вводом в эксплуатацию / началом продаж. Сопоставить ориентировочные затраты денежных и материальных ресурсов, продолжительность и кадровое обеспечение отдельных этапов аттестации.
Представить отчет по выполненным заданиям в виде файла оптимального формата, отправленного на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер лабораторной работы (сквозная нумерация по учебной дисциплине), например: *ФТЭС3-1_ГеоргиевГГ_лаб01*

Практическая работа №7 «Административно-организационные способы обеспечения информационной безопасности» (2 аудиторных часа)
Контрольные вопросы для изучения:
1) Правовая и документальная основы административно-организационных мер по обеспечению информационной безопасности.
2) Внутренние угрозы информационной безопасности и пути противодействия им с применением административно-организационных мер.
3) Должностные обязанности персонала, отвечающего за информационную безопасность

организации.
4) Физическое и логическое препятствование несанкционированному доступу к защищаемым информационным системам и объектам обеспечивающей инфраструктуры.
Практические задания:
1) Разработать раздел должностной инструкции, посвященный защите информации, для сотрудника организации по профилю профессиональной подготовки обучающегося, ответственного за обеспечение информационной безопасности (например, будущие педагоги могут разработать инструкцию для заместителя директора учебного заведения по информатизации или преподавателя информатики, исполняющего функции системного администратора).
2) Разработать систему мер для препятствования несанкционированному доступу к некоторому помещению (например, расположенному в вузе или в произвольной организации по выбору обучающегося), условно считаемому значимым объектом информационной защиты.
Представить отчет по выполненным заданиям в виде файла оптимального формата, отправленного на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер лабораторной работы (сквозная нумерация по учебной дисциплине), например: *ФТЭС3-1_ГеоргиевГГ_лаб01*

Практическая работа №8 «Интерфейс командной строки для управления компьютерной системой» (2 аудиторных часа)
Контрольные вопросы для изучения:
1) Основные понятия организации файловой системы хранения информации.
2) Интерфейсы управления компьютерной системой.
3) Преимущества интерфейса командной строки как эффективного средства тонкой настройки и администрирования компьютерной системы; применение командной строки в условиях недоступности GUI.
Практические задания:
ВНИМАНИЕ: иллюстрационный материал данной лабораторной работы (преимущественно screenshots) может потребоваться в основном при возникновении затруднений у невнимательных или недостаточно подготовленных студентов, поэтому, что бы не загромождать логическое описание работы, указанные иллюстрации вынесены в Приложение 3, а в тексте работы указаны лишь отсылки к соответствующим пронумерованным рисункам. Описание работы содержит *минимальный пояснительный материал, выделенный курсивом*.
1) *В операционных системах семейства Windows набираемые с клавиатуры и сразу же выполняемые команды исполняются с помощью так называемого командного интерпретатора, иначе именуемого «командным процессором» или «оболочкой командной строки» (command shell). Таким образом, оболочка командной строки – это отдельный программный продукт, который обеспечивает прямую связь между пользователем и операционной системой (ОС). Текстовый пользовательский интерфейс командной строки предоставляет среду, в которой выполняются приложения и служебные программы с текстовым интерфейсом. В ОС Windows 9.x командный интерпретатор был представлен исполняемых файлом command.com (как и в ОС MS-DOS). Начиная с Windows NT, он реализован в программе cmd.exe и обладает существенно бОльшими возможностями. В Windows XP+ файл cmd.exe, находятся в папке SYSTEM32. Некоторые команды распознаются и выполняются непосредственно самим командным интерпретатором – такие команды называются внутренними (например, copy и dir); другие команды ОС*

представляют собой отдельные программы, расположенные по умолчанию в том же каталоге, что и cmd.exe, которые Windows загружает и выполняет аналогично другим программам – такие команды называются внешними (например, more и xcopy).
Для полной реализации возможностей командной строки запустите её ОТ ИМЕНИ АДМИНИСТРАТОРА (рис.1). В результате откроется новое окно, в котором можно будет запускать команды и видеть результаты их работы (рис.2).
2) *Для того чтобы выполнить команду введите имя этой команды (регистр не важен), ее параметры и ключи (если они необходимы) и нажмите клавишу <Enter>.*
Создайте на диске C: файл test.txt и папку Textfiles
В командной строке наберите:
copy C:\test.txt C:\Textfiles /V
...и нажмите клавишу <Enter> (рис.3).
Имя команды здесь – copy, параметры – C:\test.txt и C:\Textfiles, а ключом является /V. Отметим, что в некоторых командах ключи могут начинаться не с символа /, а с символа - (минус), например, -V. Следует обратить внимание, что если в имени папки есть пробел, то в команде его быть не должно, как в указанном примере или же имя папки должно быть заключено в кавычки, например, "C:\Program Files"
3) *Многие команды ОС Windows имеют большое количество дополнительных параметров и ключей, и запомнить их все невозможно или по крайней мере очень трудно. Большинство команд снабжено встроенной справкой, в которой кратко описываются назначение и синтаксис данной команды. Получить доступ к такой справке можно путем ввода команды с ключом /?*
В командной строке наберите:
copy /?
...и нажмите клавишу <Enter> (рис.4).
В командной строке наберите:
ping /?
...и нажмите клавишу <Enter> (рис.5).
Команда help выводит список основных команд командной строки.
В командной строке наберите:
help
...и нажмите клавишу <Enter> (рис.6).
4) *С помощью переназначения устройств ввода/вывода одна программа может направить свой вывод на вход другой или перехватить вывод другой программы, используя его в качестве своих входных данных. Таким образом, имеется возможность передавать информацию от процесса к процессу при минимальных программных издержках. Практически это означает, что для программ, которые используют стандартные входные и выходные устройства, ОС позволяет: выводить сообщения программ не на экран, а в файл; читать входные данные не с клавиатуры , а из заранее подготовленного файла; передавать сообщения, выводимые одной программой, в качестве входных данных для другой программы и т.д. Выходные данные практически всех команд высвечиваются в окне командной строки. Даже команды, выводящие данные на диск или принтер, выдают сообщения и запросы в окне командной строки. Для перенаправления вывода команд из окна командной строки в файл или на устройство применяется оператор « > ». Этот оператор может использоваться с большинством команд.*
Для перенаправления вывода команды dir в файл test.txt введите в командной строке:
dir>C:\test.txt
...и нажмите клавишу <Enter> (рис.7).

Если указанный файл не существует, интерпретатор команд cmd.exe создаст его. Если файл существует, cmd.exe заменит информацию в файле на данные, полученные от команды dir.

Откройте файл test.txt для просмотра (например, с помощью стандартной программы Блокнот) – в нём будет содержаться результат работы команды dir (рис.8).

Следует отметить, что информация, которая была в файле до этого, будет стерта. Для того чтобы выходные файлы команды добавлялись в конец файла, необходимо использовать символы « >> », а не « > » в синтаксисе команды.

Местоположение потоков ввода и вывода называется дескриптор.

В табл.1 представлены операторы перенаправления потоков ввода и вывода команд.

Таблица 1

Оператор перенаправления	Описание
>	Записывает данные на выходе команды вместо командной строки в файл или на устройство, например, на принтер.
<	Читает поток входных данных команды из файла, а не с клавиатуры.
>>	Добавляет выходные данные команды в конец файла, не удаляя при этом существующей информации из файла.
>&	Считывает данные на выходе одного дескриптора как входные данные для другого дескриптора.
<&	Считывает входные данные одного дескриптора как выходные данные другого дескриптора.
|	Считывает выходные данные одной команды и направляет их на вход другой команды. Эта процедура обычно называется «канал».

С помощью символа « < » можно прочитать входные данные для заданной команды не с клавиатуры, а из определенного (заранее подготовленного) файла.

На диске C: создайте файл data.txt и напишите в нем: 25.12.2011

В командной строке наберите:

Date<C:\data.txt

...и нажмите клавишу <Enter> (рис.9).

Проверьте дату на вашем компьютере – она изменилась на 25 декабря 2011 года. Не забудьте вернуть актуальную дату САМОСТОЯТЕЛЬНО!

5) *Команда more выводит содержимое файла или вывода команды по 1 экрану за 1 раз.*

Например, чтобы отобразить содержимое файла test.txt поэкранно, введите следующую команду:

more C:\test.txt

...и нажмите клавишу <Enter> (рис.10).

Если файл большой, то отображается одно окно командной строки со сведениями, а затем в нижней части окна командной строки отображается строка -- More --. Для остановки просмотра следует ввести комбинацию CTRL+C. Команда more полезна при работе с командами, создающими выход более одного окна командной строки. Например, при выводе дерева каталогов жесткого диска.

6) *Другой распространенной командой фильтрации является sort – она выполняет сортировку по алфавиту текстового файла или выхода команды.*

Отредактируйте файл data.txt, добавив туда две другие даты, например, 20.12.2011 и 7.12.2011. В командной строке наберите:

sort< C:\data.txt
...и нажмите клавишу <Enter> (рис.11).
Ключ /R позволяет изменить порядок сортировки на обратный.
sort /r < C:\date.txt
...и нажмите клавишу <Enter> (рис.12).
Представить конспект выполненных заданий (команды и результаты их работы, ваши комментарии и замечания, возможные отклонения в ходе исполнения лабораторной работы, вызванные, например, различиями в конкретных версиях ОС) в виде файла оптимального формата, отправленного на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер лабораторной работы (сквозная нумерация по учебной дисциплине), например: *ФТЭС3-1_ГеоргиевГГ_лаб01*

Практическая работа №9 «Анализ сетевой активности с помощью интерфейса командной строки» (2 аудиторных часа)
Контрольные вопросы для изучения:
1) Вредоносное программное обеспечение.
2) Характеристики работы компьютерных сетей; понятие «сетевой порт»; TCP- и UDP-порты.
Практические задания:
ВНИМАНИЕ: иллюстрационный материал данной лабораторной работы (преимущественно screenshots) может потребоваться в основном при возникновении затруднений у невнимательных или недостаточно подготовленных студентов, поэтому, что бы не загромождать логическое описание работы, указанные иллюстрации вынесены в Приложение 3, а в тексте работы указаны лишь отсылки к соответствующим пронумерованным рисункам. Описание работы содержит *минимальный пояснительный материал, выделенный курсивом*.
1) *Одним из проявлений наличия вредоносной программы обычно является возросшая сетевая активность (в том числе сетевой информационный трафик). Вредоносная программа может отправлять письма от имени пользователя компьютера, загружать информацию из Интернета, передавать кому-то по сети конфиденциальные данные и т.п. При этом необходимо помнить, что легальные приложения также могут использовать Интернет без действий пользователя – например, антивирусная программа может загружать обновления антивирусной базы данных.*
Для получения полной информации о сетевой активности можно использовать команду netstat, которая выводит на экран мгновенную статистику сетевых соединений.
В командной строке наберите:
netstat /?
...и нажмите клавишу <Enter> (рис.1).
Прочитайте описание netstat.
2) Убедитесь, что для вывода наиболее полной информации нужно использовать netstat с ключом –A, для этого в командной строке наберите:
netstat /A
...и нажмите клавишу <Enter> (рис.2).
Результатом выполнения команды является список активных подключений, в который входят установленные соединения и открытые порты.
TCP-порты обозначаются строкой "TCP" в колонке Имя. Открытые TCP-порты обозначаются строкой "LISTENING" в колонке состояние. Часть портов связана с системными службами

Windows и отображается не по номеру, а по названию - epmap, microsoft-ds, netbios-ssn. Порты, не относящиеся к стандартным службам, отображаются по номерам.
UDP-порты обозначаются строкой "UDP" в колонке Имя. Они не могут находиться в разных состояниях, поэтому специальная пометка "LISTENING" в их отношении не используется. Как и TCP-порты они могут отображаться по именам или по номерам.
Порты, используемые вредоносными программами, чаще всего являются нестандартными и поэтому отображаются согласно их номерам. Впрочем, могут встречаться троянские программы, использующие для маскировки стандартные для других приложений порты, например 80, 21, 443 – порты, используемые на файловых и web-серверах.
Команда netstat, в отличие от Диспетчера задач Windows, не работает в режиме реального времени, а отображает мгновенную статистику. Следовательно, для просмотра активности соединений, скажем, через минуту, нужно заново выполнить команду.
3) Изучите команду ping и проверьте с её помощью соединение с сайтами «Яндекс» и «Google».
Представить конспект выполненных заданий (команды и результаты их работы, ваши комментарии и замечания, возможные отклонения в ходе исполнения лабораторной работы, вызванные, например, различиями в конкретных версиях ОС) в виде файла оптимального формата, отправленного на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер лабораторной работы (сквозная нумерация по учебной дисциплине), например: *ФТЭС3-1_ГеоргиевГГ_лаб01*

Практическая работа №10 «Выявление технических каналов утечки информации (ТКУИ) для объекта информатизации путем моделирования возможных действий технических разведок» (6 аудиторных часов)
Контрольные вопросы для изучения:
1) Угрозы информационной безопасности.
2) Технические каналы утечки информации – выявление и противодействие.
Практические задания:
1) Изучить ознакомительный материал для данной лабораторной работы, представленный в Приложении 3.
2) Разработать систему мер для выявления и противодействия ТКУИ в некотором помещении (например, расположенном в вузе или в произвольной организации по выбору обучающегося), условно считаемому значимым объектом информационной защиты.
а) Начертить (в электронном виде => графический файл) схему защищаемого помещения согласно образцу в ознакомительном материале. Обозначить стены, основные предметы мебели, оргтехнику, системы кондиционирования / вентиляции (если есть), окна, двери и проч.
б) Составить текстовое описание защищаемого помещения по образцу в ознакомительном материале.
в) Проанализировать защищенность рассматриваемого помещения с различных направлений и по разным видам уязвимостей (см. пример в ознакомительном материале).
г) Доказать целесообразность и предложить проведение тех или иных защитных мероприятий.
Представить отчет по выполненным заданиям в виде файла оптимального формата, отправленного на адрес электронной почты преподавателя; наименование файла должно содержать обозначение учебной группы, ФИО исполнителя и номер лабораторной работы (сквозная нумерация по учебной дисциплине), например: *ФТЭС3-1_ГеоргиевГГ_лаб01*

ТЕМАТИЧЕСКИЕ ИССЛЕДОВАНИЯ

Тематические исследования (обязательные к выполнению – 2 исследования), максимальная оценка 6 баллов за каждое исследование. Тематические исследования (дополнительные – выполняемые студентом по согласованию с преподавателем), максимальная оценка 4 балла за 1 исследование.

Задание:

Выполнить тематическое исследование по контролируемой теме и представить преподавателю отчёт-эссе.

Тематические исследования являются формой самостоятельной работы обучающихся при освоении учебной дисциплины «Методы и средства защиты информации» и направлены на формирование понимания студентами раскрываемой темы на основании сочетания целенаправленного поиска информации в различных традиционных и онлайн-ресурсах, критического анализа информационного массива и самостоятельных выбора, апробации и изучения аппаратных и/или программных средств, функционал которых задействуется в решении исследуемых задач. Предполагается обязательное исполнение обучающимся 2 тематических исследований и, по желанию студента, – произвольного количества дополнительных исследований, согласуемых обучающимся с преподавателем на основании успешности освоения им учебной дисциплины. Результатом исследования является отчёт-эссе в свободной форме, раскрывающий проделанную работу и представляющий самостоятельные выводы обучающегося.

Темы №№1 и 2 являются обязательными и должны быть исполнены каждым обучающимся; остальные темы являются дополнительными и исполняются по желанию обучающегося и по согласованию с преподавателем.

1. Формирование системы информационной безопасности критической инфраструктуры в современном российском государстве.
2. Аргументированный выбор свободного программного средства для обнаружения и удаления вредоносного программного обеспечения
3. Законодательные меры защиты информации и государственная деятельность *конкретного государства* в области обеспечения информационной безопасности.

Методические указания к выполнению темы №3:

Выбрать *государство* из нижеприведенного списка:

а) Великобритания	б) Франция	в) Германия	г) Китай
д) Южная Корея	е) Украина	ж) Беларусь	з) Казахстан
и) Финляндия	к) Швеция	л) Турция	м) Израиль
н) Италия	о) Чехия	п) Мексика	р) Канада
с) Бразилия	т) Австралия	у) Япония	ф) Индия

Примерный план исследования:

1) Федеральные (общегосударственные) органы, обеспечивающие защиту информации (министерства, комитеты, департаменты, институты, агентства и т.д.); если доступно – ресурсы этих органов (например, число работающих, годовой бюджет)
2) Какой орган из п.1 обеспечивает техническую защиту информации?
3) Есть ли частные коммерческие организации, работающие в сфере защиты государственной информации? Имеют ли они выход на мировой рынок или ограничены внутригосударственным сбытом своей продукции / услуг?
4) Основные действующие законы по обеспечению информационной безопасности
5) Строгость наказаний за нарушение информационной безопасности. Например, караются ли по закону следующие виды деятельности: написание компьютерных вирусов, «взлом»

коммерческого программного обеспечения, несанкционированный доступ к информации платежных систем?
4. Свободные и условно-бесплатные программные инструменты для оценки уязвимостей WiFi-сети (сравнительный обзор).
5. Организация эффективной и безопасной многопользовательской работы на учебных компьютерах.
6. Программные средства для восстановления информации на магнитных дисках, файловая система которых повреждена в результате целенаправленного деструктивного воздействия (сравнительный обзор).
7. Программные средства для поддержания оптимальной рабочей среды пользователя и противодействия попыткам её искажения.
8. Оптимизирующая настройка встроенных средств безопасности операционных систем семейства Windows.
9. Оптимизирующая настройка встроенных средств безопасности операционных систем семейства Android.
10. «Гражданские» общедоступные средства шифрования конфиденциальной информации.
11. Свободные и условно-бесплатные средства верификации подлинности контента.
12. Компьютеризированные средства выявления технических каналов утечки информации.

Критерии оценки

Оценки в баллах	Критерии
4	Правильное выполнение задания в полном объеме
½	Аккуратность и грамотность в оформлении результатов
1½	Целесообразная оригинальность, дополнительные соображения и т.п.
6	Максимальная оценка

Критерии оценки дополнительного исследования

Оценки в баллах	Критерии
2	Правильное выполнение задания в полном объеме
½	Аккуратность и грамотность в оформлении результатов
1½	Целесообразная оригинальность, дополнительные соображения и т.п.
4	Максимальная оценка

ТЕСТОВЫЕ ЗАДАНИЯ

Тестовое задание (всего 6 тестов), максимальная оценка 4 балла за 1 тестовое задание.
Задание:
Ответить на вопросы теста.
Каждая изучаемая тема тестируется с использованием массива тестов, включающего ряд «элементарных» тестов, раскрывающих конкретные подтемы (subjects) и представленных в 2 и более вариантах. Выбор subject выполняется либо случайным образом, либо по предпочтению преподавателя с учетом учебной траектории студента.

Критерии оценки

Оценка в баллах	Критерии
0	до 40% правильных ответов

Оценка в баллах	Критерии
1	40…59% правильных ответов
2	60…79% правильных ответов
3	80…99% правильных ответов
4	все ответы правильные

Примерное тестовое задание:

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ // ТЕСТ 3

Вариант А Фамилия И.О. _____
(печатными буквами, разборчиво)

1-А. Общепринятая классификация угроз информационной безопасности включает следующие классы угроз:
Выберите 1 или несколько правильных ответов

- ❑ естественные и искусственные угрозы
- ❑ угрозы без ущерба для информационной системы / с приемлемым ущербом / с неприемлемым ущербом
- ❑ преднамеренные и случайные угрозы
- ❑ угрозы нарушения одного из свойств информационных ресурсов (*конфиденциальности, доступности, целостности*)
- ❑ локальные и сетевые угрозы
- ❑ внутренние и внешние угрозы

2-А. Документами ФСТЭК установлены группы и классы автоматизированных (информационных) систем, отличающихся по уровню защищенности.
Выберите 1 правильное утверждение

- ❑ 3 группы, 7 классов, защищенность нарастает от 1-го к 7-му классу
- ❑ 2 группы, в каждой по 5 классов, защищенность убывает от 1-й ко 2-й группе
- ❑ 3 группы, в каждой по 3 класса, защищенность 1-й группы самая высокая
- ❑ 3 группы, всего 9 классов, защищенность 3-й группы - наименьшая

3-А. Автоматизированные (информационные) системы 2-й группы уровня защищенности имеют следующие характеристики:
Выберите 1 или несколько правильных ответов

- ❑ в системе работает только 1 пользователь, его права максимальны
- ❑ работают несколько пользователей с разными правами
- ❑ работают несколько пользователей с равными правами
- ❑ в системе используются виды памяти (информационные носители) только с равными уровнями конфиденциальности
- ❑ в системе могут использоваться носители с различными уровнями конфиденциальности

4-А. Кто устанавливает права доступа к информационным объектам при дискреционном принципе разграничения доступа?
Выберите 1 или несколько правильных ответов

- ❑ владелец объекта
- ❑ системный администратор
- ❑ "суперпользователь"
- ❑ здесь правильных ответов нет

5-А. Что означает правило *«не читать выше»* при мандатном принципе разграничения доступа?
Выберите 1 правильный ответ

- ❑ пользователь не может получить доступ на чтение информации из объекта, уровень секретности которого выше его (пользователя) уровня доступа
- ❑ пользователь имеет право читать информационный ресурс только однократно, не возвращаясь к уже прочитанной информации
- ❑ владелец информационного объекта не может читать объекты, расположенные в информационной иерархии выше данного объекта (объекты-"родители")
- ❑ здесь правильных ответов нет

«_____»_____ 201___г. Ваша подпись: _____

Ключ для примерного тестового задания:

1-А. Общепринятая классификация угроз информационной безопасности включает следующие классы угроз:
Выберите 1 или несколько правильных ответов

- ❑ естественные и искусственные угрозы
- ❑ ~~угрозы без ущерба для информационной системы / с приемлемым ущербом / с неприемлемым ущербом~~
- ❑ преднамеренные и случайные угрозы
- ❑ угрозы нарушения одного из свойств информационных ресурсов (конфиденциальности, доступности, целостности)
- ❑ ~~угрозы зашифрованные / метаморфные / полиморфные~~

2-А. Документами ФСТЭК установлены группы и классы автоматизированных (информационных) систем, отличающихся по уровню защищенности.
Выберите 1 правильное утверждение

- ❑ ~~3 группы, 7 классов, защищенность нарастает от 1-го к 7-му классу~~
- ❑ ~~2 группы, в каждой по 5 классов, защищенность убывает от 1-й ко 2-й группе~~
- ❑ ~~3 группы, в каждой по 3 класса, защищенность 1-й группы самая высокая~~
- ❑ 3 группы, всего 9 классов, защищенность 3-й группы - наименьшая

3-А. Информационные системы 2-й группы уровня защищенности имеют следующие характеристики:
Выберите 1 или несколько правильных ответов

- ❑ ~~в системе работает только 1 пользователь, его права максимальны~~
- ❑ ~~работают несколько пользователей с разными правами~~
- ❑ работают несколько пользователей с равными правами
- ❑ ~~в системе используются виды памяти (информационные носители) только с равными уровнями конфиденциальности~~
- ❑ в системе могут использоваться носители с различными уровнями конфиденциальности

4-А. Кто устанавливает права доступа к информационным объектам при дискреционном принципе разграничения доступа?
Выберите 1 или несколько правильных ответов

- ❑ владелец объекта
- ❑ ~~системный администратор~~
- ❑ "суперпользователь"
- ❑ ~~здесь правильных ответов нет~~

5-А. Что означает правило "не читать выше" при мандатном принципе разграничения доступа?
Выберите 1 правильный ответ

- ❑ пользователь не может получить доступ на чтение информации из объекта, уровень секретности которого выше его (пользователя) уровня доступа
- ❑ ~~пользователь имеет право читать информационный ресурс только однократно, не возвращаясь к уже прочитанной информации~~
- ❑ ~~владелец информационного объекта не может читать объекты, расположенные в информационной иерархии выше данного объекта (объекты "родители")~~
- ❑ ~~здесь правильных ответов нет~~

МАТЕРИАЛЫ ДЛЯ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ ЗАДАНИЙ

Примерный перечень действий по сертификации средств защиты информации

1. Подача заявки на сертификацию во ФСТЭК России.

В заявке указываются:

- наименования заявителя
- адрес заявителя
- наименование продукции, которую Заявитель хочет сертифицировать
- перечень нормативных и методических документов, на соответствие требованиям которых заявителю необходимо сертифицировать свою продукцию.
- схема сертификации (единичный образец продукции или серийное производство)
- испытательная лаборатория, в которой Заявитель хотел бы провести испытания
- дополнительные условия или требования

Заявитель указывает в заявке, что он обязуется:

- выполнять все условия сертификации;
- обеспечивать стабильность сертифицированных характеристик продукции, маркированной знаком соответствия;
- оплатить все расходы по проведению сертификации.

Важно: заявитель должен иметь лицензию ФСТЭК на соответствующий вид деятельности!

ПРИМЕР заявки на сертификацию программного комплекса:

ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

«Центр Информационных технологий
« ХХХ »

111111, Москва, Ивановское шоссе 10
тел/факс 333-33-33

ИНН XXXXXXX, КПП XXXXXX
Р/счет № XXXXXXXXXXXX
в Курском отделении № XXXX/XX, СБ РФ г. Москва
К/с XXXXXXXXXXXXXXX, БИК XXXXXX

_____ № _____
На № _____от_____

Заместителю
Директора Федеральной службы по
техническому и экспортному контролю
XXXXX X.X.

103175, г. Москва, ул. Старая Басманная, 17

ЗАЯВКА
на проведение сертификации продукции
в системе сертификации средств защиты информации
по требованиям безопасности информации
№ РОСС RU. 0001. 01БИ00

1. Закрытое акционерное общество «Центр Информационных технологий «ХХХ» (ЗАО «ХХХ»), адрес: 111111, г. Москва, Ивановское шоссе, д. 10, просит провести сертификацию следующей продукции:

«Программный комплекс «XXXX», XXXXXXXX
(наименование продукции, код ОКП, шифр)

по требованиям безопасности информации на соответствие:
- требованиям технических условий XXXXXXXXXXX;
- требованиям руководящего документа «Защита от несанкционированного доступа к информации» Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. По 2 уровню контроля.

2. Заявитель предлагает провести испытания изделия по схеме:
сертификация единичного образца в испытательной лаборатории Санкт-Петербургского научно-технического центра ФГУП «Научно-производственное предприятие «Гамма» (197110 г. Санкт-Петербург, ул. Пионерская, д. 44, тел. (812) 235-55-18).

3. Заявитель обязуется:
- выполнять все условия сертификации;
- обеспечивать стабильность сертифицированных характеристик средств защиты информации, маркированных знаком соответствия;
- оплатить все расходы по проведению сертификации.

Генеральный директор /Иванов И.И./

место гербовой печати
«___» _____ 2008 г.

2. Решение на проведение сертификационных испытаний

ФСТЭК в течение месяца после получения заявки направляет Заявителю, назначенным органу по сертификации и испытательной лаборатории решение на проведение сертификационных испытаний, которое содержит следующее:

- наименование Заявителя, адрес Заявителя;
- наименование сертифицируемой продукции, код ОКП, ТУ;
- схема проведения сертификации (испытания единичного образца продукции / партии из

N образцов / образца продукции для серийного производства);

- назначенная испытательная лаборатория и ее адрес;
- перечень нормативных и методических документов, на соответствие требованиям которых должна проводиться сертификация;
- испытательная лаборатория, назначенная для проведения последующего инспекционного контроля;
- орган по сертификации, назначенный для проведения экспертизы результатов сертификационных испытаний;
- способ оплаты работ.

Орган по сертификации и испытательная лаборатория могут быть изменены по согласованию с Заказчиком. Решение служит основанием для начала испытаний и «поводом» для заключения договора между Заявителем и испытательной лабораторией.

ПРИМЕР решения на проведение сертификации:

**СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
(СВИДЕТЕЛЬСТВО № РОСС RU.0001.01.БИ00)**

РЕШЕНИЕ № XXX

от « XX » *месяца* 2008 г.

по заявке ЗАО «Центр информационных технологий «XXX» (ЗАО «XXX») (Ивановское шоссе д.10, г. Москва, 111111, тел. (095)111-1111)
(наименование заявителя, адрес, телефон)
на сертификацию программного комплекса «XXXX», XXXXXXXX
(наименование продукции, код ОКП)

принято решение:

1. Сертификацию провести по схеме испытаний партии из 100 (ста) экземпляров продукции.
(называется схема сертификации)
2. Испытания сертифицируемой продукции провести в испытательной лаборатории Санкт-Петербургского научно-технического центра ФГУП «НПП «ГАММА» (Пионерская ул., д. 44, Санкт-Петербург, 167110, тел. (812)235-5518).
(наименование испытательного центра (лаборатории), адрес)
3. Сертификацию провести на соответствие требованиям технических условий XXXXXXXX и руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. По 2 уровню контроля.
(наименование нормативных и методических документов)
4. Инспекционный контроль осуществлять Санкт-Петербургским научно-техническим центром ФГУП «НПП «ГАММА» с периодичностью, установленной руководящими документами.
5. Экспертизу результатов сертификационных испытаний провести в органе по сертификации – ФГУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (Студенческая ул., д. 16, Воронеж, 394000).
(наименование органа по сертификации, адрес)
6. Работы по п.п. 1-5 провести на основе хозяйственного договора.
(хозяйственный договор, тариф, другие варианты оплаты)

НАЧАЛЬНИК 2 УПРАВЛЕНИЯ ФСТЭК РОССИИ

X.XXXXX

3. Заключение договора с испытательной лабораторией

В договоре с испытательной лабораторией о проведении сертификационных испытаний устанавливаются сроки, порядок проведения сертификационных испытаний, а также стоимость работ. Обычно испытательная лаборатория сначала готовит коммерческое предложение с обоснованием сроков и стоимости работ, а также проект договора. Как правило, в комплект договорных документов входят: договор, техническое задание на проведение работ, ведомость исполнения, протокол согласования цены. Помимо указанных сведений, в договоре рекомендуется предусмотреть такие пункты, как ответственность за порчу испытательных образцов или порядок приостановки испытаний в случае внесения каких-то изменений.

4. Подготовка исходных данных

Этот этап включает в себя разработку, согласование и утверждение программы и методики сертификационных испытаний.

Испытательная лаборатория разрабатывает программу и методику проведения испытаний, передает заявителю информацию о том, какие данные необходимы для испытаний. Также программа и методика отправляются в орган по сертификации на утверждение.

Заявитель получает от испытательной лаборатории программу и методику испытаний, согласовывает ее и готовит все необходимые исходные данные. Он предоставляет испытательной лаборатории средства защиты информации в комплектации, соответствующей техническим условиям или формуляру, а также комплект всей необходимой документации в соответствии с ЕСПД или ЕСКД.

5. Сертификационные испытания.

Испытательная лаборатория отбирает образцы сертифицируемой продукции, идентифицирует их и проводит сертификационные испытания продукции по утвержденным программе и методике. При этом Заявитель готовит и настраивает стенд для проведения сертификационных испытаний. Важно отметить, что запрещается вносить изменения в состав или конструкцию объекта сертификации, а также в документацию во время испытаний. Это может привести к остановке испытаний и их полному "перезапуску", что повлияет на стоимость и сроки проведения работ.

6. Оформление результатов испытаний

Результаты испытаний оформляются в виде протоколов сертификационных испытаний и технических заключений. Эти документы направляются в орган по сертификации, а копии – Заявителю. В случае отсутствия обоснованных замечаний к результатам, предоставленным испытательной лабораторией, со стороны Заявителя или органа по сертификации, ее работа по договору считается выполненной.

7. Заключение договора с органом по сертификации

Испытательная лаборатория заключает договор с органом по сертификации о проведении экспертизы результатов сертификационных испытаний, в котором оговариваются сроки (как правило, 1 месяц), порядок и стоимость. Иногда орган по сертификации требует заключить договор с Заявителем, а не с испытательной лабораторией. Этот пункт является спорным и не регламентированным. Данный вопрос лучше всего изначально оговорить с испытательной лабораторией.

8. Экспертиза результатов сертификационных испытаний

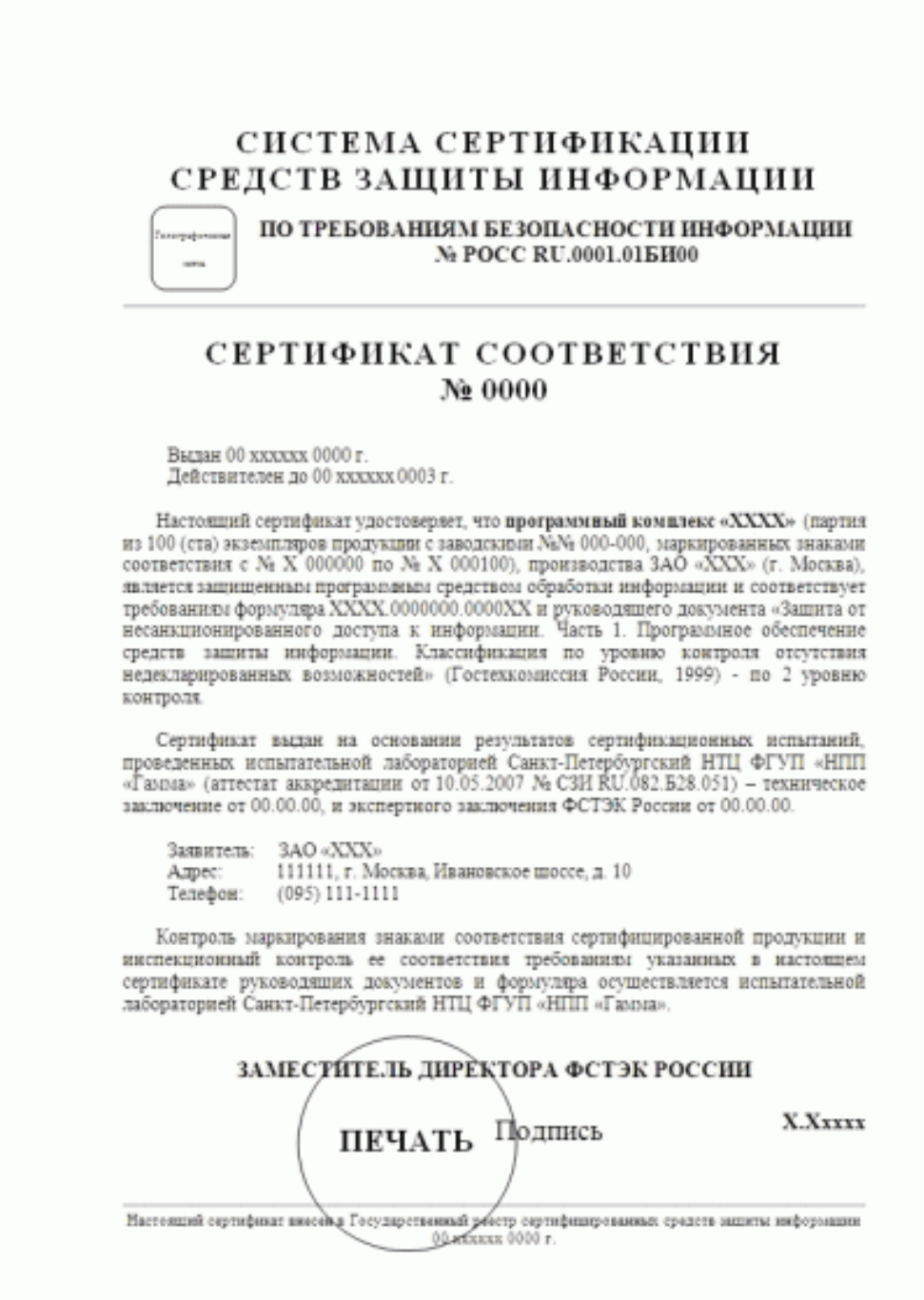
Орган по сертификации в соответствии с договором проводит экспертизу результатов сертификационных испытаний, а также технических и эксплуатационных документов на сертифицируемую продукцию. Результатом становится оформление экспертного заключения, которое вместе с техническим заключением, материалами сертификационных испытаний, комплектом необходимой технической и эксплуатационной документации на

объект сертификации представляет во ФСТЭК России для принятия решения о выпуске сертификата.

9. Решение о выдаче сертификата.

На основании полученных от органа сертификации документов, а именно технического заключения и экспертного заключения, ФСТЭК принимает решение о выдаче сертификата.

ПРИМЕР сертификата соответствия:



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 0000

Выдан 00 xxxxxx 0000 г.
Действителен до 00 xxxxxx 0003 г.

Настоящий сертификат удостоверяет, что **программный комплекс «XXXX»** (партия из 100 (ста) экземпляров продукции с заводскими №№ 000-000, маркированных знаками соответствия с № X 000000 по № X 000100), производства ЗАО «XXX» (г. Москва), является защищенным программным средством обработки информации и соответствует требованиям формуляра XXXX.0000000.0000XX и руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 2 уровню контроля.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией Санкт-Петербургский НТЦ ФГУП «НПП «Гамма» (аттестат аккредитации от 10.05.2007 № СЗИ RU.082.Б28.051) – техническое заключение от 00.00.00, и экспертного заключения ФСТЭК России от 00.00.00.

Заявитель: ЗАО «XXX»
Адрес: 111111, г. Москва, Ивановское шоссе, д. 10
Телефон: (095) 111-1111

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанных в настоящем сертификате руководящих документов и формуляра осуществляется испытательной лабораторией Санкт-Петербургский НТЦ ФГУП «НПП «Гамма».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

ПЕЧАТЬ Подпись X.Xxxxx

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 00 хххххх 0000 г.

Если в результате проверки ФСТЭК выявит несоответствие результатов испытаний требованиям законодательства, будет принято решение об отказе в выдаче сертификата. При этом Заявителю будет направлено мотивированное заключение. В случае несогласия с отказом Заявитель имеет право обратиться в апелляционный совет Федерального органа по сертификации для дополнительного рассмотрения материалов сертификации. Апелляция

рассматривается в месячный срок с привлечением заинтересованных сторон и независимых экспертов. Податель апелляции извещается о принятом решении.

Иллюстрационный материал для практической работы
«Интерфейс командной строки для управления компьютерной системой»

Рисунок 1:

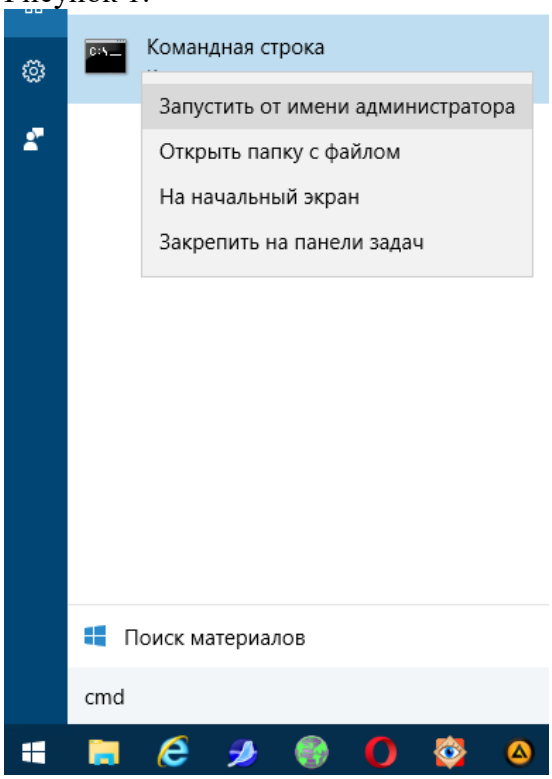


Рисунок 2:

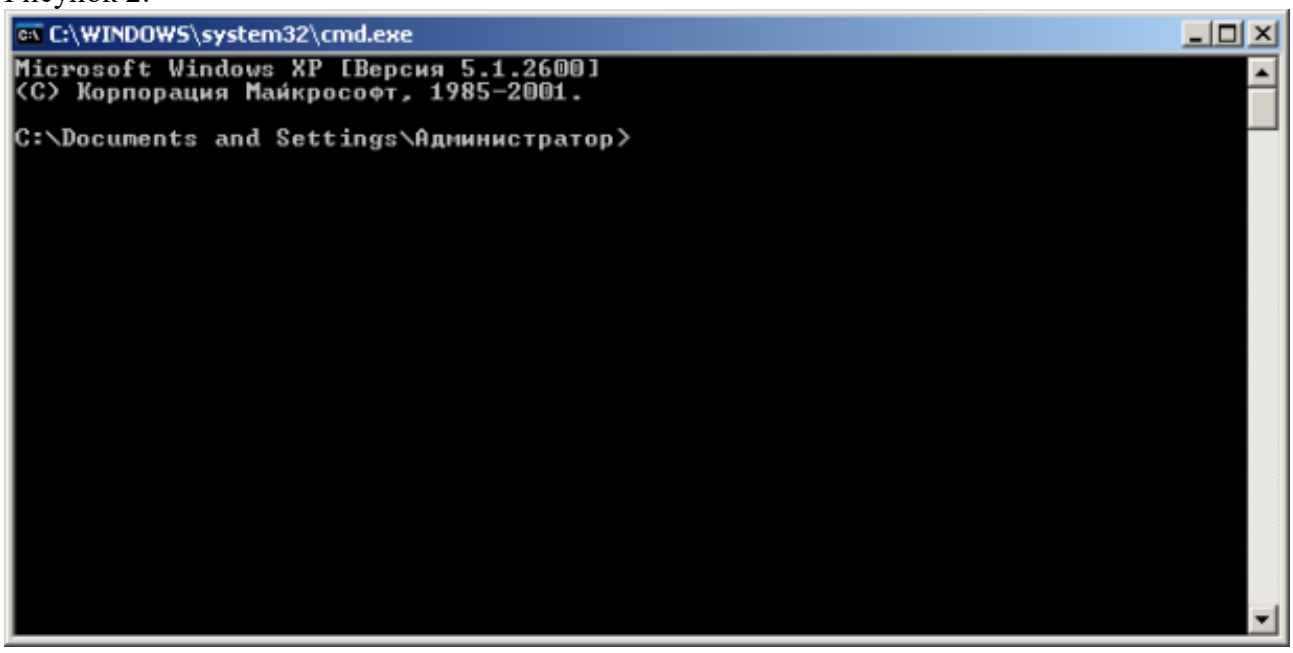


Рисунок 3:

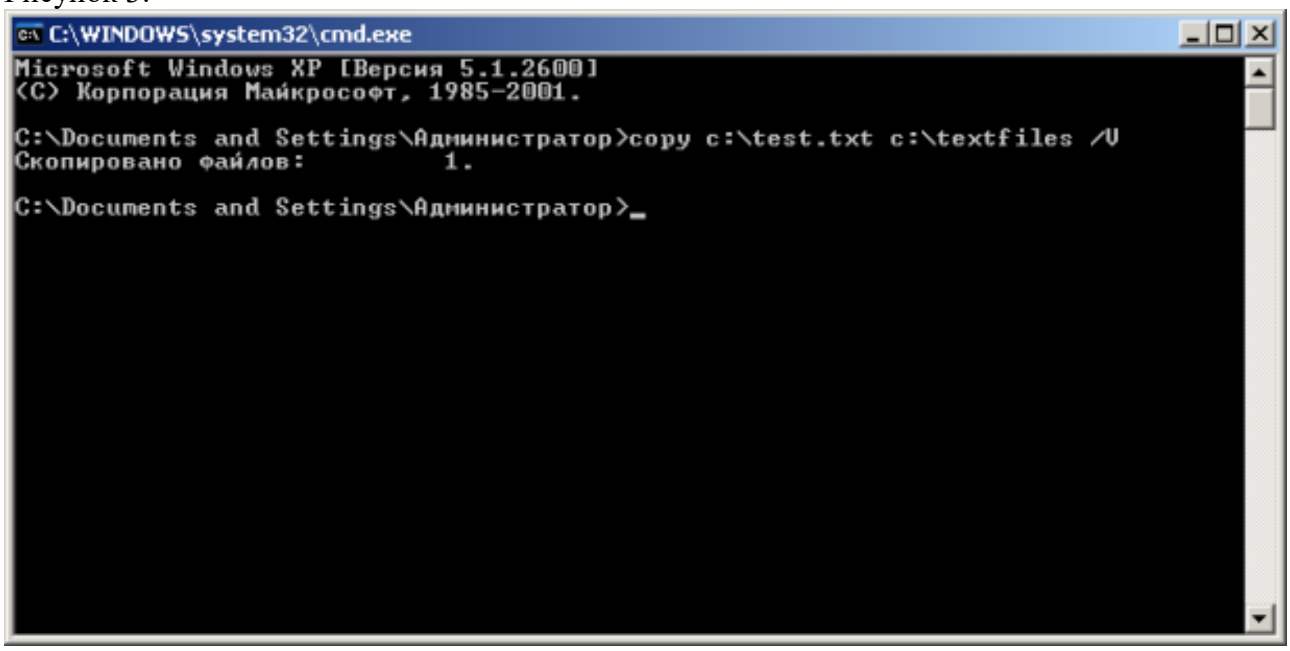


Рисунок 4:

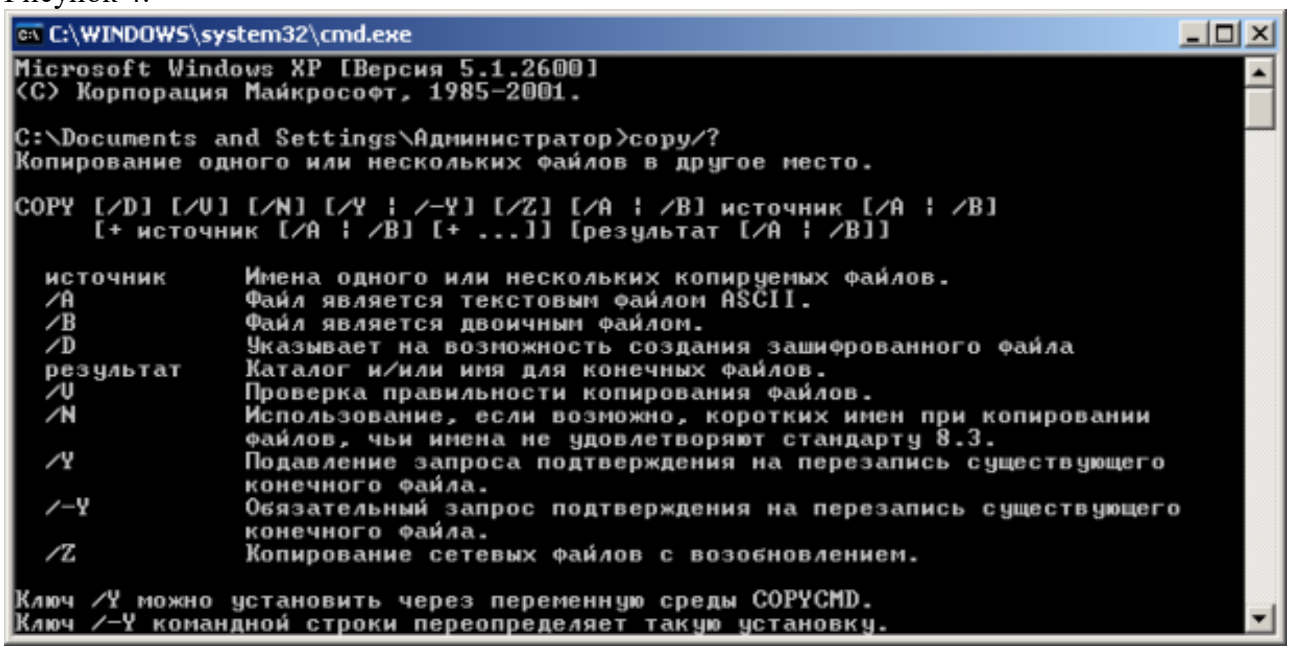


Рисунок 5:

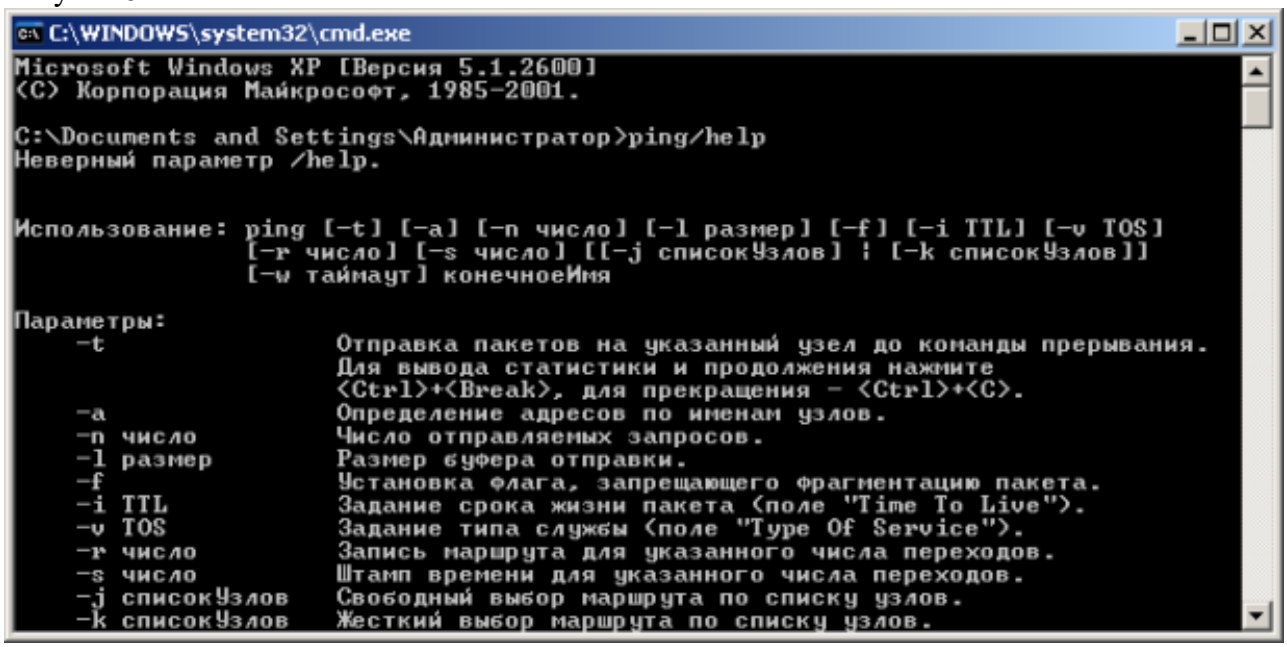


Рисунок 6:

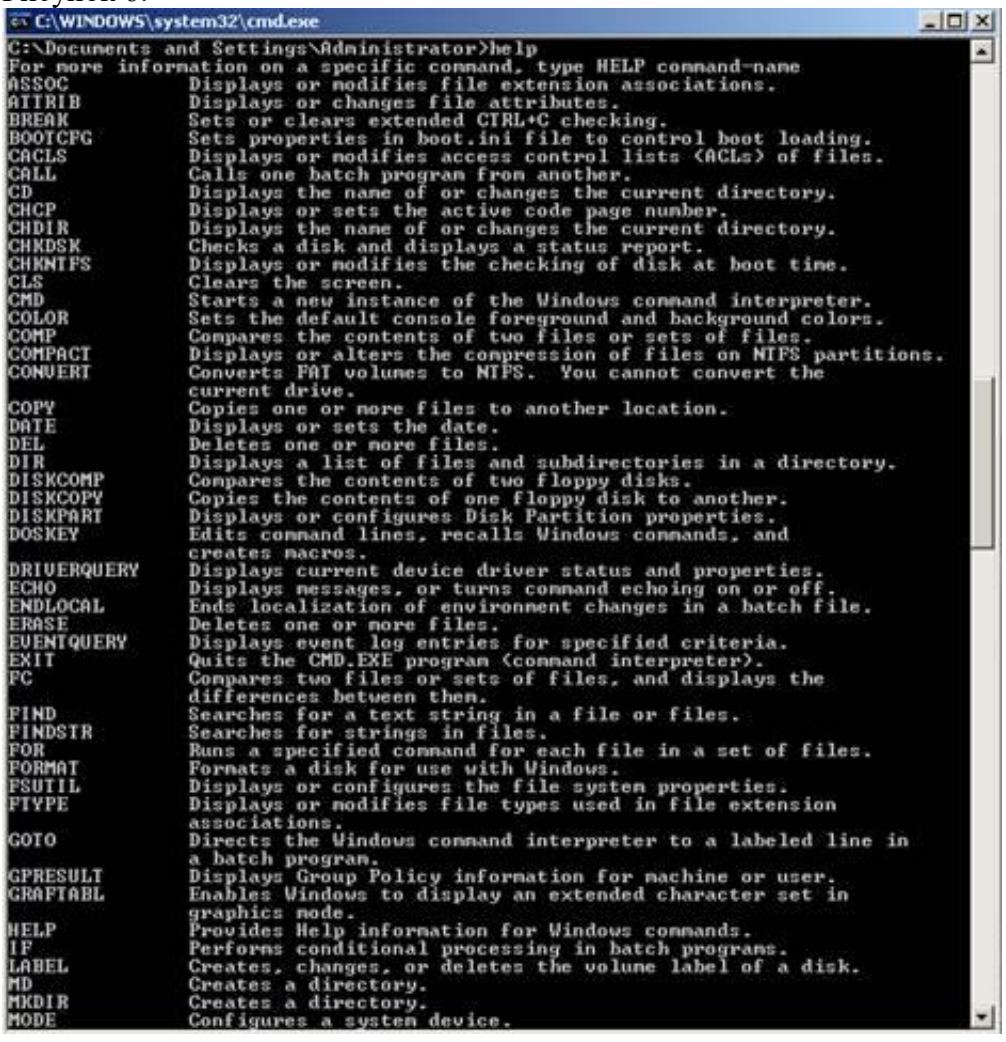


Рисунок 7:

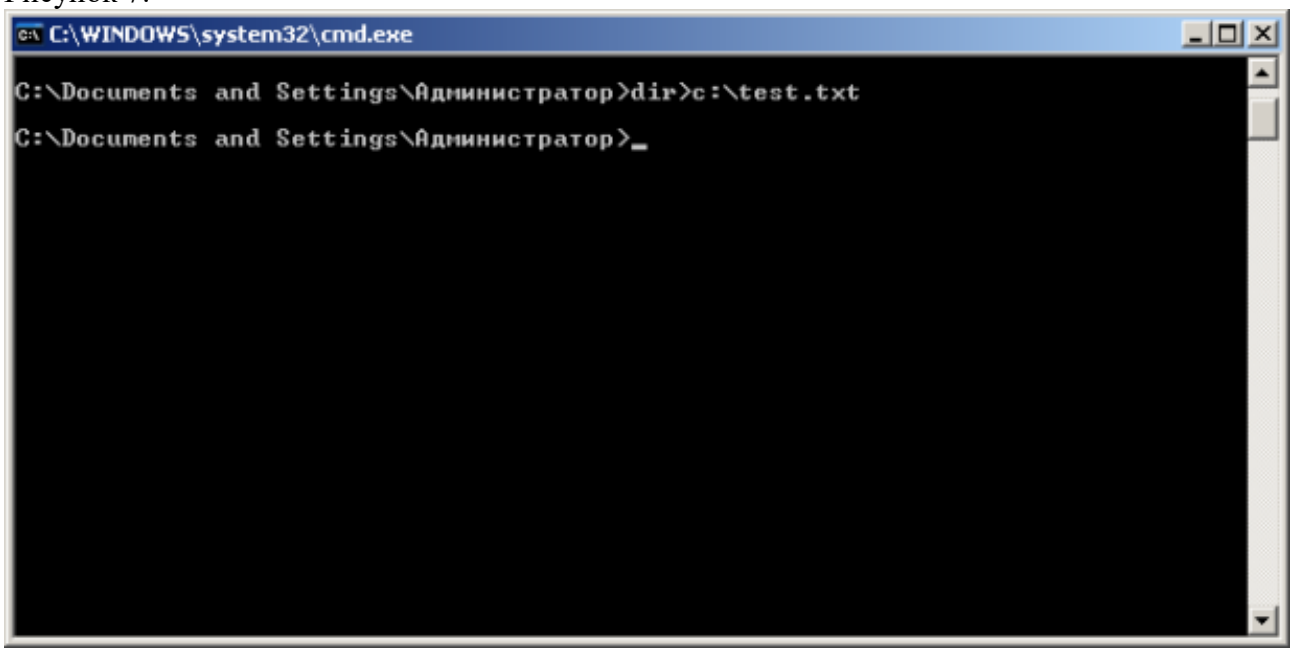


Рисунок 8:

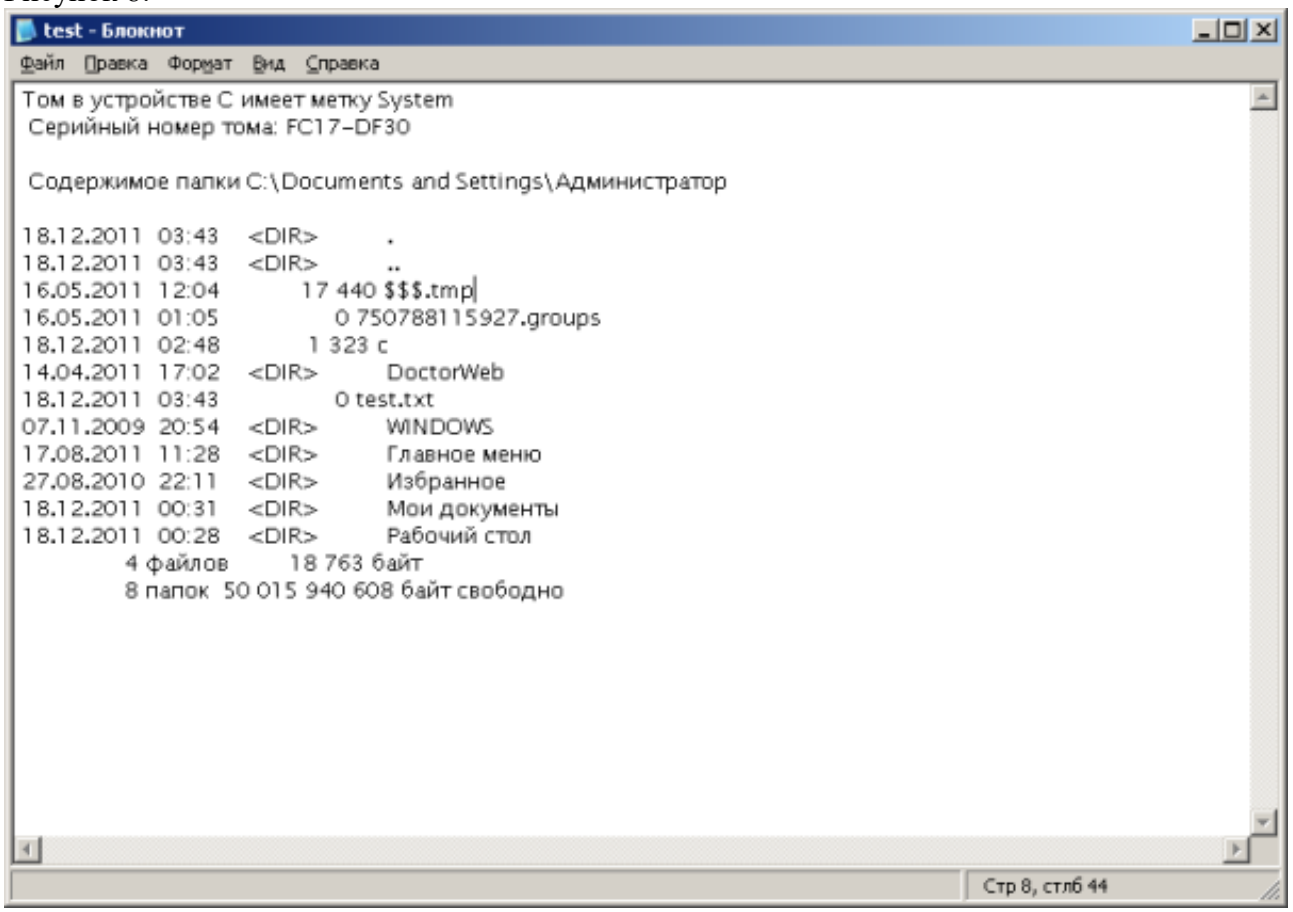


Рисунок 9:

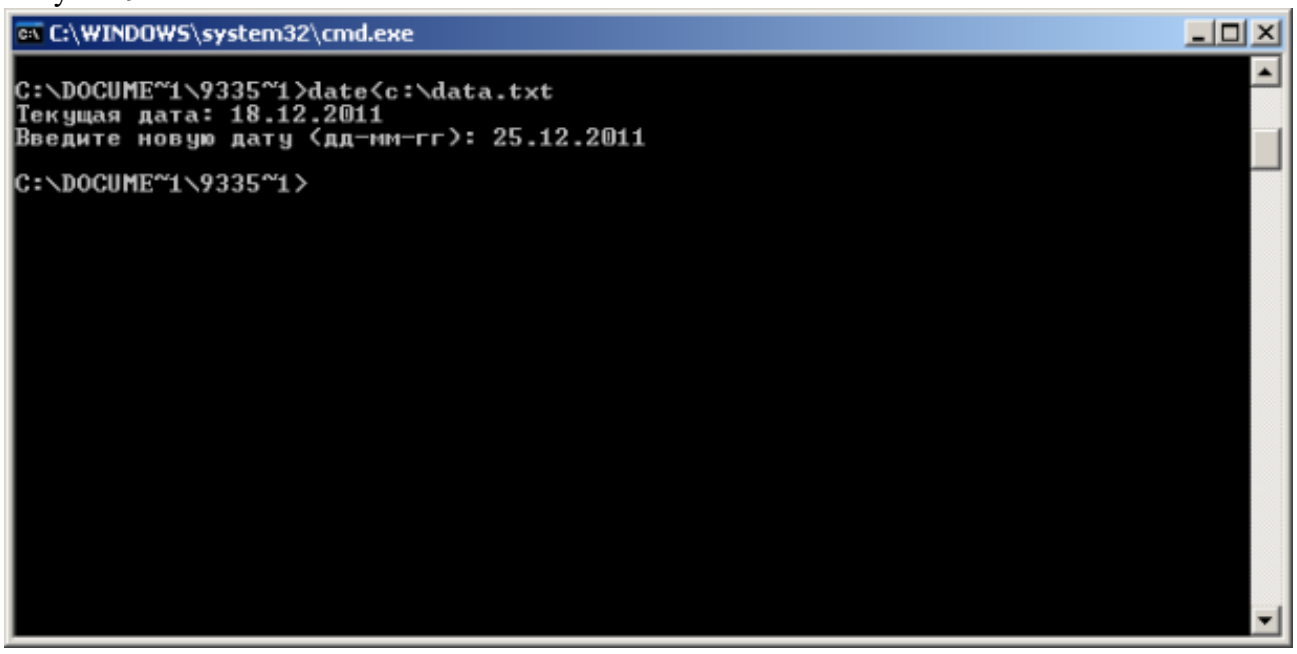


Рисунок 10:

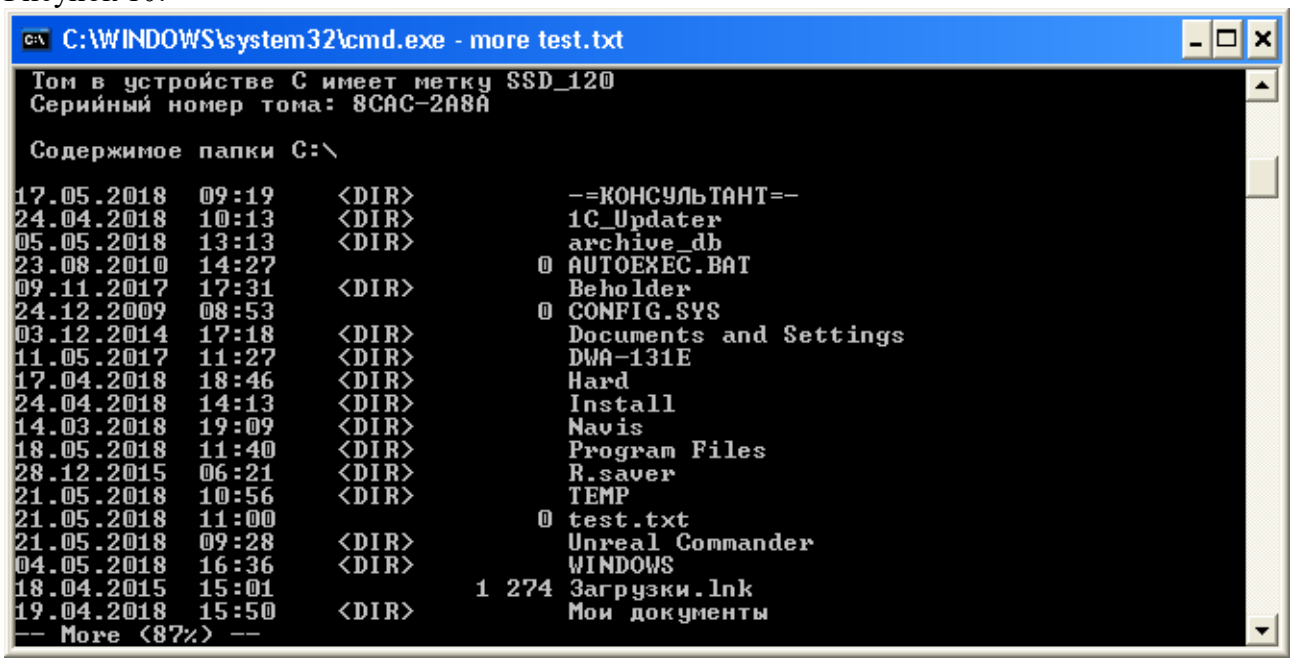


Рисунок 11:

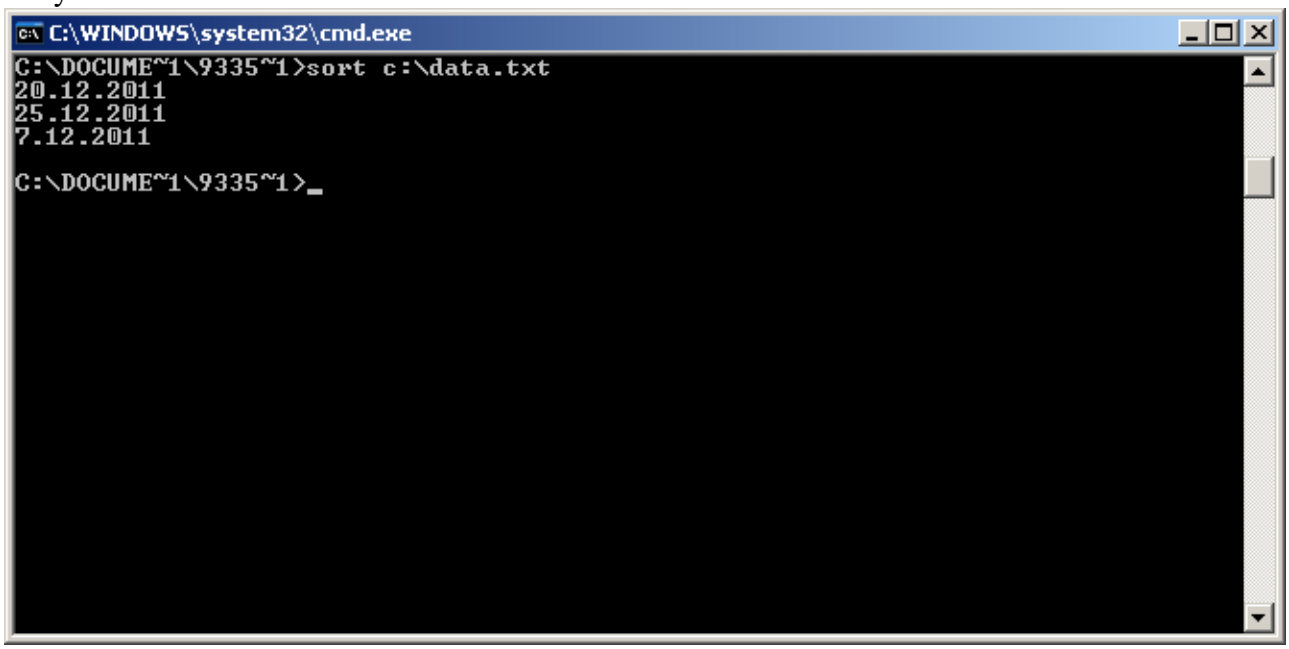
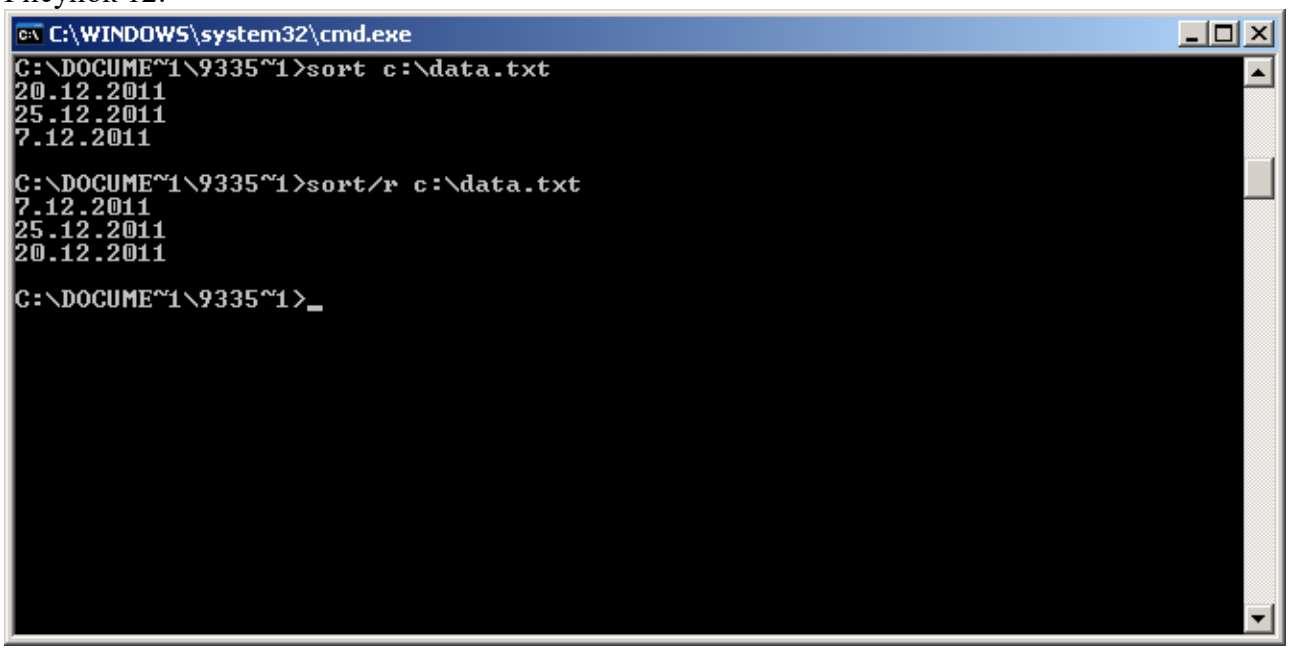


Рисунок 12:



Иллюстрационный материал для практической работы
«Анализ сетевой активности с помощью интерфейса командной строки»

Рисунок 1:

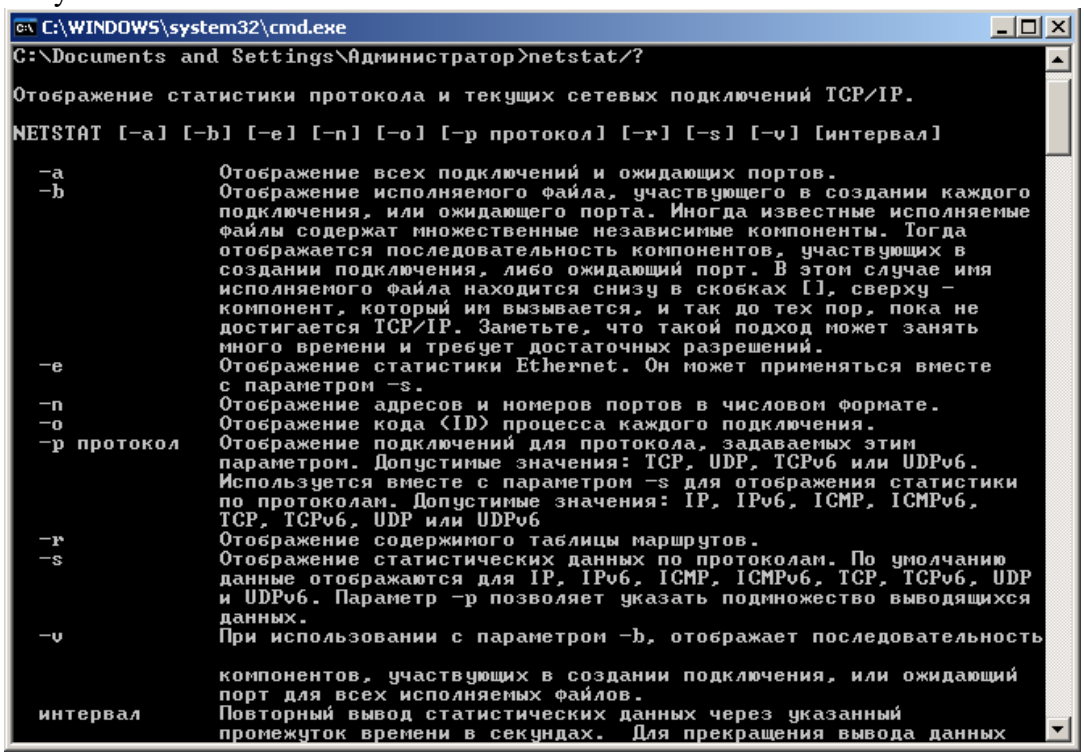
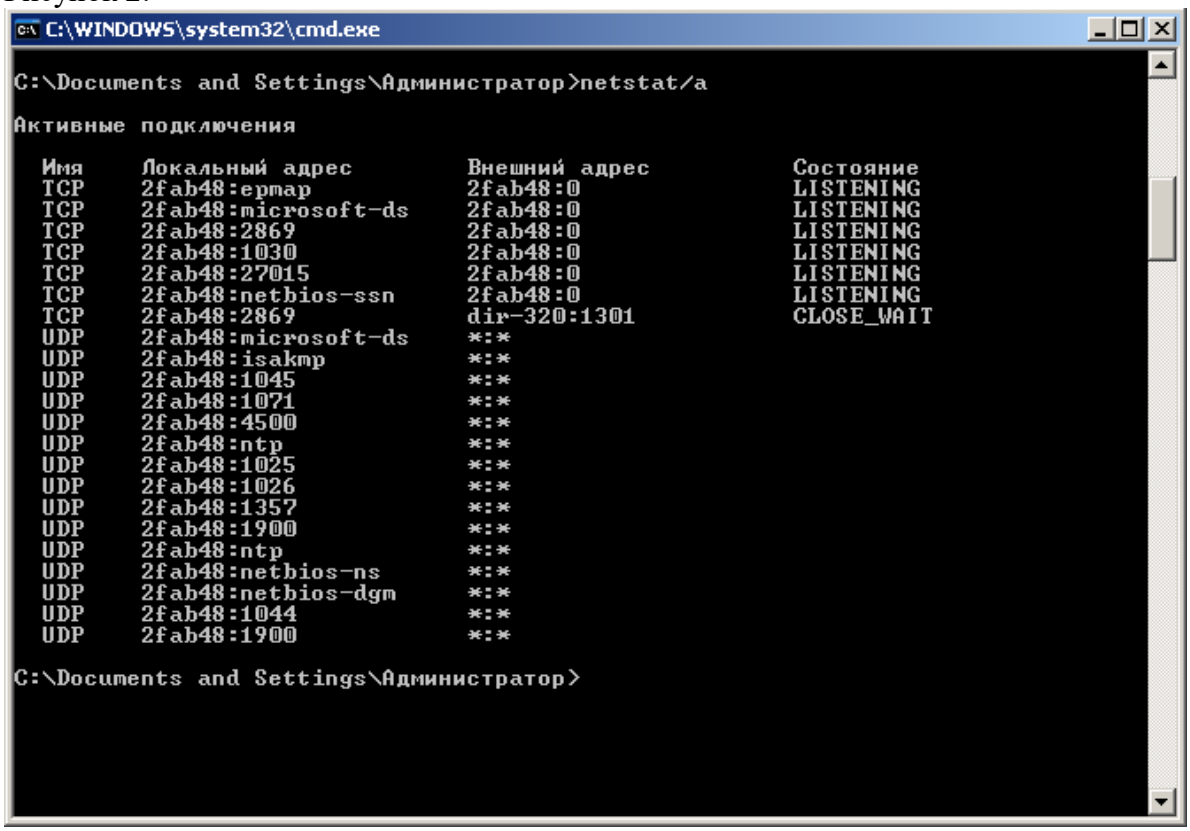


Рисунок 2:



Ознакомительный материал для практической работы «Выявление технических каналов утечки информации (ТКУИ) для объекта информатизации путем моделирования возможных действий технических разведок»

ВВЕДЕНИЕ

Для того чтобы построить эффективную систему информационной безопасности, необходимо в первую очередь определить потенциальные и реальные угрозы технического проникновения на защищаемый объект, возможные каналы для несанкционированного доступа и утечки защищаемой информации.

Данная работа базируется на знании природы возникновения технических каналов утечки информации и методов ведения технической разведки. Правильное определение потенциальных угроз на предпроектном этапе построения системы защиты позволит в дальнейшем выбрать наиболее оптимальные меры и средства защиты.

При выявлении технических каналов утечки информации необходимо рассматривать всю совокупность элементов защиты, включающую основное оборудование технических средств обработки информации , соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы вентиляции и т.п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы, такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др. Наибольшее внимание следует уделить вспомогательным средствам, имеющим линии, выходящие за пределы контролируемой зоны: «посторонние» транзитные провода и кабели, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

При оценке защищенности помещений от утечки речевой информации необходимо учитывать возможность ее прослушивания как из соседних помещений, так и с улицы. Следует проводить оценку возможности ведения разведки с использованием лазерных микрофонов. Интерес могут вызывать каналы утечки за счет вибраций, возникающих под давлением акустических волн, в твердых телах (ограждениях, трубах и т.п.).

Оценка защищенности объекта включает в себя анализ режима работы и охраны объекта, с целью моделирования действий по скрытному проникновению на них (неконтролируемому пребыванию) посторонних лиц: например, режим работы специалистов сторонних организаций, приобретение, установка и ремонт мебели, оргтехники и т.п. – то есть всю совокупность условий, позволяющих внедрить на объект специальные закладные устройства перехвата информации (микропередатчики, возможность установки миниатюрных микрофонов с подключением к внешним линиям и т.д.).

Большое, а иногда и решающее значение при оценке угрозы может иметь знание наиболее вероятного противника, его финансовых и оперативных возможностей, знание личностных качеств постоянного персонала, временных работников и другая дополнительная информация.

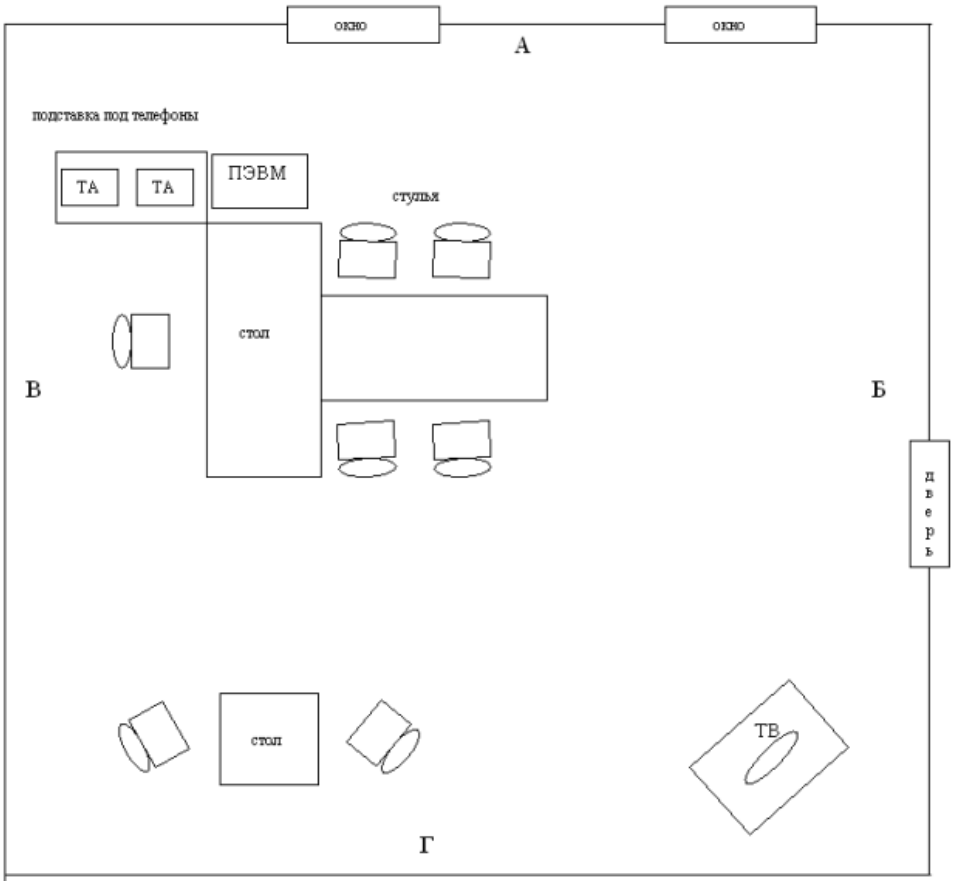
ПРИМЕР ЗАЩИЩАЕМОГО ИНФОРМАЦИОННОГО ОБЪЕКТА

ТЕКСТОВОЕ ОПИСАНИЕ

1) Защищаемое помещение расположено на четвертом этаже 7-этажного здания. Всё здание принадлежит одной организации:

а) сверху расположены служебные помещения;

б) снизу расположены технические помещения (туалет, электрощитовая);
в) со стороны стены Б расположена приемная;
г) со стороны стены Г расположен общий коридор;
Стороны А и В выходят на улицы с интенсивным пешеходным и транспортным движением. Окна помещения оборудованы шторами, смотрят на жилой дом, расположенный на расстоянии около 30 метров.
2) Из мебели в помещении установлены – рабочий и журнальный столы, стулья, подставки под телефоны, компьютер (на схеме обозначен ПЭВМ) и телевизор.
3) Из основных технических средств в помещении установлены – телефон внутренней конфиденциальной связи и компьютер (подсоединенный к локальной вычислительной сети).
4) Из вспомогательных технических средств в помещении установлены – городской телефон (ГТС), телевизор, радиотрансляционный приемник. Помещение оборудовано системой пожарной и охранной сигнализации, линии которых выходят на пульт дежурного охранника. Помещение электрифицировано (освещение, электропитание оборудования).
5) Помещение оборудовано системой вытяжной вентиляции, короб которой проложен вдоль коридора и поднимается на крышу здания. Радиаторы отопления установлены вдоль стены А. Трубы отопления спускаются в подвал.
6) Режим работы учреждения предусматривает свободное передвижение сотрудников и посетителей в рабочее время. На нерабочее время помещение запирается на ключ и сдается под охрану дежурному. Системы связи обслуживаются штатным сотрудником. Системы жизнеобеспечения (отопление, канализация) обслуживаются по заявке приходящим сотрудником.
7) Доступ штатных сотрудников к служебной информации не разграничен.
СХЕМА



ЗАЩИЩЕННОСТЬ

В качестве примера представим порядок рассуждения защищенности объекта со стороны окон. При определении вероятности существования каналов утечки, в случае недостаточности исходных данных, допущено использование оговорок типа «если.... то....».

1) Просмотр помещения непосредственно с улицы (пешеходы или из автомобиля) невозможен ввиду того, что помещение находится на 4 этаже. Однако возможен просмотр помещения извне, со стороны жилого дома с помощью оптических приборов, следовательно существует потенциальный канал утечки визуальной информации.

Однако, если организационными мероприятиями (соответствующим инструктажем ответственных лиц) введено и неукоснительно исполняется обязательное зашторивание окон во время проведением совещаний, работы с документами и т.п., то реальный продуктивный визуально-оптический канал утечки информации блокируется.

В качестве дополнительных мер можно ввести периодический контроль за соблюдением сотрудниками правила зашторивания, а также поставить тонированные или рифленые (матированные) стёкла.

2) Так как возможно прослушивание помещения, со стороны улицы и жилого дома, через открытые окна и форточки с помощью направленных микрофонов, существует потенциальный канал утечки акустический информации.

Однако, если организационными мероприятиями введено обязательное закрытие окон и форточек во время проведения совещаний, то реального акустического канала утечки информации нет.

В качестве дополнительной меры можно установить кондиционер или приобрести генератор белого шума и включать его во время проведения совещаний.

3) Так как возможен съем информации о ведущихся в помещении переговорах с оконных стекол, за счет их вибрации, путем использования дальнодействующего лазерного микрофона с поста перехвата в жилом доме, то существует ещё один потенциальный канал утечки акустической информации.

В данном случае с помощью одних организационных мероприятий устранить канал утечки не представляется возможным. Однако реальное существование канала утечки может быть констатировано лишь после проведения инструментальных измерений.

По результатам инструментальной проверки будет определяться необходимость проведение защитного мероприятия, например, установка специальных стекол или зашумление стекол и пространства между ними.

В заключение первого этапа можно предложить установку стекол с рифленой поверхностью и кондиционера. Решение представляется оптимальным, т.к. акустический и визуально оптический каналы устраняются при минимальных финансовых затратах. Также, в дальнейшем, обеспечивается удобство эксплуатации объекта и исключается негативный человеческий фактор.

При оценке вероятности использования технической разведкой потенциальных каналов утечки информации следует принимать во внимание окружающую обстановку, с точки зрения возможности по организации и ведению технической разведки, а именно:

а) скрытное размещение поста перехвата (для прослушивания и просмотра помещения) на улице с интенсивным движением затруднительно, т.к. подозрительные лица, транспортные средства и т.п. привлекают к себе внимание, легко визуально обнаруживаются;

б) скрытное размещение поста перехвата (для прослушивания и просмотра помещения, установки лазерного микрофона) в жилом здании, если, например, арендовать квартиру с окнами расположенными напротив окон защищаемого помещения, вполне реализуемо и

доступно.

Необходимо, если имеется такая возможность, проверить благонадежность (лояльность) жильцов в квартирах, потенциально пригодных для организации поста перехвата (сдаются ли квартиры, проживают ли в квартирах потенциальные конкуренты, имеются ли лица, бывшие в конфликте с законом и т.п.). Следует предположить возможности организации постов контрперехвата на технических этажах (например, на чердаке).

В случае получения в ходе проверки положительных данных можно заключить, что защитные мероприятия не требуются вообще. С точки зрения защиты от случайных утечек, например прослушивания, можно заключить, что улица с интенсивным автомобильным и пешеходным движением создает достаточно сильную акустическую помеху, за которой разговоры случайными прохожими различаться не будут. При необходимости в этом можно убедиться экспериментально.

В случае получения в ходе проверки отрицательных или неоднозначных данных оптимальным остается вариант указанный в заключение первого этапа.