Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

И.И. Баранкова
О.В. Пермякова

ОПРЕДЕЛЕНИЕ КРИТИЧЕСКИ ЗНАЧИМЫХ РЕСУРСОВ ОБЪЕКТА ЗАЩИТЫ ПРИ СОСТАВЛЕНИИ МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Утверждено Редакционно-издательским советом университета
в качестве учебного пособия

Магнитогорск
2017

УДК 004.056.52

Рецензенты:

кандидат технических наук,
заместитель директора СЦ
ООО «ТЕХНОАП Инжиниринг»
Д.В. Швидченко

кандидат технических наук,
доцент кафедры электроники и микроэлектроники,
ФГБОУ ВО «Магнитогорский государственный технический
университет им. Г.И. Носова»
Н.В. Швидченко

Баранкова И.И., Пермякова О.В.
Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс]: учебное пособие / Инна Ильинична Баранкова, Ольга Валерьевна Пермякова ; ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». – Электрон. текстовые дан. (0,66 Мб). – Магнитогорск : ФГБОУ ВО «МГТУ им. Г.И. Носова», 2017. – 1 электрон. опт. диск (CD-R). – Систем. требования : IBMPC, любой, более l GHz ; 512 Мб RAM ; 10 Мб HDD ; MS Windows XP и выше ; Adobe Reader 8.0 и выше ; CD/DVD-ROM дисковод ; мышь. – Загл. с титул. экрана.
ISBN 978-5-9967-1031-7

Пособие разработано в соответствии с рабочей программой дисциплины «Разработка и эксплуатация защищенных автоматизированных систем», и так же может использоваться в рамках изучения дисциплины: «Моделирование угроз информационной безопасности».

В пособии рассмотрены подходы к классификации автоматизированных систем, определению исходной степени защищенности объекта защиты, к процессу категорирования информационных ресурсов, подлежащих защите. Значительное внимание уделяется порядку составления перечня актуальных угроз безопасности персональных данных. Пособие содержит актуальный материал, основанный на действующих нормативных документах в сфере информационной безопасности.

Учебное пособие разработано для обеспечения образовательной программы по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем».

УДК 004.056.52

ISBN 978-5-9967-1031-7

Содержание

ВВЕДЕНИЕ

Особое значение в вопросах информационной безопасности представляет задача определения требований по защите информации и ее носителей, а также и процессов ее обработки.

Доступность, целостность и конфиденциальность являются важнейшими качествами информации в этой предметной области.

Классификация информации по уровням требований к ее защищенности обозначает введение ряда категорий (степеней) требований по обеспечению каждого из свойств безопасности информации: доступности, целостности, конфиденциальности.

Главной целью защиты информации является предотвращение или снижение величины ущерба, наносимого владельцу и/или пользователю этой системы, вследствие реализации угроз безопасности информации [1].

Частными целями защиты информации являются, согласно [1]:

- предотвращение утечки информации по техническим каналам;
- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации;
- соблюдение правового режима использования массивов, программ обработки информации, обеспечения полноты, целостности, достоверности информации в системах обработки;
- сохранение возможности управления процессом обработки и использования информации условиях несанкционированных воздействий на защищаемую информацию.

Защита информации в автоматизированных системах в защищенном исполнении (АСЗИ) должна быть:

- целенаправленной, осуществляемой в интересах реализации конкретной цели защиты;
- комплексной, осуществляемой в интересах защиты всех структурных элементов АСЗИ от всего спектра угроз;
- управляемой, осуществляемой на всех стадиях жизненного цикла АСЗИ, в зависимости от важности обрабатываемой информации;
- гарантированной; методы и средства защиты информации должны обеспечивать требуемый уровень защиты информации от ее утечки по техническим каналам, несанкционированного доступа к информации, несанкционированным и непреднамеренным воздействиям на нее, независимо от форм ее представления.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В нормативных документах: федеральных законах, ГОСТах, руководящих документах ФСТЭК, методических инструкциях ФСТЭК [1-6], приняты следующие термины и их сокращения (таблица 1):

Таблица 1

Основные термины и определения в сфере информационной безопасности

Термин	Определение	Ссылка на документ
Автоматизированная система в защищённом исполнении (АСЗИ)	Автоматизированная система, реализующая инф. технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации	ГОСТ Р53114 - 2008
Актив	всё, что имеет ценность для организации.	ISO/IEC 27000:2009
Анализ риска	Систематическое использование информации для определения источников риска и количественной оценки риска	ГОСТ Р ИСО/МЭК 27001-2006, ст.3.11 ГОСТ Р 53114-2008
Атака (компьютерная)	попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования	ISO/IEC 27000:2014 http://bdu.fstec.ru/ubi/terms/terms/index
Аудит информационной безопасности организации	Систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению ИБ и установлению степени выполнения в организации критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии ИБ организации	ГОСТ Р 53114-2008

Термин	Определение	Ссылка на документ
База данных (БД)	набор данных, который достаточен для установленной цели и представлен на машинном носителе в виде, позволяющем осуществлять автоматизированную переработку содержащейся в нем информации	ГОСТ 7.73-96 http://bdu.fstec.ru/ubi/terms/terms/index
Банк данных	информационно-поисковая система, состоящая из одной или нескольких баз данных и системы хранения, обработки и поиска информации в них	ГОСТ 7.73-96
Безопасность информации	Состояние защищённости информации, при котором обеспечены её конфиденциальность, доступность и целостность	ГОСТ Р50922 - 2006, п.2.4.5 ГОСТ Р 53114-2008
Безопасность информации [данных]	состояние защищённости информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность	ГОСТ Р 50922-2006
Безопасность персональных данных	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.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Биометрические персональные данные	сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.	
Блокирование доступа к информации	Прекращение или затруднение доступа к информации лиц, имеющих на это право прекращение или затруднение доступа законных пользователей к информации	ГОСТ Р 53114-2008

Термин	Определение	Ссылка на документ
Блокирование персональных данных	временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Ботнет	компьютерная сеть, узлы которой содержат в себе скрытно функционирующие экземпляры вредоносного программного обеспечения, предназначенного для осуществления нелегальной деятельности: обработки информации или вредоносного воздействия на другие узлы компьютерной сети (рассылки спама, проведения атак типа "распределённый отказ в обслуживании" и т.п.)	http://bdu.fstec.ru/ubi/terms/terms/index
Вирус	Вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы	ГОСТ Р 51275-2006
Впервые выявленная уязвимость	уязвимость, выявленная впервые и неопубликованная в общедоступных источниках	ГОСТ Р 56545-2015
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы. Программа, используемая для осуществления НСД к информации и (или) воздействия на информацию или ресурсы автоматизированной системы	ГОСТ Р 50922-2006
Вредоносная программа [программное обеспечение]	программа [программное обеспечение], предназначенная для осуществления несанкционированного доступа к информации и или деструктивного воздействия на информацию или ресурсы информационной системы нарушение их целостности и/или доступности	ГОСТ Р 53113.1-2008

Термин	Определение	Ссылка на документ
Вспомогательные технические средства и системы (ВТСС)	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.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Доступ в операционную среду компьютера (информационной системы персональных данных)	получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Доступ к информации	возможность получения информации и её использования	ГОСТ Р 50922-2006
Доступность информации	состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно	Р 50.1.056-2005
Замысел защиты информации	Основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.	ГОСТ Р 50922-2006
Защита информации (ЗИ)	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию	ГОСТ Р50922 - 2006 ГОСТ Р 53114-2008
Защита информации от (иностранной) разведки	Защита информации, направленная на предотвращение получения защищаемой информации (иностранной) разведкой.	ГОСТ Р 50922-2006

Термин	Определение	Ссылка на документ
Защита информации от непреднамеренного воздействия	Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.	ГОСТ Р 50922-2006
Защита информации от несанкционированного воздействия (ЗИ от НСВ)	Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.	ГОСТ Р 50922-2006
Защита информации от несанкционированного доступа (ЗИ от НСД)	Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.	ГОСТ Р 50922-2006

Термин	Определение	Ссылка на документ
Защита информации от преднамеренного воздействия (ЗИ от ПДВ)	Защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.	ГОСТ Р 50922-2006
Защита информации от разглашения	Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.	ГОСТ Р 50922-2006
Защита информации от утечки	ЗИ, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и НСД к ней, а также на исключение получения защищаемой информации разведками и другими заинтересованными субъектами	ГОСТ Р 50922-2006
Защищаемая информационная система	Информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.	ГОСТ Р 50922-2006
Защищаемая информация	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.	ГОСТ Р 50922-2006
Защищаемый объект информатизации	Объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.	ГОСТ Р 50922-2006
Идентификатор типа ошибки	идентификатор, устанавливаемый в соответствии с общим перечнем ошибок CWE (Common Weakness Enumeration)	http://bdu.fstec.ru/ubi/terms/terms/index

Термин	Определение	Ссылка на документ
Идентификация	присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Известная уязвимость	Уязвимость, опубликованная в общедоступных источниках с описанием соответствующих мер защиты информации, исправлений недостатков или соответствующих обновлений.	ГОСТ Р 56545-2015
Инсайдер	сотрудник предприятия, который причиняет или планирует причинение ущерба активам организации или помогает в такой акции внешнему нарушителю	http://bdu.fstec.ru/ubi/terms/terms/index
Информативный сигнал	Сигнал, по параметрам которого может быть определена защищаемая информация	Р 50.1.053-2005, п.3.2.6 ГОСТ Р 53114-2008
Информационная система	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 50922-2006 ГОСТ Р 51583-2014
Информационная система персональных данных (ИСПДн)	это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Информационно-телекоммуникационная сеть	технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники	http://bdu.fstec.ru/ubi/terms/terms/index

Термин	Определение	Ссылка на документ
Информационные технологии	процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов	ГОСТ Р 56546-2015
Информация	сведения сообщения, данные независимо от формы их представления	http://bdu.fstec.ru/ubi/terms/terms/index
Инцидент инф. безопасности	Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность	ГОСТ Р ИСО/МЭК 27001- 2006, ст.3.6
Источник угрозы безопасности информации	Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.	ГОСТ Р 50922-2006
Класс уязвимости	характеристика, уязвимости программного обеспечения, определяющая причину возникновения уязвимости.	http://bdu.fstec.ru/ubi/terms/terms/index
Компонент информационной системы	Часть информационной системы, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств.	ГОСТ Р 56546-2015
Компьютерная атака	Целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение НСД к ним с применением программных или программно-аппаратных средств	ГОСТ Р 51275-2006

Термин	Определение	Ссылка на документ
Компьютерный вирус	программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения.	ГОСТ Р 51188-98
Контекстные метрики	метрики, отражающие характеристики уязвимости, зависящие от среды функционирования программного обеспечения	http://bdu.fstec.ru/ubi/terms/terms/index
Контролируемая зона (КЗ)	это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Контроль обеспечения информационной безопасности организации	Проверка соответствия обеспечения информационной безопасности в организации, наличия и содержания документов требования нормативных документов, технической, правовой организационно-распорядительной документации в области ИБ	ГОСТ Р 53114-2008
Конфигурация информационной системы	Взаимосвязанные структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы . физические, логические, функциональные и технологические взаимосвязи между компонентами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, а также с полномочиями субъектов доступа к объектам доступа информационной системы.	ГОСТ Р 56546-2015

Термин	Определение	Ссылка на документ
Конфиденциальность информации	обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя	ГОСТ Р 50922-2006
Конфиденциальность персональных данных	обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Криптографическая защита информации	ЗИ с помощью ее криптографического преобразования	ГОСТ Р 50922-2006
Криптографическое средство защиты информации	Средство защиты информации, реализующее алгоритмы криптографического преобразования информации.	ГОСТ Р 50922-2006
Критерий аудита ИБ организации	Совокупность принципов, положений, требований и показателей действующих нормативных документов, относящихся к деятельности в области ИБ	ГОСТ Р 53114-2008
Критически важная система инф. инфраструктуры (КСИИ)	Информационно-управляющая система, осуществляющая управление или информационное обеспечение критическим объектом или процессом, или используемая для офиц. информирования общества и граждан, нарушение или прерывание которой может привести к ЧС со значительными негативными последствиями	ГОСТ Р 53114-2008
Критический объект	Объект или процесс, нарушение непрерывности функционирования которого может нанести значительный ущерб	ГОСТ Р 53114-2008

Термин	Определение	Ссылка на документ
Лицензирование в области защиты информации	Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ.	ГОСТ Р 50922-2006
Межсетевой экран (МЭ)	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.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Менеджмент информационной безопасности организации	Скоординированные действия по руководству и управлению организацией в части ее обеспечения ее информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды организации	ГОСТ Р 53114-2008
Мера безопасности	Сложившаяся практика, процедура или механизм обработки риска	ГОСТ Р 53114-2008
Мероприятия по защите информации	Совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации.	ГОСТ Р 51583-2014
Меры обеспечения информационной безопасности	Совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения ИБ	ГОСТ Р 53114-2008
Метаданные	информация, закреплённая за любым файлом и содержащая дополнительные сведения о нём (владелец информации, права доступа, дата создания и др.)	http://bdu.fstec.ru/ubi/terms/terms/index

Термин	Определение	Ссылка на документ
Множественные уязвимости	две и более уязвимости, содержащиеся в компоненте программного обеспечения, сведения о которых опубликованы в общедоступных источниках информации	http://bdu.fstec.ru/ubi/terms/terms/index
Модель угроз	Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации	ГОСТ Р 53114-2008 ГОСТ Р 50922-2006
Мониторинг информационной безопасности организации	Постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.	ГОСТ Р 53114-2008
Наведенный в токопроводящих линейных элементах технических средств сигнал (наводка)	Ток и напряжение в токопроводящих элементов, вызванные электромагнитным излучением, емкостными и индуктивными связями	ГОСТ Р 51275-2006
Нарушитель безопасности	физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.	ГОСТ 53113.1-2008
Нарушитель безопасности персональных данных	физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн

Термин	Определение	Ссылка на документ
Недекларированные возможности (НДВ)	Функциональные возможности ПО, не описанные в документации; функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.	ГОСТ Р 51275-2006
Недекларированные возможности [программного обеспечения]	функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности и (или) целостности обрабатываемой информации.	РД Гостехкомиссии России «Защита от НСД. Часть 1. ПО средств ЗИ. Классификация по уровню контроля отсутствия НДВ»
Несанкционированное воздействие на информацию	Воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.	ГОСТ Р 50922-2006
Несанкционированный доступ к информации (НСД)	доступ к информации ресурсам информационной системы, осуществляемый с нарушением установленных прав и/или правил доступа к информации ресурсам информационной системы с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.	Рекомендации по стандартизации Р 50.1.056-2005
Норма эффективности защиты информации	Значение показателя эффективности защиты информации, установленное нормативными и правовыми документами	ГОСТ Р 50922-2006

Термин	Определение	Ссылка на документ
Носитель защищаемой информации	Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.	ГОСТ Р 50922-2006
Носитель информации	физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Обеспечение ИБ организации	Деятельность, направленная на устранение внутренних и внешних угроз ИБ организации или на минимизацию ущерба от возможной реализации таких угроз	ГОСТ Р 53114-2008
Обработка информации	Выполнение любого действия (операции) или совокупности действий (операций) с информацией (например, сбор, накопление, ввод, вывод, прием, передача, запись, хранение, регистрация, преобразование, отображение и т.п.), совершаемых с заданной целью.	ГОСТ Р 51583-2014
Обработка персональных данных	действия (операции) с персональными данными, включая: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Объект защиты информации	Информация или носитель информации, или информационный процесс, который необходимо защищать в соответствии с целью защиты информации	ГОСТ Р 53114-2008 ГОСТ Р 50922-2006

Термин	Определение	Ссылка на документ
Объект информатизации	Совокупность инф. ресурсов, средств и систем обработки информации, используемых в соответствии с заданной инф. технологией, а также средств их обеспечения, помещений или объектов, в которых эти системы и средства установлены, или помещений и объектов для ведения конфиденциальных переговоров	ГОСТ Р51275-2006,п.3.1 ГОСТ Р 53114-2008
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Описание уязвимости	Информация о выявленной уязвимости.	ГОСТ Р 56545-2015
Организационные меры обеспечения ИБ	Меры обеспечения ИБ, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режима работы объекта информации	ГОСТ Р 53114-2008
Оценка риска	Процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку	ГОСТ Р ИСО/МЭК 13335-1 - 2006, п.2.21 ГОСТ Р 53114-2008
Оценка соответствия ИБ организации установленным требованиям	Деятельность, связанная с прямым или косвенным определением выполнения или невыполнения в организации установленных требований ИБ	ГОСТ Р 53114-2008 ГОСТ Р 50922-2006
Паразитное электромагнитное излучение	Электромагнитное излучение, являющееся результатом паразитной генерации в электрических цепях технических средств обработки информации	ГОСТ Р 51275-2006

Термин	Определение	Ссылка на документ
Паспорт уязвимости	Документ (формализованное представление), содержащий описание уязвимости, определяющий характеристики уязвимости и выполненный в соответствии с правилами описания уязвимости.	ГОСТ Р 56545-2015
Перенаправление портов	внесение изменений в таблицу маршрутизации сетевого трафика определённых параметров работы активных сетевых устройств, позволяющее пользователю как санкционированному, так и нарушителю выполнять удалённое подключение к узлу сети, скрытому за активным сетевым устройством (межсетевым экраном, маршрутизатором и др.), путём принудительного перенаправления сетевого трафика.	http://bdu.fstec.ru/ubi/terms/terms/index
Перехват информации	Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов	Р 50.1.053-2005, п.3.2.5 ГОСТ Р 53114-2008
Персональные данные (ПДн)	Любая информация, относящаяся к определенному или определяемому на основании такой информации физ. лицу, в том числе его ФИО, дата и место рождения, адрес, соц. положение, образование и др.	ФЗ РФ от 27 июля 2006г. ст.3, п.9 ГОСТ Р 53114-2008
Плагин	независимо компилируемый программный модуль, динамически подключаемый к основной программе и предназначенный для расширения её функциональных возможностей.	http://bdu.fstec.ru/ubi/terms/terms/index
Показатель эффективности защиты информации	Мера или характеристика для оценки эффективности защиты информации.	ГОСТ Р 50922-2006

Термин	Определение	Ссылка на документ
Политика информационной безопасности	Формальное изложение правил, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности	ГОСТ Р 53114-2008
Пользователь информационной системы персональных данных	лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Потенциал нарушителя	мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе.	На основе МД ФСТЭК России «Меры ЗИ в государственных ИС»
Потенциальная уязвимость	Предполагаемая, но не подтвержденная уязвимость	http://bdu.fstec.ru/ubi/terms/terms/index
Правила описания уязвимости	Совокупность положений, регламентирующих структуру и содержащего описания уязвимости.	ГОСТ Р 56545-2015
Правила разграничения доступа	совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Правовая защита информации	ЗИ правовыми методами, включающая в себя разработку законодательных и нормативных актов, регулирующих отношения субъектов по ЗИ, применение этих документов, а также надзор и контроль за их исполнением	ГОСТ Р 50922-2006

Термин	Определение	Ссылка на документ
Преднамеренное силовое электромагнитное воздействие на информацию	Несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем.	ГОСТ Р 50922-2006
Предоставление информации	действия, направленные на получение информации определённым кругом лиц или передачу информации определённому кругу лиц	Федеральный закон от 27.07.2006 N 149-ФЗ
Признак классификации уязвимостей	Свойство или характеристика уязвимостей, по которым производится классификация.	ГОСТ Р 56546-2015
Прикладная программа	программа, предназначенная для решения задачи или класса задач в определённой области применения системы обработки информации	ГОСТ 19781-90
Программная закладка	Преднамеренно внесенный в ПО функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей ПО	ГОСТ Р 51275-2006
Программное воздействие	Несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ	ГОСТ Р 51275-2006
Программное воздействие	несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ	Рекомендации по стандартизации Р 50.1.053-2005
Прозрачный прокси-сервер	вид прокси-сервера, использование которого не требует от конечного пользователя осуществление какой-было дополнительной настройки браузера	http://bdu.fstec.ru/ubi/terms/terms/index

Термин	Определение	Ссылка на документ
Ресурс информационной системы	именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Риск	влияние неопределённости на цели	ISO Guide 73:2009
Сертификация на соответствие требованиям по безопасности информации	Форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.	ГОСТ Р 50922-2006
Сетевая авторизация	процесс создания безопасного канала связи между клиентом сети и контроллером домена для проведения проверки подлинности пользователя и назначения ему прав доступа к другим ресурсам сети в соответствии с текущей политикой безопасности домена	http://bdu.fstec.ru/ubi/terms/terms/index
Сетевая атака	Компьютерная атака с использованием протоколов межсетевого взаимодействия	ГОСТ Р 51275-2006
Система защиты информации	Совокупность органов и (или) исполнителей, исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.	ГОСТ Р 50922-2006
Система защиты информации автоматизированной системы	Совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.	ГОСТ Р 51583-2014

Термин	Определение	Ссылка на документ
Система менеджмента ИБ (СМИБ)	Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработка, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения ИБ	ГОСТ Р ИСО/МЭК 27001-2006, п.3.7 ГОСТ Р 53114-2008
Система обработки информации	Совокупность технических средств и ПО, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации	ГОСТ Р 51275-2006
Системная программа (программное обеспечение)	программа (программное обеспечение), предназначенная для поддержания работоспособности системы обработки информации или повышения эффективности ее использования в процессе выполнения прикладных программ	ГОСТ 19781-90
Слабость программного обеспечения	любая ошибка, допущенная в ходе реализации, написании, разработки или проектирования программного обеспечения (дефект, неисправность, «баг», уязвимость), которая, в случае оставления её неисправленной, может являться причиной уязвимости системы или сети для атак	http://bdu.fstec.ru/ubi/terms/terms/index
Событие	возникновение или изменение определённого набора обстоятельств	ISO Guide 73:2009
Событие информационной безопасности	выявленное наступление состояния системы, сервисов или вычислительной сети, указывающее на возможное нарушение политики информационной безопасности, на сбой или отсутствие необходимых мер защиты или на прежде неизвестную ситуацию, относящейся к обеспечению безопасности	ISO/IEC 27000:2014
Специальная проверка	Проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.	ГОСТ Р 50922-2006

Термин	Определение	Ссылка на документ
Специальное исследование	Исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации.	ГОСТ Р 50922-2006
Способ защиты информации	Порядок и правила применения определенных принципов и средств защиты информации	ГОСТ Р 50922-2006
Средства вычислительной техники (СВТ)	совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Средство защиты информации	Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.	ГОСТ Р 50922-2006
Средство защиты от НСД	Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения НСД	ГОСТ Р 53114-2008
Средство контроля эффективности защиты информации	Средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации.	ГОСТ Р 50922-2006
Средство обнаружения вторжений	Программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента ИБ	ГОСТ Р 53114-2008
Статус уязвимости	характеристика уязвимости, определяющая степень подтверждения факта существования уязвимости.	http://bdu.fstec.ru/ubi/terms/terms/index

Термин	Определение	Ссылка на документ
Степень опасности уязвимости	мера, сравнительная величина, характеризующая подверженность информационной системы уязвимостям, использование которых может привести к нарушению свойств безопасности информации	ГОСТ Р 56546-2015
Субъект доступа	лицо или процесс, действия которого регламентируются правилами разграничения доступа.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Техника защиты информации	Средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.	ГОСТ Р 50922-2006
Техническая защита информации (ТЗИ)	ЗИ, заключающаяся в обеспечении некриптографическими методами безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств	ГОСТ Р 50922-2006

Термин	Определение	Ссылка на документ
Технические средства информационной системы персональных данных (ТС)	средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Технический канал утечки информации (ТКУИ)	совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Техническое средство обеспечения ИБ	Оборудование, используемое для обеспечения ИБ организации некриптографическими методами	ГОСТ Р 53114-2008
Трассировка стека	процесс пошаговой обработки структур данных в том числе программного кода с целью выявления возможных ошибок уязвимостей, способных при их эксплуатации привести к нарушению безопасности информационной системы	http://bdu.fstec.ru/ubi/terms/terms/index
Требование по защите информации	Установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.	ГОСТ Р 50922-2006

Термин	Определение	Ссылка на документ
Угроза	возможная причина нежелательного инцидента, которая может нанести ущерб [информационной] системе или всей организации	ISO/IEC 27000:2014
Угроза безопасности информации	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации	ГОСТ Р 50922-2006, п.2.6.1 ГОСТ Р 56546-2015 ГОСТ Р 56545-2015
Угрозы безопасности персональных данных (УБПДн)	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.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Уничтожение персональных данных	действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Управление [риском]	меры, направленные на изменение риска.	ISO Guide 73:2009
Управление рисками	Координированные действия по направлению и контролю над деятельностью организации в связи с рисками	ГОСТ Р 53114-2008
Уровень опасности уязвимости	оценка опасности уязвимостей, определяемая на основе численного значения базовой оценки уязвимости. В банке данных в зависимости от значения базовой оценки уязвимости V используются следующие уровни опасности: ·низкий уровень, если $0,0 \leq V \leq 3,9$; средний уровень, если $4,0 \leq V \leq 6,9$; высокий уровень, если $7,0 \leq V \leq 9,9$; критический уровень, если $V = 10,0$.	http://bdu.fstec.ru/ubi/terms/terms/index

Термин	Определение	Ссылка на документ
Утечка (защищаемой) информации по техническим каналам	неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.	ФСТЭК Базовая модель угроз безопасности ПДн при из обработке в ИСПДн
Утечка информации	Неконтролируемое распространение защищаемой информации в результате ее разглашения, НСД к информации и получения защищаемой информации иностранными разведками	ГОСТ Р 53114-2008
Уязвимость	Свойство инф. системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации	ГОСТ Р 50922-2006, п.2.6.4 ГОСТ Р 56545-2015 ISO/IEC 27000:2014 ГОСТ Р 56546-2015
Уязвимость архитектуры	Уязвимость, появившаяся в процессе проектирования информационной системы.	ГОСТ Р 56546-2015
Уязвимость конфигурации	Уязвимость, появившаяся в процессе задания конфигурации (применения параметров настройки) программного обеспечения и технических средств информационной системы.	ГОСТ Р 56546-2015
Уязвимость многофакторная	Уязвимость, появившаяся в результате наличия нескольких недостатков различных типов.	ГОСТ Р 56546-2015
Уязвимость нулевого дня	уязвимость, которая становится известной до момента выпуска разработчиком программного обеспечения информационной системы мер защиты информации по ее устранению, исправлений ошибок или соответствующих обновлений	ФСТЭК России: МД от 11.02.2014 «Меры защиты информации в государственных информационных системах» ГОСТ Р 56545-2015

Термин	Определение	Ссылка на документ
Уязвимость организационная	Уязвимость, появившаяся в связи с отсутствием (или недостатками) организационных мер защиты информации в информационной системе и (или) несоблюдением правил эксплуатации системы защиты информации информационной системы, требований организационно-распорядительных документов по защите информации и (или) несвоевременном выполнении соответствующих действий должностным лицом (работником) или подразделением, ответственными за защиту информации.	ГОСТ Р 56546-2015
Уязвимость программного обеспечения	ошибка в программном обеспечении, способная напрямую быть использована хакером для получения доступа к системе или сети	http://bdu.fstec.ru/ubi/terms/terms/index
Фактор, воздействующий на защищаемую информацию	Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.	ГОСТ Р 50922-2006
Физическая защита информации	ЗИ путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты	ГОСТ Р 50922-2006
Целостность информации	состояние информации, при котором обеспечивается ее неизменность в условиях преднамеренного и или непреднамеренного воздействия на нее	Рекомендации по стандартизации Р 50.1.056-2005
Цель	требуемый для достижения результат	ISO/IEC 27000:2014
Цель защиты информации	Заранее намеченный результат защиты информации.	ГОСТ Р 50922-2006

Термин	Определение	Ссылка на документ
Цель информационной безопасности	Заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике ИБ	ГОСТ Р 53114-2008
Эффективность защиты информации	Степень соответствия результатов защиты информации цели защиты информации.	ГОСТ Р 50922-2006

2. ВИДЫ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ НА ОБЪЕКТАХ ЗАЩИТЫ

В руководящих документах ФСТЭК под объектами информатизации, аттестуемыми по требованиям безопасности информации, понимаются автоматизированные системы (АС) различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.

Защищаемыми объектами информатизации (объектами защиты) в соответствии со специальными требованиями и рекомендациями (СТР-К) по защите конфиденциальной информации ФСТЭК являются:

- средства и системы информатизации (средства вычислительной техники (СВТ), автоматизированные системы различного уровня и назначения на базе средств вычислительной техники), в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, 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, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации (ОТСС);
- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует) (ВТСС);
- защищаемые помещения.

Объектами защиты информациияв являются: информация или ее носитель, а также информационный процесс, которые необходимо защищать в соответствии с заданной целью защиты информации.

В статье 5, ФЗ "Об информации, информационных технологиях и защите информации" от 27.7.2006 г. № 149-ФЗ, изложено следующее: "Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)".

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную. Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской

Федерации "О государственной тайне". Перечень сведений, отнесенных к государственной тайне" опубликован в ст. 5 Закона РФ 1993 г. № 5485 "О государственной тайне". Существует три степени секретности такой информации:

- особой важности
- совершенно секретно
- секретно

В зависимости от порядка предоставления или распространения, информация подразделяется на:

1. информацию, свободно распространяемую;
2. информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3. информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
4. информацию, распространение которой в Российской Федерации ограничивается или запрещается.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации. К общедоступной также относится информация, доступ к которой нельзя ограничить. Примером может служить информация о состоянии окружающей среды, о деятельности органов государственной власти и органов местного самоуправления, документы, накапливаемые в открытых фондах библиотек и архивов. Так же в эту категорию можно отнести нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, правовое положение организаций и полномочия государственных органов, органов местного самоуправления.

Перечень сведений конфиденциального характера опубликован в Указе Президента РФ от 6.03.97 г. № 188 "Об утверждении перечня сведений конфиденциального характера". К видам конфиденциальной информации относятся следующие:

- персональные данные - сведения о фактах, событиях и обстоятельствах частой жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленном федеральными законами случаях;
- тайна следствия и судопроизводства - сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с ФЗ от 20 августа 2004 г. № 119-ФЗ и другими нормативными правовыми актами Российской Федерации;

- служебная тайна - служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
- профессиональная тайна - сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.);
- коммерческая тайна - сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
- сведения о сущности изобретения - сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

3. ВЫЯВЛЕНИЕ КРИТИЧЕСКИХ РЕСУРСОВ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Основой для разработки и проведения эффективных мероприятий по защите информации является выявление и учет факторов, воздействующих на защищаемую информацию.

Полнота и достоверность выявленных факторов, воздействующих на защищаемую информацию достигаются путем рассмотрения полного множества факторов, воздействующих на все элементы ОИ (технические и программные средства обработки информации, средства обеспечения ОИ и т.д.) и на всех этапах обработки информации.

Выявление факторов, воздействующих на защищаемую информацию, должно осуществляться с учетом следующих требований [1]:

- достаточности уровней классификации факторов, воздействующих на защищаемую информацию, позволяющих формировать их полное множество;
- гибкости классификации, позволяющей расширять множества классифицируемых факторов, группировок и признаков, а также вносить необходимые изменения без нарушения структуры классификации.

3.1 Классификация факторов, воздействующих на безопасность защищаемой информации, согласно ГОСТ 51275-2006

Факторы, воздействующие на критические свойства защищаемой информации, и подлежащие учету, по природе возникновения подразделяют на классы: объективные и субъективные.

По отношению к объекту информатизации факторы, воздействующие на безопасность защищаемой информации, подразделяют на внутренние и внешние.

Факторы, воздействующие на безопасность защищаемой информации, подразделяют на подклассы; группы; подгруппы; виды; подвиды.

Далее представлен перечень объективных и субъективных факторов, воздействующих на безопасность защищаемой информации.

3.1.1 Перечень объективных факторов, воздействующих на безопасность защищаемой информации

3.1.1.1 Внутренние факторы

Передача сигналов:

а) по проводным линиям связи;

б) по оптико-волоконным линиям связи;

в) в диапазоне радиоволн и в оптическом диапазоне длин волн.

Излучения сигналов, функционально присущие техническим средствам (ТС) (устройствам) объекта информатизации:

а) излучения акустических сигналов:

- сопутствующие работе технических средств обработки и передачи информации (ТС ОПИ);
- сопутствующие произносимой или воспроизводимой ТС речи;

б) электромагнитные излучения и поля в радиодиапазоне или в оптическом диапазоне.

Побочные электромагнитные излучения:

а) элементов (устройств) ТС ОПИ;

б) на частотах работы высокочастотных генераторов устройств, входящих в состав ТС ОПИ:

- модуляция побочных электромагнитных излучений информативным сигналом, сопровождающим работу ТС ОПИ;
- модуляция побочных электромагнитных излучений акустическим сигналом, сопровождающим работу ТО ОПИ;

в) на частотах самовозбуждения усилителей, входящих в состав ТС ОПИ.

Паразитное электромагнитное излучение:

а) модуляция паразитного электромагнитного излучения информационными сигналами;

б) модуляция паразитного электромагнитного излучения акустическими сигналами.

Наводка:

а) в электрических цепях ТС, имеющих выход за пределы ОИ;

б) в линиях связи:
- вызванная побочными и/или паразитными электромагнитными излучениями, несущими информацию;
- вызванная внутренними емкостными и/или индуктивными связями;

в) в цепях электропитания:
- вызванная побочными и/или паразитными электромагнитными излучениями, несущими информацию;
- вызванная внутренними емкостными и/или индуктивными связями;
- через блоки питания ТС ОИ;

г) в цепях заземления:
- вызванная побочными и/или паразитными электромагнитными излучениями, несущими информацию;
- вызванная внутренними емкостными и/или индуктивными связями;
- обусловленная гальванической связью схемной (рабочей) "земли" узлов и блоков ТС ОИ;

д) в технических средствах, проводах, кабелях и иных токопроводящих коммуникациях и конструкциях, гальванически не связанных с ТС ОИ, вызванная побочными и /или паразитными электромагнитными излучениями, несущими информацию.

Наличие акустоэлектрических преобразователей в элементах ТС ОИ.

Дефекты, сбои и отказы, аварии ТС и систем ОИ.

Дефекты, сбои и отказы программного обеспечения ОИ.

3.1.1.2 Внешние факторы

Явления техногенного характера:

а) непреднамеренные электромагнитные облучения ОИ;

б) радиационные облучения ОИ;

в) сбои, отказы и аварии систем обеспечения ОИ.

Природные явления, стихийные бедствия:

а) термические факторы (пожары и т.д.);

б) климатические факторы (наводнения и т.д.);

в) механические факторы (землетрясения и т.д.);

г) электромагнитные факторы (грозовые разряды и т.д.);

д) биологические факторы (микробы, грызуны и т.д.);

е) химические факторы (химически агрессивные среды и т.д.).

3.1.2 Перечень субъективных факторов, воздействующих на безопасность защищаемой информации

3.1.2.1 Внутренние факторы

Разглашение защищаемой информации лицами, имеющими к ней право доступа, через:

а) лиц, не имеющих права доступа к защищаемой информации;

б) передачу информации по открытым линиям связи;

в) обработку информации на незащищенных ТС обработки информации;

г) опубликование информации в открытой печати и других средствах массовой информации;

д) копирование информации на незарегистрированный носитель информации;

е) передачу носителя информации лицам, не имеющим права доступа к ней;

ж) утрату носителя информации.

Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации, путем:

а) несанкционированного изменения информации;

б) несанкционированного копирования защищаемой информации.

Несанкционированный доступ к информации путем:

в) подключения к техническим средствам и системам ОИ;

г) использования закладочных средств [устройств];

д) использования программного обеспечения технических средств ОИ через:

- маскировку под зарегистрированного пользователя;
- дефекты и уязвимости программного обеспечения ОИ;
- внесение программных закладок;
- применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

е) хищения носителя защищаемой информации;

ж) нарушения функционирования ТС обработки информации.

Недостатки организационного обеспечения защиты информации при:

а) задании требований по защите информации (требования противоречивы, не обеспечивают эффективную защиту информации и т.д.);

б) несоблюдении требований по защите информации;

в) контроле эффективности защиты информации.

Ошибки обслуживающего персонала ОИ при эксплуатации технических, программных средств; а также средств и систем защиты информации.

3.1.2.2 Внешние факторы

Доступ к защищаемой информации с применением технических средств:

а) разведки:
- радиоэлектронной;
- оптико-электронной;
- фотографической;
- визуально-оптической;
- акустической;
- гидроакустической;
- технической компьютерной;

б) съема информации.

Несанкционированный доступ к защищаемой информации путем:

а) подключения к техническим средствам и системам ОИ;

б) использования закладочных средств [устройств];

в) использования программного обеспечения технических средств ОИ через:
- маскировку под зарегистрированного пользователя;
- дефекты и уязвимости программного обеспечения ОИ;
- внесение программных закладок;
- применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

г) несанкционированного физического доступа к ОИ;

д) хищения носителя информации.

Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.

Действия криминальных групп и отдельных преступных субъектов:

а) диверсия в отношении ОИ;

б) диверсия в отношении элементов ОИ.

Искажение, уничтожение или блокирование информации с применением технических средств путем:

а) преднамеренного силового электромагнитного воздействия;
- по сети электропитания на порты электропитания постоянного и переменного тока;
- по проводным линиям связи на порты ввода-вывода сигналов и порты связи;

- по металлоконструкциям на порты заземления и порты корпуса;
- посредством электромагнитного быстроизменяющегося поля на порты корпуса, порты ввода-вывода сигналов и порты связи;

б) преднамеренного силового воздействия различной физической природы;

в) использования программных или программно-аппаратных средств при осуществлении компьютерной или сетевой атаки.

г) воздействия программными средствами в комплексе с преднамеренным силовым электромагнитным воздействием.

4. КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Классификация, согласно [4], распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД.

Необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

• наличие в АС информации различного уровня конфиденциальности;

• уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

• режим обработки данных в АС: коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса-2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Согласно руководящему документу ФСТЭК России [4] (РД СВТ. Защита от НСД. Показатели защищенности от НСД. Классы СВТ.

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

СВТ классифицируются в соответствии с Руководящим документом Гостехкомиссиии России "СВТ. Защита от НСД к информации. Показатели защищенности от НСД".

Руководящий документ устанавливает классификацию средств вычислительной техники по уровню защищённости от НСД к информации на базе перечня показателей защищённости и совокупности описывающих их требований.

Установленны 7 классов защищённости СВТ от НСД к информации, при этом самый низкий класс – седьмой, самый высокий – первый. Каждый класс разбит на 4 группы:

• I. 7 класс – СВТ, которые были представлены к оценке, однако не удовлетворяют требованиям более высоких классов.

• II. 6 и 5 классы – дискреционная защита.

• III. 4, 3 и 2 классы – мандатная защита.

• IV. 1 класс – верифицированная защита.

Требования ужесточаются с уменьшением номера класса.

Классы являются иерархически упорядоченными: каждый последующий класс содержит требования всех предыдущих. Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

В общем случае требования предъявляются к следующим показателям защищённости:

• Дискреционный принцип контроля доступа.

• Мандатный принцип контроля доступа.

• Очистка памяти.

• Изоляция модулей.

• Маркировка документов.

5. КАТЕГОРИРОВАНИЕ РЕСУРСОВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Категорирование ресурсов автоматизированных систем, подлежащих защите, предполагает:

- установление категорий важности обеспечения защиты ресурсов;
- отнесение конкретных ресурсов к соответствующим категориям.

Основными целями категорирования ресурсов (определение требований к защите ресурсов) автоматизированных систем являются:

- создание нормативно-методической основы для дифференцированного подхода к защите ресурсов автоматизированных систем на основе их классификации по степени риска в случае нарушения свойств безопасности информации;
- типизацию принимаемых контрмер и распределения физических и аппаратно-программных средств зашиты по компьютерам автоматизированной ситемы и унификацию и настроек защитных механизмов.

Основанием для предоставления должностным лицам определенных полномочий к информационным ресурсам с указанием типов разрешенных доступов являются заявки на должностных лиц отделов и служб, допущенных к защищаемым ресурсам объекта информатизации, которые утверждаются руководителем.

Инициаторами категорирования средств вычислительной техники и получения соответствующих предписаний на использование ПЭВМ выступают руководители подразделений учреждения, в которых используются данные ПЭВМ.

Доступ должностных лиц отделов и служб, допущенных к защищаемым ресурсам объекта информатизации, оформляется в виде формы, приведенной в табл. 2.

Таблица 1

Доступ должностных лиц к защищаемым ресурсам объекта информатизации

Фамилия и инициалы должностного лица	Защищаемые ресурсы				
	полное наименование ресурса	условное наименование ресурса	разрешенные виды доступа к ресурсу		
			чтение	запись	запуск

Категорирование ресурсов автоматизированной системы проводится на основе их инвентаризации и предполагает составление и последующее ведение перечней ресурсов АС, подлежащих защите.

В каждой автоматизированной системе разрабатывается документ «Перечень защищаемых ресурсов на объекте информатизации».

Ответственность за составление и ведение перечней защищаемых ресурсов объекта информатизации возлагается на подразделения сопровождения и эксплуатации программного обеспечения, подразделения автоматизации, связи и защиты информации в автоматизированных системах организации:

Перечни разрабатываются в процессе анализа решаемых в интересах подразделений функциональных задач, состава автоматизированных рабочих мест, организуемых банков данных, возможностей и режимов использования программных средств, а также средств, обеспечивающих обмен информацией между объектами автоматизированных систем.

Категории конфиденциальности защищаемой информации:

• «строго конфиденциальная» - информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства (коммерческая и банковская тайны, персональные данные), а также информация, ограничения на распространение которой введены решениями руководства организации, разглашение которой может привести к тяжким финансово-экономическим последствиям для организации вплоть до банкротства (нанесению тяжкого ущерба жизненно важным интересам его клиентов, корреспондентов, партнеров или сотрудников);

• «конфиденциальная» - информация, не отнесенная к категории «строго конфиденциальная», ограничения на распространение которой вводятся решением руководства организации, разглашение которой может привести к

значительным убыткам и потере конкурентоспособности организации (нанесению ощутимого ущерба интересам его клиентов, корреспондентов, партнеров или сотрудников);

«открытая» - информация, обеспечения конфиденциальности которой не требуется.

Категории целостности защищаемой информации:

• «высокая» - информация, несанкционированная модификация или фальсификация которой может привести к нанесению значительного прямого ущерба организации, ее клиентам и корреспондентам, целостность и аутентичность которой должна обеспечиваться гарантированными методами в соответствии с обязательными требованиями действующего законодательства, приказов, директив и других нормативных актов;

• «низкая» - информация, несанкционированная модификация, подмена или удаление которой может привести к нанесению незначительного косвенного ущерба организации, целостность (а при необходимости и аутентичность) которой должна обеспечиваться в соответствии с решением руководства организации (методами подсчета контрольных сумм, хеш-функций и т.п.);

• «нет требований» информация, к обеспечению целостности (и аутентичности) которой требований не предъявляется.

Категории функциональных задач:

В зависимости от периодичности решения функциональных задач и максимально допустимой задержки получения результатов их решения вводится четыре требуемых степени (категории) доступности функциональных задач.

• «беспрепятственная доступность» – доступ к задаче должен обеспечиваться в любое время (задача решается постоянно, задержка получения результата не должна превышать нескольких секунд или минут);

• «высокая доступность» – доступ к задаче должен осуществляться без существенных временных задержек (задача решается ежедневно, задержка получения результата не должна превышать нескольких часов);

• «средняя доступность» – доступ к задаче может обеспечиваться с существенными временными задержками (задача решается раз в несколько дней, задержка получения результата не должна превышать нескольких дней);

• «низкая доступность» – временные задержки при доступе к задаче практически не лимитированы (задача решается с периодом в несколько недель или месяцев, допустимая задержка получения результата - несколько недель).

В перечнях защищаемых ресурсов указываются сведения о допуске к этим ресурсам соответствующих подразделений или должностных лиц.

Примерная форма Перечня защищаемых ресурсов на объекте представлена в табл. 3

Таблица 2

Перечень защищаемых ресурсов на объекте информатизации

№ п/п	Защищаемый ресурс			К ресурсу допущены
	полное наименование	условное наименование	категория доступа	

6. ФОРМИРОВАНИЕ ПЕРЕЧНЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ, ПОДЛЕЖАЩИХ ЗАЩИТЕ

Перечень информационных ресурсов, подлежащих защите составляется согласно нижеперечисленному порядку действий:

1. Выявление и описание всех функциональных задач, решаемых с использованием автоматизированных систем, а также всех видов информации, используемых при решении текущих задач в подразделениях.

2. Составление общий перечень функциональных задач. При этом следует учесть, что одна и та же задача в разных подразделениях может называться по-разному, и наоборот, различные задачи могут иметь одно и то же название. Одновременно с этим вести учет программных средств, используемых при решении функциональных задач подразделения.

3. Выявление в процессе обследовании подсистем и анализе задач всех видов входящей, исходящей, хранимой, обрабатываемой информации; выявление конфиденциальной информации, а также информации, подлежащей защите в силу того, что нарушение ее критических свойств приведет к ощутимому ущербу организации.

4. Оценка серьезности последствий нарушения таких свойств информации, как конфиденциальность и целостность. В случае невозможности количественной оценки вероятного ущерба производится его качественная оценка (такими категориями, как низкая, средняя, высокая, очень высокая).

5. Выявление периодичности решения функциональных задач, максимально допустимого времени задержки получения результатов и степени серьезности последствий, при блокировании решения задач. В случае невозможности количественной оценки вероятного ущерба произвести качественную оценку.

6. Определение видов конфиденциальной информации: банковская, коммерческая, персональные данные, не составляющая тайны.

7. Категорирование всех специальных функциональных задач, решаемых в подразделениях с использованием автоматизированных систем

(выполняется на основе требований по доступности информации, предъявляемых руководителями подразделений организации).

8. Уточнение состава информационных и программных ресурсов задач каждой группы пользователей; указания по настройке применяемых при их решении средств защиты (указание полномочий доступа групп пользователей к перечисленным ресурсам).

Выявленные сведения будут использоваться в качестве эталона настроек средств защиты рабочих станций, на которых будет решаться данная задача, и для контроля правильности их установки.

9. Категорирование рабочих станций устанавливается, исходя из максимальной категории специальных задач, решаемых на рабочих станциях, и максимальных категорий конфиденциальности и целостности информации, используемой при решении задач.

10. Определение типовых конфигураций мер и защитных механизмов программно-аппаратных средств защиты информации для рабочих станций различных категорий (согласно таблице 4).

Полученные в результате категорирования РС и задач средств являются неотъемлемой составной частью плана защиты АС организации и Политики безопасности организации.

7. ПОРЯДОК ОПРЕДЕЛЕНИЯ ТРЕБОВАНИЙ К ЗАЩИЩЁННОСТИ ИНФОРМАЦИИ

1) Составить перечень типов информационных ресурсов. Для этого, учитывая предметную область системы, разделить данные на типы по следующим признакам: тематике, функциональному назначению, сходности технологии обработки и т. д. Впоследствии это разбиение данных может быть дополнено с учетом требований к их защищенности.

2) Для каждого типа данных, выделенного на первом шаге, и с учетом критического свойства информации (доступности, целостности, конфиденциальности) определить:

- перечень и важность субъектов, интересы которых затрагиваются при нарушении данного свойства информации;
- уровень наносимого им при этом ущерба (незначительный, малый, средний, большой, очень большой и т. п.)
- соответствующий уровень требований к защищенности.

Классификация конфиденциальности информации (по грифам секретности и категориям) производится на основании приказов, руководств и других документов, определяющих ограничения на доступ к информации определенного грифа секретности или определенной тематики. Признаком для ограничения доступа к сведениям могут быть также должностные обязанности допущенных лиц.

Первичными данными для проведения классификации информации являются:

- уровень звена управления, для которого проектируется система защиты;
- организационно-штатная структура организации с перечнем должностных лиц и подразделений, в интересах которых будет функционировать СЗИ;
- функциональные задачи, которые предполагается решать в АС в интересах подразделений и должностных лиц;
- архитектура АС;
- для определения уровня наносимого ущерба стоит учесть:
  - ✓ стоимость возможных потерь при получении информации противником;
  - ✓ стоимость восстановления информации при ее утрате;
  - ✓ затраты на восстановление нормального процесса функционирования АС.

3) Для каждого типа информационных пакетов с учетом значимости

субъектов и уровней наносимого им ущерба установить степень необходимой защищенности (низкая, средняя, высокая, требования не предъявляются) по каждому из свойств информации (при равенстве значимости субъектов следует выбрать максимальное значение уровня).

Пример оценки требований к защищенности некоторого типа информационных субъектов приведен в табл. 1

Таблица 3

Оценка требований к защищенности
информационных ресурсов АС

Субъекты	Уровень ущерба по свойствам информации		
	конфиденциальность	целостность	доступность
№ 1	Нет	Средняя	Средняя
№2	Высокая	Средняя	Средняя
№3	Низкая	Низкая	Низкая
В итоге	Высокая	Средняя	Средняя

8. ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ К МЕРАМ И НАСТРОЙКАМ ЗАЩИТНЫХ МЕХАНИЗМОВ СЗИ

В результате анализа объекта информатизации, категорирования ресурсов АС, следует определить требования к применяемым мерам и настройкам защитных механизмов средств защиты на рабочих станциях АС организации различных категорий.

Требования по защите информации от несанкционированного доступа для автоматизированных систем [4].

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

В зависимости от класса АС в рамках этих подсистем должны быть реализованы требования

8.1 Требования к автоматизированным системам третьей группы

8.1.1 Требования к классу защищенности 3Б

подсистема управления доступом:

должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия, длиной не менее шести символов.

подсистема регистрации и учета:

• должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова.

• Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы;

должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки с занесением учетных данных в журнал (учетную карточку).

подсистема обеспечения целостности:

• должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды , при этом:

• целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ, целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

8.1.2 Требования к классу защищенности 3А

подсистема управления доступом:

должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести символов.

подсистема регистрации и учета:

• должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова.

Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы, результат попытки входа: успешный или неуспешный (при НСД);

• должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

время и дата выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности, спецификация устройства выдачи (логическое имя/номер внешнего устройства);

• должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки, должно проводиться несколько видов учета (дублирующих) с регистрацией выдачи/приема носителей информации;

• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

подсистема обеспечения целостности:

• должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды, при этом:

• целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ, целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;

должны использоваться сертифицированные средства защиты.

Их сертификация проводится специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации средств защиты СЗИ НСД.

8.2 Требования к автоматизированным системам второй группы

8.2.1 Требования к классу защищенности 2Б

подсистема управления доступом:

• должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести символов.

подсистема регистрации и учета:

• должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова.

• Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы, результат попытки входа: успешный или неуспешный (при НСД);

• должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и занесением учетных данных в журнал (карточку).

подсистема обеспечения целостности:

• должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды, при этом:

• целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ, целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;

• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест -программ, имитирующих попытки НСД;

• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

8.2.2 Требования к классу защищенности 2А

подсистема управления доступом:

• должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести символов;

• должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по их логическим адресам (номерам);

• должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

• должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.

подсистема регистрации и учета:

• должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова.

• Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы, результат попытки входа: успешный или неуспешный (при НСД), идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

• должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

время и дата выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя/номер внешнего устройства), краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ;

• должна осуществляться регистрация запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный - несанкционированный);

• должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная,

идентификатор субъекта доступа, спецификация защищаемого файла;

• должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная, идентификатор субъекта доступа, спецификация защищаемого объекта (логическое имя/номер);

• должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

• должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки, учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи/приема, должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

криптографическая подсистема:

• должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа.

При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

• доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;

• должны использоваться сертифицированные средства криптографической защиты. Их сертификация проводится специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации криптографических средств защиты.

подсистема обеспечения целостности:

• должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды , при этом:

целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ, целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

• должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД;

• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;

• должны использоваться сертифицированные средства защиты.

Их сертификация проводится специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации средств защиты СЗИ НСД.

8.3 Требования к автоматизированным системам первой группы

8.3.1 Требования к классу защищенности 1Д

подсистема управления доступом:

• должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести символов.

подсистема регистрации и учета:

• должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова.

• Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы, результат попытки входа: успешный или неуспешный - несанкционированный, идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

• должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки, учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи/приема.

подсистема обеспечения целостности:

• должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды , при этом:

целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ, целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

8.3.2 Требования к классу защищенности 1Г

подсистема управления доступом:

• должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести символов;

• должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;

• должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

• должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

подсистема регистрации и учета:

• должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова.

• Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы, результат попытки входа: успешный или неуспешный - несанкционированный,

идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;

• должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются:

время и дата выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя/номер внешнего устройства), краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ, должна осуществляться регистрация запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный - несанкционированный);

• должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная, идентификатор субъекта доступа, спецификация защищаемого файла;

• должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная, идентификатор субъекта доступа, спецификация защищаемого объекта (логическое имя/номер);

• должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки, учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи/приема;

• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);

подсистема обеспечения целостности:

• должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды , при этом:

целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ, целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

• должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

8.3.3 Требования к классу защищенности 1В

подсистема управления доступом:

• должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

• должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и/или адресам;

• должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

• должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

• должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

подсистема регистрации и учета:

• должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова.

• Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы, результат попытки входа: успешный или неуспешный - несанкционированный, идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;

• должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

время и дата выдачи (обращение к подсистеме вывода), спецификация устройства выдачи (логическое имя/номер внешнего устройства), краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ, объем фактически выданного документа (количество страниц, листов, копий) и результат (успешный, неуспешный);

• должна осуществляться регистрация запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный - несанкционированный);

• должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная, идентификатор субъекта доступа, спецификация защищаемого файла, имя программы (процесса, задания, задачи), осуществляющей доступ к файлу, вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

• должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная, идентификатор субъекта доступа, спецификация защищаемого объекта (логическое имя/номер), имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту, вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

• должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

дата и время изменения полномочий, идентификатор субъекта доступа (администратора), осуществившего изменения;

• должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

• должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки, учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи/приема, должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

• должна осуществляться сигнализация попыток нарушения защиты.

подсистема обеспечения целостности:

• должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды , при этом:

целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ, целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации;

• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

• должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

• должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год;

• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;

• должны использоваться сертифицированные средства защиты.

Их сертификация проводится специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации средств защиты СЗИ НСД.

8.3.4 Требования к классу защищенности 1Б

подсистема управления доступом:

• должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми символов.

• должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам);

• должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

• должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

• должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

подсистема регистрации и учета:

• должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы , либо регистрация загрузки и инициализации операционной системы и ее программного останова.

• Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы, результат попытки входа: успешный или неуспешный - несанкционированный, идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;

• должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа - фактически выданного количества листов в графе брака). В параметрах регистрации указываются:

время и дата выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя/номер внешнего устройства), краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ, объем фактически выданного документа (количество страниц, листов, копий) и результат: успешный, неуспешный;

• должна осуществляться регистрация запуска/завершения всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:

дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный - несанкционированный), должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная, идентификатор субъекта доступа, спецификация защищаемого файла, имя программы (процесса, задания, задачи), осуществляющей доступ к файлу, вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

• должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная, идентификатор субъекта доступа, спецификация защищаемого объекта (логическое имя/номер), имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту, вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

• должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

дата и время изменения полномочий, идентификатор субъекта доступа (администратора), осуществившего изменения, идентификатор субъекта, у которого проведено изменение полномочий и вид изменения (пароль, код, профиль и т.п.), спецификация объекта, у которого проведено изменение статуса защиты и вид изменения (код защиты, уровень конфиденциальности);

• должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

• должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки, учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи/приема, должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

• должна осуществляться сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

криптографическая подсистема:

• должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные портативные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

• доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;

• должны использоваться сертифицированные средства криптографической защиты. Их сертификация проводится специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации криптографических средств защиты.

подсистема обеспечения целостности:

• должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды , при этом:

целостность СЗИ НСД проверяется по контрольным суммам всех компонент СЗИ как в процессе загрузки, так и динамически в процессе работы АС, целостность программной среды обеспечивается качеством приемки программных средств в АС, предназначенных для обработки защищенных файлов;

• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

• должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

• должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;

• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также оперативное восстановление функций СЗИ НСД при сбоях;

• должны использоваться сертифицированные средства защиты.

Их сертификация проводится специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации средств защиты СЗИ НСД.

8.3.5 Требования к классу защищенности 1А

подсистема управления доступом:

• должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия длиной не менее восьми буквенно-цифровых символов.

• должна осуществляться аппаратурная идентификация и проверка подлинности терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по уникальным встроенным устройствам;

• должна осуществляться идентификация и проверка подлинности программ, томов, каталогов, файлов, записей, полей записей по именам и контрольным суммам (паролям, ключам);

• должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

• должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

подсистема регистрации и учета:

• должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова.

• Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы, результат попытки входа: успешный или неуспешный - несанкционированный,

идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;

• должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа - фактически выданного количества листов в графе брака). В параметрах регистрации указываются:

время и дата выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя/номер внешнего устройства), краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ, объем фактически выданного документа (количество страниц, листов, копий) и результат (успешный, неуспешный);

• должна осуществляться регистрация запуска/завершения всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:

дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный - несанкционированный), полная спецификация соответствующего файла "образа" программы (процесса, задания) - устройство (том, каталог), имя файла (расширение);

• должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная, идентификатор субъекта доступа, спецификация защищаемого файла, имя программы (процесса, задания, задачи), осуществляющей доступ к файлу, вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

• должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная, идентификатор субъекта доступа, спецификация защищаемого объекта (логическое имя/номер), имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту, вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

• должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

дата и время изменения полномочий и статуса, идентификатор субъекта доступа (администратора), осуществившего изменения, идентификатор субъекта доступа, у которого изменены полномочия и вид изменений (пароль, код, профиль и т.п.), спецификация объекта, у которого изменен статус защиты, и вид изменения (код защиты, уровень конфиденциальности);

• должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

• должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки, учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи/приема, должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

• должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, в которой содержалась защищаемая информация;

• должна осуществляться надежная сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

криптографическая подсистема:

• должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на любые съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться автоматическая очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

• должны использоваться разные криптографические ключи для шифрования информации, принадлежащей различным субъектам доступа (группам субъектов);

• доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;

• должны использоваться сертифицированные средства криптографической защиты. Их сертификация проводится специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации криптографических средств защиты.

подсистема обеспечения целостности:

• должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды , при этом:

целостность СЗИ НСД проверяется по имитовставкам алгоритма ГОСТ 28147-89 или по контрольным суммам другого аттестованного алгоритма всех компонент СЗИ как в процессе загрузки, так и динамически в процессе функционирования АС, целостность программной среды обеспечивается качеством приемки любых программных средств в АС;

• должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

• должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

• должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;

• должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также автоматическое оперативное восстановление функций СЗИ НСД при сбоях;

• должны использоваться сертифицированные средства защиты.

Их сертификация проводится специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации средств защиты СЗИ НСД.

Организационные мероприятия в рамках СЗИ НСД в АС, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.

При обработке или хранении в АС информации, не отнесенной к категории секретной, в рамках СЗИ НСД государственным, коллективным, частным и совместным предприятиям, а также частным лицам рекомендуются следующие организационные мероприятия:

• выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;

• определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;

• установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;

• ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;

• получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;

• обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;

• выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;

• организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;

• разработка СЗИ НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;

• осуществление приемки СЗИ НСД в составе АС.

Составляется матрица мер защиты для каждого из критичных свойств информации по категориям (табл. 5), в которой используются данные из таблицы 4. Стандартные рекомендуемые меры и защитные механизмы приведены в перечне ниже.

Таблица 5

Требования к применяемым мерам и настройкам защитных механизмов средств защиты на рабочих станциях АС

	конфиденциальность информации			целостность информации			доступность информации			
	строго конфиденциальная	конфиденциальная	открытая	высокая	низкая	нет требований	высокая доступность	средняя доступность	низкая доступность	беспрепятственная доступность
Применяемые меры и защитные механизмы	Варианты применения мер защиты (1 – 5), согласно таблице 4									

Таблица 4

Варианты применяемых мер и настроек защитных механизмов средств защиты на рабочих станциях АС организации

Применяемые меры и защитные механизмы	Варианты принимаемых мер или настроек защитных механизмов				
	1	2	3	4	5
Меры физической защиты					
Расположение в охраняемом помещении с кодовым замком и сигнализацией	Обязательно	Желательно	Нет требований		
Обеспечение физической целостности технических средств РС	Обязательно (опечатывание системных блоков)	Желательно (опечатывание системных блоков)	Нет требований		
Организационные меры защиты					
Состав программных средств на РС	Строго ограничен в соответствии с задачами РС	Не ограничен			
Наличие диагностических программных средств на РС	Запрещено	Разрешено. Доступны отдельным пользователям	Разрешено использовать всем		
Наличие и использование инструментальных средств создания и отладки программ на РС	Запрещено	Разрешено отдельным пользователям	Разрешено всем		

Применяемые меры и защитные механизмы	Варианты принимаемых мер или настроек защитных механизмов				
	1	2	3	4	5
Ограничения на совмещение задач на одной РС	РС участвует в решении задач только одной подсистемы	РС участвует в решении задач в составе ограниченного числа подсистем	Ограничений нет		
Ограничение числа пользователей РС	Один конечный пользователь РС	Допускается работа нескольких пользователей	Число пользователей РС не ограничено		
Анализ отказов и других нештатных ситуаций при работе РС, а также техническое обслуживание программных и аппаратных средств РС	Производится специальным персоналом и только в присутствии администратора безопасности (СЗИ НСД)	Производится специальным персоналом в присутствии ответственного за безопасность в подразделении. Обязательное оповещение администратора безопасности (в установленный срок). Вызов администратора безопасности при необходимости.	Производится специальным персоналом. Присутствие или извещение специалистов службы защиты информации не требуется		

Применяемые меры и защитные механизмы	Варианты принимаемых мер или настроек защитных механизмов				
	1	2	3	4	5
Применение аппаратно-программных средств защиты					
Именование (идентификация) пользователей	Единственное уникальное имя для каждого сотрудника	Возможно наличие нескольких уникальных имен у одного сотрудника	Возможно использование групповых имен		
Наличие паролей у пользователей	Обязательно для всех пользователей РС	Для некоторых пользователей РС может быть разрешен вход без пароля			
Указание имени основного пользователя РС по умолчанию	Запрещено	Разрешено	Нет требований		
Аппаратная поддержка средств защиты рабочих станций	Обязательно, с использованием Touch Memory, Smart Card и т.п.	Обязательно. Возможно с использованием Touch Memory, Smart Card и т.п.	Обязательно. Без поддержки Touch Memory, Smart Card и т.п.	Использование возможностей BIOS компьютера	Не требуется
Жесткий режим входа пользователей (только по предъявлении Touch Memory, Smart Card и т.п.)	Обязательно	Желательно (возможно)	Не требуется		

Применяемые меры и защитные механизмы	Варианты принимаемых мер или настроек защитных механизмов				
	1	2	3	4	5
Избирательное разграничение доступа к ресурсам рабочей станции	Минимально необходимый доступ всех пользователей к ресурсам РС	Ограничение по доступу пользователей к отдельным ресурсам РС	Все пользователи имеют полный доступ ко всем ресурсам		
Полномочное управление доступом к ресурсам	Обязательно	Желательно (возможно)	Не требуется		
Ограничения по запуску программ (замкнутая программная среда)	Обязательно для всех пользователей РС	Для некоторых пользователей РС	Не устанавливается		
Ограничения на использование устройств (НГМД, локального принтера, COM-портов)	Обязательно для всех пользователей	Для некоторых пользователей РС	Не устанавливается		
Режим регистрация событий в системном журнале	Максимально подробный для локальных и сетевых событий	Максимально подробный для локальных и минимальный для сетевых событий	Максимально подробный для сетевых и минимальный для локальных событий	Минимальный для локальных и сетевых событий	Не установлен
Хранение журналов регистрации событий	Долгосрочное (свыше трех месяцев)	Среднесрочное (до трех месяцев)	Краткосрочное (до 7 дней)	Нет	

Применяемые меры и защитные механизмы	Варианты принимаемых мер или настроек защитных механизмов				
	1	2	3	4	5
Периодичность анализа журналов регистрации событий	Ежедневный экспресс анализ	Еженедельный анализ	Анализ по необходимости	Нет требований	
Оперативный контроль за работой пользователей (за попытками НСД)	Постоянный	Периодический	По мере необходимости	Нет требований	
Использование режима затирания удаляемых файлов	Обязательно	Возможно	Не требуется		
Контроль целостности программ системы защиты и системных областей дисков	При каждой перезагрузке и с установленной периодичностью	При каждой перезагрузке	Один раз в день (при первой перезагрузке)	По требованию администратора (пользователя)	Не проводится
Применяемые методы и средства контроля целостности (и аутентичности)	Гарантированных методы контроля (ЭЦП)	Стойкие негарантированные методы (хэш-функция, имитовставка)	Нестойкие негарантированные методы (контрольное суммирование, CRC и т.п.)	Не требуется	
Контроль целостности особых файлов (программ, конфигураций и т.п.)	При каждой перезагрузке и с установленной периодичностью	При каждой перезагрузке	Один раз в день (при первой перезагрузке)	По требованию администратора (пользователя)	Не проводится

Применяемые меры и защитные механизмы	Варианты принимаемых мер или настроек защитных механизмов				
	1	2	3	4	5
Действия при обнаружении нарушений целостности программ, файлов, системных областей диска	Регистрация в системном журнале и блокировка работы РС, снять которую может только администратор безопасности	Только регистрация в системном журнале	Не предусмотрены		
Применение средств шифрования – расшифрования данных	Обязательно для обмена и хранения указанных типов данных	Обязательно для обмена указанными типами данных (файлами)	Возможно для некоторых файлов по решению пользователя	Не требуется	
Возможность удаленного контроля и управления РС	Запрещено	Обязательно	Разрешено (не обязательно)	Не требуется	
Обеспечение живучести РС					
Резервирование технических средств	Горячее резервирование (t < 5 мин)	Холодное резервирование (t < 30 мин)	Групповой резерв (t < 3 час)	Не требуется	
Резервное (страховое) копирование критичных данных	Автоматическое с периодом < 10 мин	Автоматическое с периодом < 1 часа	Ручное с периодом < 24 час	Ручное с периодом > 24 час	Не требуется

Применяемые меры и защитные механизмы	Варианты принимаемых мер или настроек защитных механизмов				
	1	2	3	4	5
Организация защиты от утечки по техническим каналам					
Проведение спецпроверок и специсследованийСВТ	Обязательно	Желательно	Нет требований		
Применение генераторов помех	Обязательно	Желательно	Нет требований		
Расположение, исключающее визуальный просмотр экрана посторонними	Обязательно	Желательно	Нет требований		

Перечень рекомендуемых к применению мер и защитных механизмов

1. Расположение в охраняемом помещении с кодовым замком и сигнализацией.
2. Обеспечение физической целостности технических средств РС.
3. Состав программных средств на РС.
4. Наличие диагностических программных средств на РС.
5. Наличие и использование инструментальных средств создания и отладки программ на РС.
6. Ограничения на совмещение задач на одной РС.
7. Ограничение числа пользователей РС.
8. Анализ отказов и других нештатных ситуаций при работе РС, а также техническое обслуживание программных и аппаратных средств РС.
9. Именование (идентификация) пользователей.
10. Наличие паролей у пользователей.
11. Указание имени основного пользователя РС по умолчанию.
12. Аппаратная поддержка средств защиты рабочих станций.
13. Жесткий режим входа пользователей (только по предъявлении Touch Memory, Smart Card и т.п.).
14. Избирательное разграничение доступа к ресурсам рабочей станции.
15. Полномочное управление доступом к ресурсам.
16. Ограничения по запуску программ (замкнутая программная среда).
17. Ограничения на использование отдельных устройств (НГМД, принтера, COM-портов).
18. Режим регистрация событий в системном журнале.
19. Хранение журналов регистрации событий.
20. Периодичность анализа журналов регистрации событий.
21. Оперативный контроль за работой пользователей (за попытками НСД).
22. Использование режима затирания удаляемых файлов.
23. Контроль целостности программ системы защиты и системных областей дисков.
24. Применяемые методы и средства контроля целостности (и аутентичности).
25. Контроль целостности особых файлов (программ, конфигураций).
26. Действия при обнаружении нарушений целостности программ, файлов, системных областей диска.
27. Применение средств шифрования -расшифрования данных.
28. Возможность удаленного контроля и управления рабочей станцией.
29. Резервирование технических средств.
30. Резервное (страховое) копирование критичных данных.
31. Проведение спецпроверок и специсследований СВТ.
32. Применение генераторов помех.
33. Расположение, исключающее визуальный просмотр экрана посторонними.

ЗАДАНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Для конкретного объекта информатизации (автоматизированной системы) по выбору преподавателя или обучающегося:

- провести идентификацию, спецификацию и оценивание объектов защиты и угроз безопасности;
- классифицировать категории персонала и программно-аппаратных средств, на которые распространяется политика безопасности.
- определить классы защищенности;
- определить показатели защищенности автоматизированных систем и СВТ;
- составить функциональные требования по защите информации в АС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 51624-2000 Автоматизированные системы в защищенном исполнении
2. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. //Стандартинформ, Москва
3. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
4. RD_1992.03.30_1 Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
5. РД ФСТЭК_СВТ Защита от НСД Показатели защищенности от НСД КЛАССЫ СВТ Руководящий документ Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации
6. Методика определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных
7. Основы программно-аппаратной защиты информации: Учебное пособие. Изд. 2-е. М.: Книжный дом «ЛИБРОКОМ», 2013. – 376 с. (Основы защиты информации.)
8. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g
9. Бешта А.А. Модель сбора информации о корпоративной вычислительной сети // Вестник ВолГУ. Серия 10: Инновационная деятельность . 2011. №5. URL: http://cyberleninka.ru/article/n/model-sbora-informatsii-o-korporativnoy-vychislitelnoy-seti.

Учебное текстовое электронное издание

Баранкова Инна Ильинична
Пермякова Ольга Валерьевна

ОПРЕДЕЛЕНИЕ КРИТИЧЕСКИ ЗНАЧИМЫХ РЕСУРСОВ ОБЪЕКТА ЗАЩИТЫ ПРИ СОСТАВЛЕНИИ МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

0,66 Мб
1 электрон. опт. диск

г. Магнитогорск, 2017 год
ФГБОУ ВО «МГТУ им. Г.И. Носова»
Адрес: 455000, Россия, Челябинская область, г. Магнитогорск,
пр. Ленина 38

ФГБОУ ВО «Магнитогорский государственный
технический университет им. Г.И. Носова»
Кафедра информатики и информационной безопасности
Центр электронных образовательных ресурсов и
дистанционных образовательных технологий
e-mail: ceor_dot@mail.ru