МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Югорский государственный университет» (ЮГУ)

НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

РАССМОТРЕНО
На заседании ПЦК МиЕНД
Протокол заседания № 07
«31» августа 2022 г.
Председатель ПЦК
_____Бойко Я.С.

УТВЕРЖДАЮ
Зам. директора по УВР
НефтИН (филиала) ФГБОУ ВО «ЮГУ»
«31» августа 2022 г.
_____Хайбулина Р.И.

КОМПЛЕКТ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ МАТЕРИАЛОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ (МЕЖДИСЦИПЛИНАРНОМУ КУРСУ)

ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

МДК.01.04
индекс

(наименование учебной дисциплины, МДК)

программы подготовки специалистов среднего звена (ППССЗ)
по специальности СПО

10.02.05
код

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
(наименование)

базовой подготовки

г. Нижневартовск

-2022-

Комплект контрольно-измерительных материалов по учебной дисциплине МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении программы подготовки специалистов среднего звена (ППССЗ) по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем базового уровня разработан на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем в соответствии с рабочей программой учебной дисциплины МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

Разработчик:

Нефтяной институт (НефтИн (филиал) ФГБОУ ВО «ЮГУ»)	преподаватель	А.В. Винник
(место работы)	(занимаемая должность)	(инициалы, фамилия)

1. Паспорт комплекта контрольно-измерительных материалов по учебной дисциплине МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

1.1. Область применения

Комплект контрольно-измерительных материалов предназначен для проверки результатов освоения учебной дисциплины (далее - УД) МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении программы подготовки специалистов среднего звена (ППССЗ) по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Комплект контрольно-измерительных материалов позволяет оценивать:

1.1.1. Освоение профессиональных компетенций (ПК) и общих компетенций (ОК)

Профессиональные и общие компетенции	Средства проверки(№ задания)
ПК1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	ПЗ №4, ПЗ №6, ПЗ №12, ПЗ №13
ПК1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	ПЗ №1-16
ПК1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	ПЗ №9-23
ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	ПЗ №1-23
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	ПЗ №16, ПЗ №19, ПЗ №21
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	ПЗ №4, ПЗ №18, ПЗ №21
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Итоговый тест
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	ПЗ №1-23
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	ПЗ №2, ПЗ №5, ПЗ 9
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	ПЗ №1-23,
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	ПЗ №21-29
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической	ПЗ №1-29

подготовленности.	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	ПЗ №1-23
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	ПЗ №14, ПЗ №21, ПЗ №24

1.1.2. Освоение умений и усвоение знаний

Освоенные умения, усвоенные знания	№№ заданий для проверки
1	2
У1. Осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;	ПЗ №5
У2. Организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;	ПЗ №7, ПЗ №16, ПЗ №15
У3. Осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;	ПЗ №18, ПЗ №26
У4. Производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы	ПЗ №1, ПЗ №6
У5. Настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;	ПЗ №6, ПЗ №20, ПЗ №27, ПЗ №29
У6. Обеспечивать работоспособность, обнаруживать и устранять неисправности	ПЗ №6, ПЗ №17, ПЗ №19
З 1. Состав и принципы работы автоматизированных систем, операционных систем и сред; принципы основных методов организации и проведения технического обслуживания вычислительной техники и другихтехнических средств информатизации.	ПЗ №1-5
З 2. Принципы разработки алгоритмов программ, основных приемов программирования;	ПЗ №1
З 3. Модели баз данных;	ПЗ №5-21
З 4. Принципы построения, физические основы работы периферийных устройств;	ПЗ №3
З 5. Теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;	ПЗ №1-6
З 6. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;	ПЗ №4, ПЗ №8, ПЗ №17

1.2. Система контроля и оценки освоения программы учебной дисциплины МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

1.2.1. Формы рубежной аттестации по ППССЗ при освоении учебной дисциплины МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Учебная дисциплина	Формы промежуточной аттестации
1	2
МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
4 семестр	Дифференцированный зачет
6 семестр	Экзамен

1.2.2. Организация контроля и оценки освоения программы учебной дисциплины МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

Рубежный контроль по дисциплине МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении осуществляется на учебных занятиях.

Промежуточный контроль по дисциплине МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении – Экзамен, Дифференцированный зачет.

Экзаменационные билеты содержат задания по всему курсу дисциплины МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

Условием допуска к экзамену является выполнение 70% практических и лабораторных работ на положительную оценку.

Экзамен проводится 1 час в виде тестирования.

Условием положительной аттестации по дисциплине на экзамене является положительная оценка освоения всех умений, знаний, а также формируемых профессиональных и общих компетенций по всем контролируемым показателям.

2. Задания для оценки освоения умений и усвоения знаний при изучении учебной дисциплины МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

2.1. Комплект материалов для оценки освоения умений и усвоения знаний

2.1.1. Комплект заданий для обучающихся

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ ИХТЕМАТИКА ПО УЧЕБНОЙ ДИСЦИПЛИНЕ МДК.01.04 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Раздел	Номер и тема занятия	Количество аудиторных часов
1	**2**	**3**
1.	Практическое занятие №1 Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	2

1.	Практическое занятие №2 Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	2
1.	Практическое занятие №3 Разработка технического задания на проектирование автоматизированной системы	2
1.	Практическое занятие №4 Разработка технического задания на проектирование автоматизированной системы	2
1.	Практическое занятие №5 Категорирование информационных ресурсов	2
1.	Практическое занятие №6 Категорирование информационных ресурсов	2
1.	Практическое занятие №7 Анализ угроз безопасности информации	2
1.	Практическое занятие №8 Анализ угроз безопасности информации.	2
1.	Практическое занятие №9 Построение модели угроз	2
1.	Практическое занятие №10 Построение модели угроз	2
1.	Практическое занятие №11 Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	2
1.	Практическое занятие №12 Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	2
2.	Практическое занятие №13 Установка и настройка СЗИ от НСД	2
2.	Практическое занятие №14 Установка и настройка СЗИ от НСД.	2
2.	Практическое занятие №15 Защита входа в систему (идентификация и аутентификация пользователей)	2
2.	Практическое занятие №16 Разграничение доступа к устройствам	2
2.	Практическое занятие №17 Разграничение доступа к устройствам	2
2.	Практическое занятие №18 Управление доступом	2
2.	Практическое занятие №19 Использование принтеров для печати конфиденциальных документов. Контроль печати	2
2.	Практическое занятие №20 Использование принтеров для печати конфиденциальных документов. Контроль печати	2
2.	Практическое занятие №21 Настройка системы для задач аудита	2
2.	Практическое занятие №22 Настройка контроля целостности и замкнутой программной среды.	2
2.	Практическое занятие №23 Настройка контроля целостности и замкнутой программной среды	2
2	Практическое занятие №24 Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	2
2	Практическое занятие №25 Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	2

2	Практическое занятие №26 Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	2
2	Практическое занятие №27 Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	2
2	Практическое занятие №28 Оформление основных эксплуатационных документов на автоматизированную систему	2
2	Практическое занятие №29 Оформление основных эксплуатационных документов на автоматизированную систему	2
	Итого:	**58**

Практическое занятие №1-2
Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационнаясистема компании)

Цель: ознакомится с видами АИС их назначениями, типами.

Задание для самостоятельного выполнения.

1. Рассмотреть примеры функционирования АИС
1) этапы развития
2) процессы в АИС
3) Классификация АИС
4) Классификация по признакам
5) Классификация по сфере применения
6) Классификация по характеру обработки информации
7) Классификация по способу хранения данных
8) Структура
2. Работу оформить в виде таблиц, схем.

Практическое занятие №3-4
Разработка технического задания на проектирование автоматизированной системы

Цель: усвоить понятие технического задания, структуру, оформление, требования, назначение и цели

Задание для самостоятельного выполнения:

1. Ознакомится с нижеуказанными стандартами для проекта автоматизации.

- IEEE 830-1998. Методика составления спецификаций требований к программному обеспечению.
- ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств.
- ISO/IEC/IEEE 29148-2011. Systems and software engineering — Life cycle processes — Requirements engineering.

- ГОСТ Р 54869-2011. Проектный менеджмент. Требования к управлению проектом.
- ГОСТы серии 34.

2. Составить техническое задание на АС.

Техническое задание на автоматизированную систему управления (ТЗ на АС) – основной документ, предъявляющий требования к создаваемой автоматизированной системе и устанавливающий порядок, в соответствии с которым будет проводиться разработка АСУ ТП и ее прием при вводе в эксплуатацию.

ТЗ может разрабатываться как на всю систему, так и на составные части:

- ✔ составные части АС (по ГОСТ 34.602);
- ✔ технические средства (компоненты) входящие в состав АС (по ГОСТ ЕСКД);
- ✔ программные средства (компоненты) входящие в состав АС (по ГОСТ ЕСПД).

Современное техническое задание на разработку автоматизированной систему АСУ должно разрабатываться с учётом требований современного уровня развития науки и технического прогресса, а так же с учётом лучших мировых практик в области предъявляемых требований на разрабатываемые автоматизированные системы управления АСУ.

Структура и разделы

ТЗ на АСУ может содержать следующие разделы:

1) общие сведения;
2) цели и назначение создания автоматизированной системы;
3) характеристика объектов автоматизации;
4) требования к автоматизированной системе;
5) состав и содержание работ по созданию автоматизированной системы;
6) порядок разработки автоматизированной системы;
7) порядок контроля и приемки автоматизированной системы;
8) требования к составу и содержанию работ по подготовке объекта автоматизации к вводу автоматизированной системы в действие;
9) требования к документированию;
10) источники разработки.

Допускается разделение указанных разделов на подразделы. В зависимости от функционального назначения и условий, в которых будет функционировать АСУ, допускаются следующие действия с разделами ТЗ:

- ✔ ввод дополнительных разделов (подразделов);
- ✔ исключение разделов (подразделов);
- ✔ объединение разделов (подразделов).

Практическое занятие №5-6
Категорирование информационных ресурсов

Цель: ознакомится с категориями конфиденциальности информации

С целью создания нормативно-методической основы для дифференцированного подхода к защите ресурсов и типизации принимаемых организационных мер в организации разрабатывается Положение об определении требований по защите (о категорировании) ресурсов автоматизированной системы организации. (Далее - Положение)

В разделе Положения 2.1. Категории конфиденциальности защищаемой информации, информация, циркулирующая в организации, раделена на 3 категории:

«СТРОГО КОНФИДЕНЦИАЛЬНАЯ» - к данной категории относится информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства (коммерческая и банковская тайны, персональные данные и т.д.), 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»- к данной категории относится информация, не отнесенная к категории «СТРОГО КОНФИДЕНЦИАЛЬНАЯ», ограничения на распространение которой вводятся решением руководства Организации в соответствии с предоставленными ему как собственнику (уполномоченному собственником лицу) информации действующим законодательством правами, разглашение которой может привести к значительным убыткам и потере конкурентоспособности ОРГАНИЗАЦИИ (нанесению ощутимого ущерба интересам его клиентов, корреспондентов, партнеров или сотрудников);

«ОТКРЫТАЯ»- к данной категории относится информация, обеспечения конфиденциальности (введения ограничений на распространение) которой не требуется.

Переходя к классификации, необходимо отметить, что классификация информационных систем персональных данных стоит особняком и регламентирована Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 " Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Классификация Государственных информационных систем регламентируется Приказом ФСТЭК от 11 февраля 2013 г. №17 "11 февраля 2013 г. N 17 Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

Для автоматизации процесса определения уровня защищенности и определения класса Государственной информационной системы нами разработаны следующие сервисы:

1.Расчет уровня защищенности для ИСПДн.

2.Расчет класса защищенности для ГИС

Определение мероприятий по защите осуществляется с учетом модели угроз. В свою очередь порядок составления модели угроз указан в Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и основывается на Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Также при использовании средств криптографической защиты на основании Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ РФ 21 февраля 2008 г. N 149/54-144) составляется Модель нарушителя.

Классификация информации ограниченного распространения, не содержащей персональных данных, производится на основании РД "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.)

Подробно расписать

Категории защищаемой информации:

1) Категории конфиденциальности защищаемой информации:

2) Категории целостности защищаемой информации:

3) Требуемые степени доступности функциональных задач

Практическое занятие №7-8
Анализ угроз безопасности информации

Цель: исследование терминологической базы; закрепление знаний основного понятийного аппарата, применяемого в области защиты информации; формирование навыка работы с нормативными документами по исследуемому вопросу; анализ угроз информационной безопасности

Задание для самостоятельного выполнения (оформить в виде отчета):

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы

Приоритет	Виды угроз	Субъекты угроз			
		Стихия	Нарушитель	Злоумышленник	
				На территории	Вне территории
1	Травмы и гибель людей	+	+	+	+
2	Повреждение оборудование, техники	+	+	+	+
3	Повреждение систем жизнеобеспечения	+	+	+	+
4	Несанкционированное изменение технологического процесса		+	+	
5	Использование нерегламентированных технических и программных средств		+	+	
6	Дезорганизация функционирования предприятия	+		+	
7	Хищение материальных ценностей			+	
8	Уничтожение или перехват данных путем хищения носителей информации			+	
9	Устное разглашение конфиденциальной информации		+		
10	Несанкционированный съем информации			+	+
11	Нарушение правил эксплуатации средств защиты		+	+	

Практическое занятие №9-10
Построение модели угроз

Цель: оздание полной характеристики потенциального нарушителя безопасности и перечня актуальных угроз безопасности для заданного объекта.

Задания для самостоятельного выполнения:

Задание 1. Построение модели вероятного нарушителя безопасности объекта. Под моделью нарушителя понимается совокупность количественных и качественных характеристик нарушителя, с учетом которых определяются требования к комплексу инженерно-технических средств охраны и/или его составным частям.

Составить список внешних и внутренних нарушителей безопасности заданного объекта. Проанализировать следующие характеристики, присущие нарушителям, заполнить таблицу 1.

Таблица 1 - Характеристики нарушителя

Признак характеристики нарушителя	Характеристика
Цели и задачи	проникновение на охраняемый объект без причинения объекту видимого ущерба
	причинение ущерба объекту
	преднамеренное проникновение при отсутствии враждебных намерений
	случайное проникновение
	Дополнить
Степень принадлежности вероятного нарушителя к объекту	сотрудник охраны
	сотрудник учреждения
	посетитель
	постороннее лицо
	Дополнить
Степень осведомленности вероятного нарушителя об объекте	детальное знание объекта
	осведомленность о назначении объекта, его внешних признаках и чертах
	неосведомленный вероятный нарушитель
Степень осведомленности нарушителя о системе охраны объекта	полная информация о системе охраны объекта
	информация о системе охраны вообще и о системе охраны конкретного объекта охраны

	информация о системе охраны вообще, но не о системе охраны конкретного объекта
	неосведомленный вероятный нарушитель
Степень профессиональной подготовленности вероятного нарушителя	специальная подготовка по преодолению систем охраны
	не имеет специальной подготовки по преодолению систем охраны
Степень физической подготовленности вероятного нарушителя	специальная физическая подготовка
	низкая физическая подготовка
Владение вероятным нарушителем способами маскировки	владеет
	не владеет
Степень технической оснащенности вероятного нарушителя	высокая
	средняя
	низкая
Способ проникновения вероятного нарушителя на объект	взлом замка
	проход по поддельным документам
	Дополнить

Определить категорию нарушителя (существует четыре категории нарушителей).

Построить неформализованную модель нарушителя безопасности в соответствии с таблицей. данного учебного пособия.

Задание 2. Разработка модели угроз безопасности объекта. Анализ угроз безопасности включает:

- - описание угроз;
- - оценку вероятности возникновения угроз;
- - оценку реализуемости угроз;
- - оценку опасности угроз;
- - определение актуальности угроз.

Составить список всех возможных угроз физической безопасности для заданного объекта. При этом использовать перечень угроз, данный в таблице. Вычислить все необходимые показатели угроз. Построить модель угроз по примеру таблицы 2

Таблица 2 - Модель угроз безопасности защищаемого объекта

Угроза	Вероятность реализаци и угрозы	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы

Несанкционированный доступ к компьютерам	Маловероятно (0)	• 0,25 • (низкая)	Низкая опасность	Неактуальная
Кража технических средств с хранящейся в них информацией	Маловероятно (0)	• 0,25 • (низкая)	Низкая опасность	Неактуальная
Кража носителей информации	Маловероятно (0)	• 0,25 • (низкая)	Низкая опасность	Неактуальная
Кража материальных и финансовых ценностей	Средняя вероятность (5)	• 0,5 • (средняя)	Высокая	Актуальная
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей	Средняя вероятность (5)	• 0,6 • (средняя)	Высокая	Актуальная
Прослушивание телефонных и радиопереговоров	Средняя вероятность^)	• 0,5 • (средняя)	Высокая	Актуальная
Внедрение «закладок»	Маловероятно (0)	• 0,25 • (низкая)	Низкая опасность	Неактуальная

Выписать из таблицы только актуальные угрозы безопасности.

Контрольные вопросы

- 1 Дать определение понятия «угроза физической безопасности», «нарушитель физической безопасности».
- 2 Назвать и дать характеристику типичных угроз физической безопасности объектов информатизации.
- 3 Назвать типичные объекты воздействия угроз безопасности.
- 4 Назвать и охарактеризовать типы и категории нарушителей.
- 5 Какой тип нарушителя считается самым опасным, привести обоснование ответа.
- 6 Дать определение понятия «модель нарушителя». Назвать и описать основные характеристики нарушителя безопасности.
- 7 Дать определение понятия «формализованная модель нарушителя». Привести методы построения формализованной модели нарушителя.
- 8 Перечислить основные действия, которые может совершить внешний нарушитель.
- 9 Дать определение понятия «модель угроз безопасности». Назвать основные показатели, определяющие актуальность угроз.
- 10 Что подразумевают под частотой (вероятностью) реализации угрозы? Назовите вербальные градации этого показателя.
- 11 За счет чего могут быть реализованы угрозы безопасности.
- 12 По какой формуле определяется коэффициент реализуемости угрозы, какова вербальная интерпретация реализуемости угрозы?

- 13 Каким образом оценивается опасность каждой угрозы?
- 14 Как используют в дальнейшем список актуальных угроз безопасности?

Практическое занятие №11-12
Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.

Ц е л ь :

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для персональных данных. Подход к составлению перечня актуальных угроз состоит в следующем.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 1.

Таблица 1. Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом			+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)			+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации		+	
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий		+	
локальная ИСПДн, развернутая в пределах одного здания	+		
2. По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть общего пользования			+
ИСПДн, имеющая одноточечный выход в сеть общего пользования		+	
ИСПДн, физически отделенная от сети общего пользования	+		
3. По встроенным (легальным) операциям с записями баз персональных данных			
чтение, поиск	+		
запись, удаление, сортировка		+	
модификация, передача			+
4. По разграничению доступа к персональным данным			
ИСПДн, к которой имеют доступ определенные переченем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн		+	
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся			+

владельцем ИСПДн			
ИСПДн с открытым доступом			+
5. По наличию соединений с другими базами ПДн иных ИСПДн			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)			+
ИСПДн, в которой используется	+		
Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
одна база ПДн, принадлежащая организации – владельцу данной ИСПДн			
6. По уровню обобщения (обезличивания) ПДн			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)	+		
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации		+	
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки			
ИСПДн, предоставляющая всю базу данных с ПДн			+
ИСПДн, предоставляющая часть ПДн		+	
ИСПДн, не предоставляющая никакой информации	+		

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением $Y=(Y_1+Y_2)/20$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если $0 \leq Y \leq 0,3$, то возможность реализации угрозы признается низкой;

если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признается средней;

если $0,6 < Y \leq 0,8$, то возможность реализации угрозы признается высокой;

если $Y > 0,8$, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 2.

Таблица 2. Правила отнесения угрозы безопасности персональных данных к актуальной

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

С использованием данных об уровне защищенности ИСПДн и составленного перечня актуальных угроз формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

Задание

На основе исходных данных, предоставленных преподавателем, и описанной методики определения актуальных УБПДн построить модель УБПДн.

Отчет о практической работе должен содержать описание процесса построения модели УБПДн, перечень актуальных УБПДн и их описание (последствия реализации). Для составления модели угроз рекомендуется в качестве дополнительного источника использовать методический документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»

Практическое занятие №13-14
Установка и настройка СЗИ от НСД.

Ц е л ь :

Архитектура и системные требования СЗИ НСД Dallas Lock Linux

Архитектура Dallas Lock Linux состоит из следующих подсистем:

- ✔ Подсистема идентификации и аутентификации
- ✔ Подсистема управления доступом
- ✔ Подсистема гарантированной зачистки информации
- ✔ Подсистема контроля устройств (аппаратной среды)
- ✔ Подсистема контроля целостности
- ✔ Подсистема регистрации и учета

Рисунок 1. Архитектура СЗИ НСД Dallas Lock Linux

СЗИ НСД Dallas Lock Linux работает на компьютерах под управлением следующих операционных систем семейства Linux:

- Debian 7.11 x64 (systemd, версия ядра 3.18).
- CentOS 7 x64 (версия ядра 3.18, 4.4). Поддерживаются все минорные версии дистрибутива в рамках указанного мажорного релиза.
- Red Hat Enterprise Linux Server 7 x64 (версия ядра 3.18, 4.4). Поддерживаются все минорные версии дистрибутива в рамках указанного мажорного релиза.
- Fedora 24 x64 (версия ядра 4.4, 3.18).

- OpenSUSE 42 x64 (версия ядра 4.4). Поддерживаются все минорные версии дистрибутива в рамках указанного мажорного релиза.
- Ubuntu 16.04 x64 (версия ядра 4.4). Поддерживаются все минорные версии дистрибутива в рамках указанного мажорного релиза.
- ЛотОС2 2.1 x64 (версия ядра 3.18).
- Alt Linux 8 (будет доступно в рамках планового обновления).

Изделие предназначено для использования на технических средствах (ТС), таких как: персональные компьютеры, портативные компьютеры (ноутбуки), сервера и ТС с поддержкой виртуальных сред (например, KVM).

Изделие поставляется в виде установочных пакетов для каждой из заявленных поддерживаемых операционных систем. В состав пакетов входит локальный клиент СЗИ НСД. Настройка и управление СЗИ НСД Dallas Lock Linux осуществляется через графическую (реализовано для Linux и Windows) или консольную оболочки администрирования

Обзор СЗИ ВИ Dallas Lock

Работа с СЗИ НСД Dallas Lock Linux

Установка продукта

Установка продукта осуществляется из стандартного для Linux пакета. При установке СЗИ НСД требуется скачивание дополнительных пакетов из глобальной сети. Если производится установка на автономный компьютер, необходимо, чтобы в локальной сети был расположен официальный репозиторий соответствующего дистрибутива операционной системы и были выполнены соответствующие настройки инфраструктуры.

Следует обратить внимание, что все сервисы, которые требуют создания пользователей в системе, рекомендуется устанавливать до установки СЗИ НСД. В противном случае, если после установки СЗИ НСД возникла необходимость установить какой-либо сервис, который требует создания в системе специального пользователя, можно создать его средствами СЗИ НСД (с флагом «системный») до установки сервиса. Необходимо учитывать, что этот способ может не привести к тому, что сервис установится корректно.

После установки системы защиты необходимо следить за сроком действия корневого и пользовательского сертификатов и при необходимости вовремя их обновлять. Данный сертификат используется для взаимодействия между системой защиты и консолью управления. Для проверки срока действия сертификата необходимо выполнить команду openssl x509 -noout -text -in <путь к сертификату>. В результате выполнения команды будут предоставлены данные по сертификату, в том числе и срок действия.

Кроме установки самого СЗИ необходимо определить, каким образом будет осуществляться управление. Существует три возможных варианта управления:

- локально установить оболочку администрирования (консольную и/или графическую);
- установить графическую оболочку администрирования на АРМ под управлением Windows;
- централизованным управлением через сервер безопасности Dallas Lock 8.0.

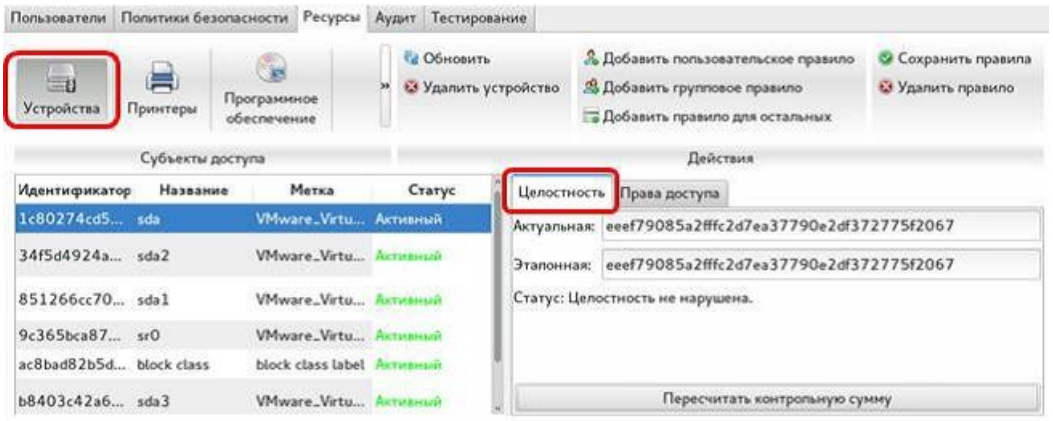
В нашем обзоре мы будем использовать локальную консольную и графическую оболочку администрирования.

Подсистема контроля целостности

Подсистема реализует контроль целостности аппаратной среды, целостность объектов файловой системы и целостность программных компонентов СЗИ, а также восстановление целостности для программных компонентов средства защиты информации.

Основу механизмов контроля целостности представляет проверка соответствия контролируемого объекта эталонному образцу. Для этого используются контрольные суммы.

Рисунок 2. Контроль целостности устройств СЗИ НСД Dallas Lock Linux



В консольной оболочке администрирования ishl аналогичная настройка будет выглядеть следующим образом:

policies
hardware-integrity-set
set-check-on-boot yes
set-generate-audit yes
execute

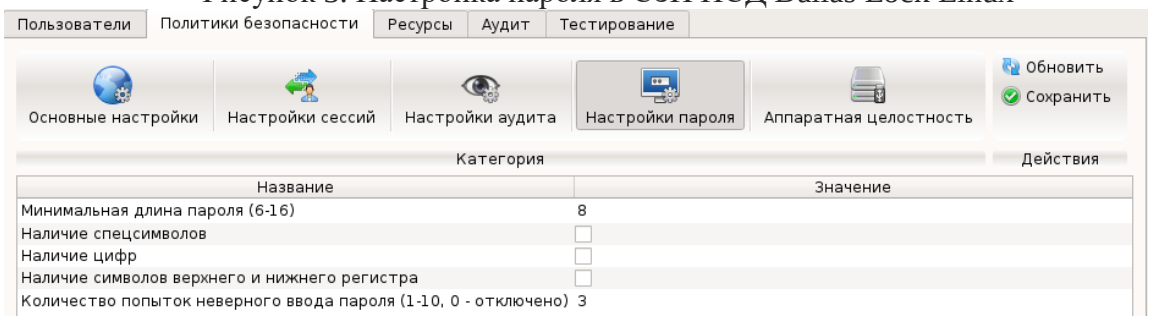
При использовании консольной оболочки администрирования необходимые команды можно записать в файл и вызвать их, выполнив следующую команду: ishl –f <имя файла>

Подсистема идентификации и аутентификации

Подсистема идентификации и аутентификации реализует механизмы проверки пользователей при каждом входе в операционную систему и в консольное приложение управления СЗИ НСД. Проверяется имя пользователя и пароль.

Подсистема содержит механизмы проверки качества (надежности) задаваемого пароля при его изменении пользователем.

Рисунок 3. Настройка пароля в СЗИ НСД Dallas Lock Linux



В СЗИ НСД для усиления процедур идентификации и аутентификации возможно применение аппаратных идентификаторов. В идентификаторе может храниться ключ (сертификат) для усиленной аутентификации пользователя.

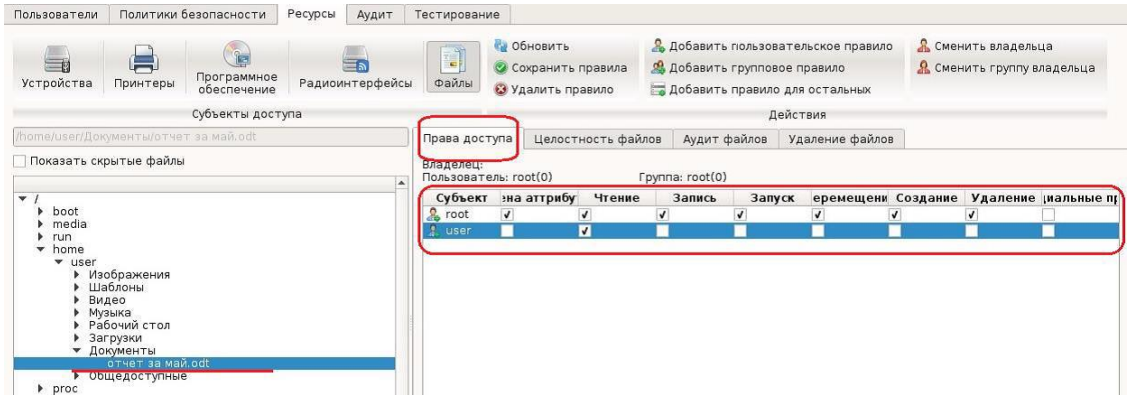
Подсистема управления доступом

Подсистема управления доступом реализует механизмы, направленные на разграничение доступа пользователей к защищаемым объектам — к объектам файловой системы и к накопителям информации.

СЗИ НСД Dallas Lock Linux позволяет гибко задавать пользователям права на доступ к защищаемым объектам. После задания прав пользователи могут работать только с теми объектами, доступ к которым им разрешен, и совершать над ними только санкционированные операции.

При настройке доступа к файлам и каталогам предусмотрено управление как классическими правами UNIX, так и списками расширенного контроля доступа через POSIX ACL.

Рисунок 4. Настройка прав доступа на файл в СЗИ НСД Dallas Lock Linux

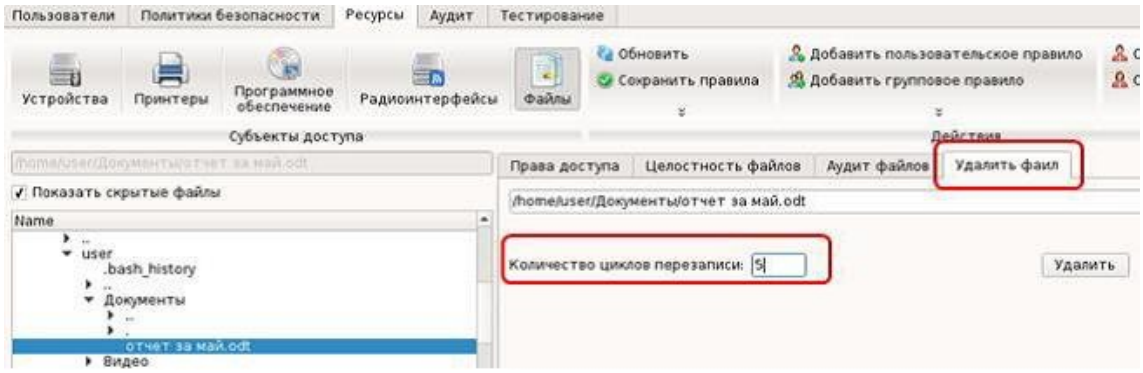


Подсистема гарантированной зачистки информации Подсистема контроля гарантированной зачистки информации реализует очистку освобождаемых областей оперативной памяти, гарантированную зачистку объектов ФС и внешних подключаемых накопителей.

Гарантированная очистка памяти функционирует с момента установки СЗИ НСД и не требует ввода дополнительных команд в консольном приложении управления средством защиты информации.

Для очистки остаточной информации на съемных накопителях и объектов ФС необходимо использовать дополнительную утилиту, поставляемую совместно с СЗИ НСД.

Рисунок 5. Гарантированное удаление объекта файловой системы в СЗИ НСД Dallas Lock Linux



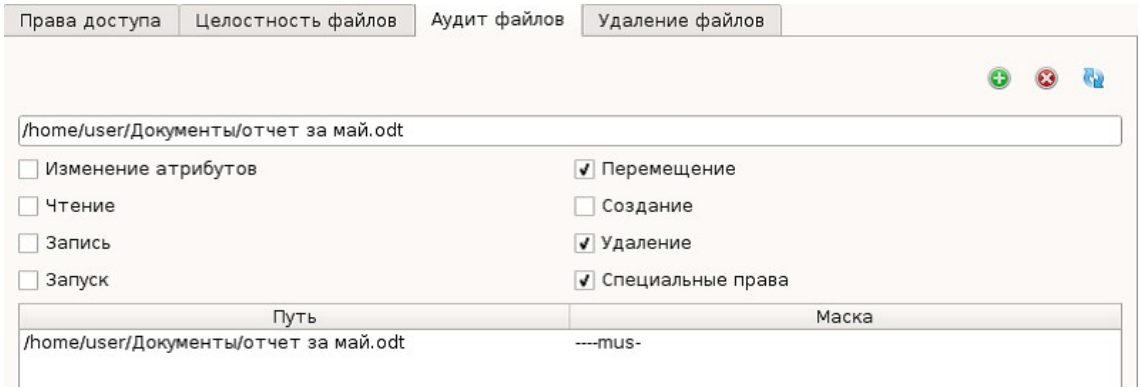
Подсистема контроля устройств

Подсистема контроля устройств реализует разграничение доступа пользователей и групп пользователей к блочным устройствам (сменным накопителям информации), ограничения доступа к беспроводным устройствам передачи информации, устройствам вывода на печать в целях предотвращения несанкционированной утечки информации.

Подсистема регистрации и учета

Подсистема регистрации и учета (подсистема анализа) реализует возможность аудита событий, производимых пользователями над защищаемыми объектами, аудита событий входов (выходов) в информационную систему, в т. ч. сетевых, аудита системных событий, отчуждения информации на накопители или твердую копию, а также фиксацию таких событий в журналах информационной безопасности.

Рисунок 6. Настройка аудита файлов в СЗИ НСД Dallas Lock Linux



Выводы

На сегодняшний день для обработки информации в государственных информационных системах, информационных системах персональных данных или в автоматизированных системах управления производственными и технологическими процессами организациям требуется выполнять требования регулятора — Приказы №17, №21 и №31 ФСТЭК России. Так и СЗИ НСД Dallas Lock Linux предназначена для использования в информационных системах персональных данных 1 уровня защищенности, в государственных информационных системах 1 класса защищенности и автоматизированных систем управления производственными и технологическими процессами до 1 класса защищенности включительно, создания защищенных многопользовательских автоматизированных систем до класса защищенности 1Г включительно.

Процесс установки прост и интуитивно понятен. Администратору безопасности предоставляется возможность управления паролями, доступом к объектам файловой системы, подсистемой контроля целостности.

Достоинства

- Наличие механизмов удаленного и централизованного управления (в т. ч. оболочка администрирования для Windows).
- Наличие механизмов проверки подлинности клиентских частей СЗИ, сервера безопасности (OpenSSL).
- Поддержка работы на большом наборе наиболее популярных дистрибутивов Linux.
- Механизмы централизованного управления для клиентских частей СЗИ НСД Dallas Lock Linux и сервера безопасности СЗИ Dallas Lock 8.0.
- Защита от подмены ядра и процедур инициализации.
- Собственный механизм дискреционного доступа и аудита доступа.
- Для консольной оболочки администрирования есть возможность выполнять команды из файла.

Недостатки

- До развертывания системы защиты рекомендуется установить все сервисы, которые создают учетные записи.
- Необходимо следить за сроком действия корневого и пользовательского сертификатов и при необходимости вовремя их обновлять.
- На несколько объектов файловой системы нельзя установить права доступа и политику аудита.

Практическое занятие №15

Защита входа в систему (идентификация и аутентификация пользователей)

Цель:

Защита от несанкционированного входа предназначена для предотвращения доступа посторонних лиц к защищенному компьютеру. К этой группе средств относятся:

- программные и аппаратные средства идентификации;
- средства блокировки компьютера.

Идентификация и аутентификация пользователей

Идентификация и аутентификация пользователя выполняются при каждом входе в систему. Штатная для ОС Windows процедура входа предусматривает ввод имени и пароля пользователя или использование аппаратных средств, поддерживаемых операционной системой.

Для обеспечения дополнительной защиты входа в Secret Net 6 могут применяться средства идентификации и аутентификации на базе идентификаторов eToken, iKey, Rutoken или iButton. Такие устройства должны быть зарегистрированы (присвоены пользователям) средствами системы защиты и могут использоваться в составе аппаратных средств защиты. Кроме того, предусмотрен режим усиленной аутентификации, основанный на дополнительной проверке подлинности предъявленной ключевой информации пользователя. Носителями ключевой информации могут являться идентификаторы или сменные носители, такие как дискеты, Flash-карты, Flash-накопители и т. п. Генерация ключевой информации выполняется средствами системы Secret Net 6.

В системе Secret Net 6 идентификация и аутентификация пользователей может выполняться в следующих режимах:

"Стандартный" — пользователь может войти в систему, выполнив ввод имени и пароля, или используя аппаратные средства, стандартные для ОС Windows;

"Смешанный" — пользователь может войти в систему, выполнив ввод имени и пароля, а также может использовать персональный идентификатор, поддерживаемый системой Secret Net 6;

"Только по идентификатору" — каждый пользователь для входа в систему должен обязательно использовать персональный идентификатор, поддерживаемый системой Secret Net 6.

Для повышения степени защищенности компьютеров от несанкционированного использования предусмотрены следующие возможности:

включение режима разрешения интерактивного входа только для доменных пользователей — в этом режиме блокируется вход в систему локальных учетных записей (не зарегистрированных в домене);

включение режима запрета вторичного входа в систему — в этом режиме блокируется запуск команд и сетевых подсоединений с вводом учетных данных другого пользователя (не выполнившего интерактивный вход в систему).

Блокировка компьютера

Под блокировкой компьютера понимается запрет доступа пользователей (исключая администратора) к работе на данном компьютере. Механизм временной блокировки предназначен для предотвращения несанкционированного использования компьютера.

Для пользователей могут быть установлены ограничения на количество неудачных попыток входа в систему. В дополнение к стандартным возможностям ОС Windows (блокировка учетной записи пользователя после определенного числа попыток ввода неправильного пароля) система Secret Net 6 контролирует неудачные попытки аутентификации пользователя по ключевой информации. Если в режиме усиленной аутентификации пользователь определенное количество раз предъявляет неверную ключевую информацию, система блокирует компьютер. Разблокирование компьютера осуществляется администратором. Счетчик неудачных попыток обнуляется при удачном входе пользователя или после разблокирования компьютера.

Для временной блокировки компьютера используется стандартный механизм ОС Windows. Режим временной блокировки может быть включен самим пользователем или системой после некоторого периода простоя компьютера. Длительность интервала неактивности (простоя компьютера), после которого автоматически включается режим блокировки, устанавливается настройкой параметров и распространяется на всех пользователей. Для снятия блокировки необходимо указать пароль текущего пользователя.

Блокировка компьютера предусмотрена и в алгоритмах работы защитных механизмов. Такой тип блокировки используется в следующих ситуациях:

• при нарушении ***функциональной целостности системы Secret Net 6***;

• при нарушении аппаратной ***конфигурации компьютера***;

• при нарушении целостности ***контролируемых объектов***.

Разблокирование компьютера в перечисленных случаях осуществляется администратором.

В сетевом режиме функционирования блокировка и разблокирование защищаемого компьютера могут осуществляться удаленно по команде пользователя программы мониторинга.

Задание

Ответить на вопросы:

1. Функциональная целостность системы Secret Net 6
2. Аппаратная конфигурация компьютера
3. Целостность контролируемых объектов.

Практическое занятие №16-17

Разграничение доступа к устройствам.

Ц е л ь : Изучить способы разграничения доступа. Научиться распределять права доступа сотрудникам предприятия в зависимости от их должностных обязанностей.

Порядок выполнения работы

1 Выполнить разграничение доступа по спискам контроля доступа для всех пользователей информационной системы Белорусской железной дороги из практической работы № 1. В таблице 4 разделить всех пользователей на не менее чем 5 групп. В таблице 5 прописать разрешенные действия для групп и активов, для обозначения прав использовать следующие сокращения: X – нет прав; R – чтение; W – запись; C – создание; E – редактирование; D – удаление.

Таблица 1 – Разделение пользователей на группы

Группа пользователей	Состав группы пользователей			

Таблица 5 – Разграничение прав пользователей по спискам контроля доступа

Актив	Группы пользователей				

2 Выполнить избирательное разграничение доступа для всех пользователей предприятия (не менее семи). Задание выполнить в виде таблицы 6.

Таблица 6 – Разграничение прав пользователь по избирательному контролю доступа

Пользователи	Активы					

3 Выполнить полномочное управление доступом для всех пользователей предприятия. В таблицах 7 и 8 распределить метки критичности для пользователей (не менее семи) и активов (не менее семи).

Таблица 7 – Определение меток критичности для пользователей

Пользователи	Метка критичности				
	Особой важности	Совершенно секретно	Секретно	Для служебного пользования	Несекретно

Таблица 8 – Определение меток критичности для активов

Активы	Метка критичности				
	Особой важности	Совершенно секретно	Секретно	Для служебного пользования	Несекретно

Содержание отчета

1 Цель работы.
2 Результаты выполнения задания.
3 Описание информационного объекта.
4 Таблицы правил разграничения доступа.
5 Вывод по работе.

Контрольные вопросы

1 Основные отличия избирательного и полномочного управления доступом.
2 В каких сферах может использоваться мандатное управление доступом?
3 Достоинства и недостатки мандатного разграничения доступа.
4 Особенности разграничения доступа по спискам.

Практическое занятие №18
Управление доступом.

Ц е л ь : изучение составляющих элементов систем удаленного управления и контроля объектов.

Выполнение работы

Задание 1. Изучите составляющие элементы системы обслуживания информационных систем удаленного управления и контроля объектов.

Задание 2. Подберите все составляющие элементы для системы удаленного управления и контроля доступом объектов техникума. Дайте им короткую характеристику.

Задание 3. Приведите 5 различных примеров различных конфигураций систем контроля управления доступом.

Практическое занятие №19-20
Использование принтеров для печати конфиденциальных документов. Контроль печати

МОНИТОРИНГ ПЕЧАТИ ПРИНТЕРОВ

Выбираете как вести контроль и мониторинг печати на принтер?

Контроль печати документов часто становится головной болью руководителя или ИТ специалистов в организации:

- - как подсчитать затраты на печать документов?
- - как выявить сотрудников, использующих принтеры в личных целях?

- - как снизить затраты на расходники за счет сокращения нецелевой печати?
- - как предотвратить кражу важной информации в виде напечатанных документов?
- - Как же на самом деле выбрать простую и надежную систему контроля печати.

Также вы можете попробовать программу контроля печати

Содержание:

- **С чего начать аудит печати**
- **Что важно учесть при выборе системы контроля печати**
- **Как происходит контроль печати в организации, что и куда поставить**
- **дополнительные возможности, которые сильно упростят вашу задачу**

Обратите внимание, контроль печати – это лишь одна из функций LanAgent.

С чего начать аудит печати

Очевидно, что первое, что требуется сделать, это определить начальное состояние.

Чек лист может выглядеть так:

- 1). Определить сколько и каких принтеров сейчас используется в организации.
- 2). Оценить текущие расходы на бумагу и заправку принтеров по бухгалтерским документам.
- 3). Подсчитать стоимость печати одной страницы (например, исходя из ресурса картриджа и стоимости его заправки, а также стоимости листа бумаги)
- 4). Выяснить каким сотрудникам принтеры доступны и на сколько выбор принтеров соответствует задачам. Печать на некоторых принтерах обходится дороже.

В случае небольших компаний эти этапы можно сократить просто до подсчета текущих расходов и прикидкой стоимости печати каждой страницы.

Следующий шаг – это оптимизация расходов на печать. Для этого вам потребуется выяснить какие отделы или конкретные сотрудники печатают больше других. И как много среди напечатанных документов не относящихся к работе. Или проще говоря, личных.

Для этого вам уже потребуется программа контроля печати.

Что важно учесть при выборе системы контроля печати

Первое: софт контроля за печатью документов должен уметь кроме определения количества страниц и копий в напечатанных документах еще определять название документа и имя принтера на который отправлено задание.

В идеале также и программу, из которой задание направлено. Это поможет даже при беглом первичном анализе выявить нецелевую печать.

И работать это должно при любом принтере!

Важно! Многие программы мониторинга печати работают только с локальными принтерами (подключенными непосредственно к компьютеру, с которого печатают). Вам же может потребоваться учет и сетевых и «расшаренных» принтеров.

«Расшаренные» принтеры – это принтеры, подключенные к какому-то компьютеру и к ним открывается общий доступ.

Именно поэтому в LanAgent мы учитывали все типы принтеров.

Подсчет статистики печати поможет определить кто печатает больше и оценить затраты и потери. Однако, не всегда по названию документа понятно что именно в нем содержится.

Например, напечатан «Документ1» на 50 страниц. Что это было?

Опять же так можно распечатать и базу клиентов и другую конфиденциальную информацию.

Поэтому мы подходим ко второму критерию: система контроля печати должна сохранять изображение напечатанных документов.

И делать это в том формате, в котором вы его сможете просмотреть!

Это ловит вам сразу двух зайцев: и нецелевую печать помогает достоверно выявить и попытку передачи коммерческой информации конкурентам обнаружить.

Именно поэтому, LanAgent обязательно делает копии напечатанных документов и сохраняет их в pdf формате.

Третий важный момент: система должна сама предупреждать вас о нестандартной активности.

Это будет полезно как при выявлении нецелевого использования принтеров, так и для защиты важной информации.

Что это может быть за нестандартная активность:

- - печать документов в нерабочее время (когда на месте нет коллег, которые могут увидеть)

- - печать слишком большого количества страниц или документов (больше чем человек делает обычно)

- - обнаружение ключевых слов в названии документов или их содержимом

Скорее всего, у вас не так много свободного времени, чтобы постоянно контролировать сотрудников. Поэтому, важно чтобы система давала вам знать, когда следует обратить особое внимание.

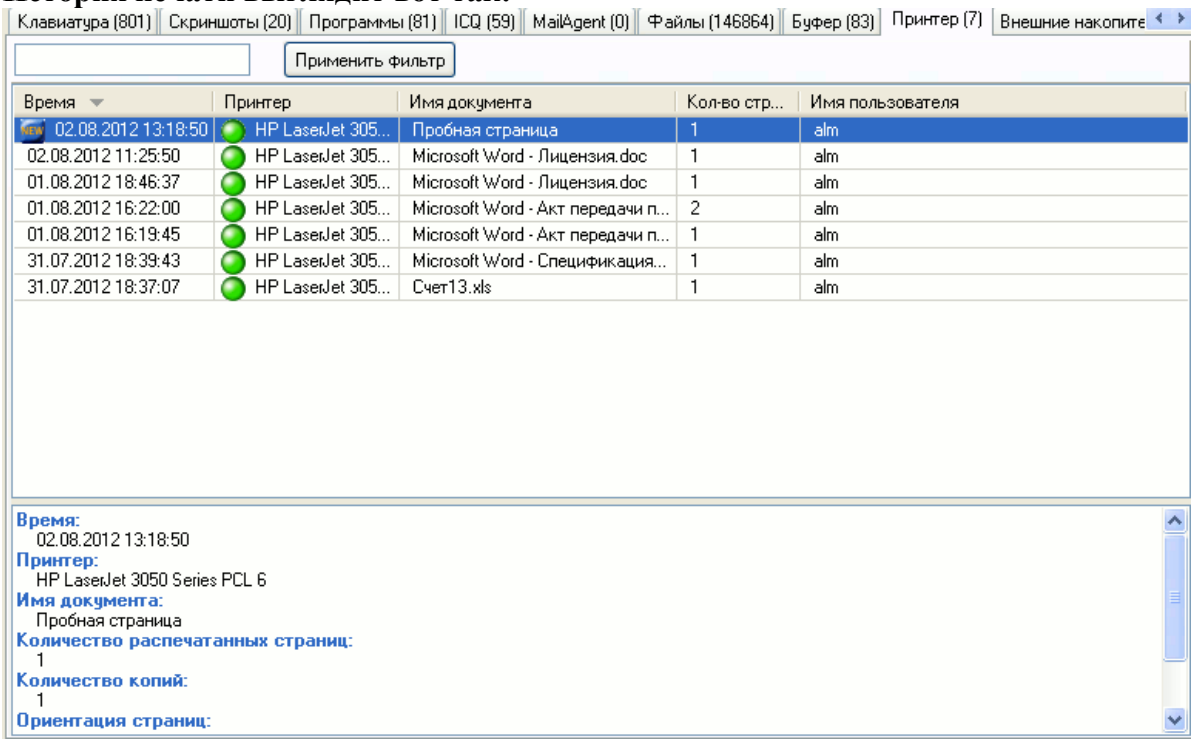
Для этих целей в LanAgent реализованы и все указанные выше алгоритмы обнаружения подозрительных действий, и уведомления о них администратора программы.

Как происходит контроль печати в организации, что и куда поставить

В составе программного комплекса LanAgent две части. Модуль слежения, который ставится на компьютеры сотрудников. И серверная часть, которая ставится на отдельный ПК.

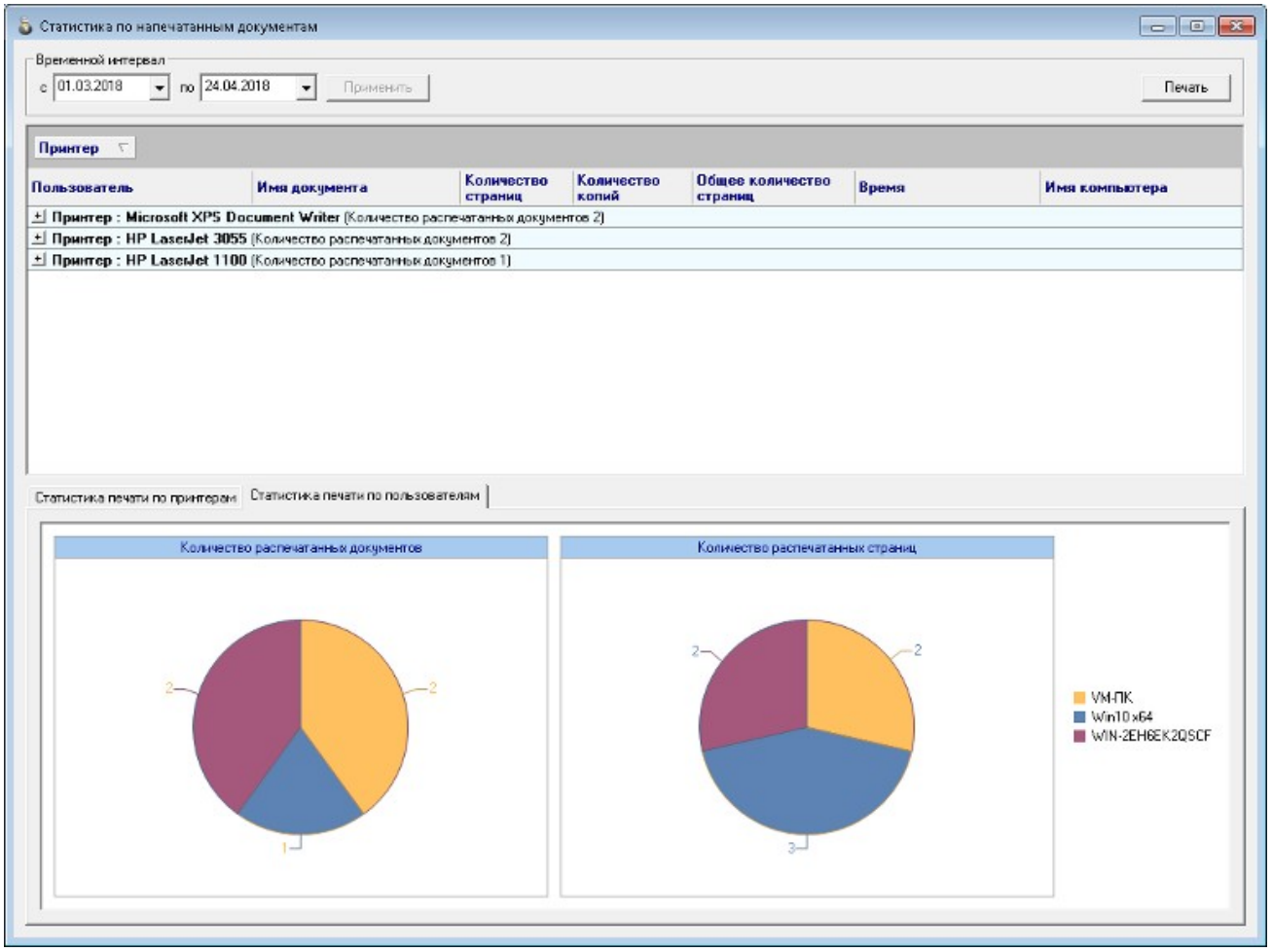
При отправке работником документа на печать, программа это зафиксирует и сохранит параметры и изображение документа.

История печати выглядит вот так:



Дважды щелкнув на интересующей строке можно просмотреть изображение документа.

Анализ кто и сколько печатал можно провести в такой форме:



Дополнительные возможности, которые сильно упростят вашу задачу

Контроль печати – это лишь одна из функций LanAgent.

Для обнаружения недобросовестных сотрудников будет также полезна функция контроля состава оборудования. Она предупредит вас, если работник снимет с компьютера планку оперативной памяти или отключит видеокарту и принесет из дома другую попроще.

Предотвращению утечки важной информации помогут контроль файлов, копируемых на съемные накопители или в интернет, а также снимки экрана монитора.

Практическое занятие №21
Настройка системы для задач аудита.

Ц е л ь : научится проводить аудит безопасности**.**

Проведение аудита безопасности также невозможно качественно осуществить без наличия системных журналов аудита ИБ. Однако, большое количество данных для обработки имеет и очевидный минус: нас может просто «засыпать» сообщениями, логами, уведомлениями. Необходимо выбрать самые значимые с точки зрения ИБ события, обогатить их данными от сторонних средств защиты, скоррелировать между собой и эффективно осуществлять по ним поиск. Поэтому в настоящей статье мы сконцентрируемся на наиболее полезных и эффективных (с нашей точки зрения) политиках аудита безопасности и типах событий безопасности на примере ОС Windows, а также рассмотрим использование утилиты Sysmon для обогащения данных журналов аудита безопасности. Начнем!

Как мы уже писали в предыдущей части, начиная с Microsoft Windows Server 2008 и Vista в Windows используются политики расширенного аудита информационной безопасности, которые позволяют следить практически за всеми значимыми событиями

безопасности. Пройдем последовательно по настройкам, эффективным для решения задач аудита ИБ и выработки целостной политики аудита безопасности.

Категория аудита	Подкатегория аудита	События аудита	EventID	Комментарии
Вход учетной записи	Аудит проверки учетных данных	Успех, Отказ	4776	Целесообразно контролировать на домен-контроллерах при использовании NTLM-аутентификации.
	Аудит службы проверки подлинности Kerberos	Успех, Отказ	4771	Неуспешная аутентификация учетной записи на контроллере домена с использованием Kerberos-аутентификации.
			4768	Запрос билета Kerberos, при этом следует анализировать коды ответа сервера.
	Примечание: Данный тип аудита следует включать на контроллерах домена, при этом для детального изучения попыток подключения и получения IP-адреса подключающегося устройства на контроллере домена следует выполнить команду nltest /dbflag:2080ffff и проводить аудит текстового лог-файла %windir%\debug\netlogon.log			
Управление учетными записями	Аудит управления учетными записями компьютеров	Успех	4741	Заведение устройства в домен Active Directory. Может использоваться злоумышленниками, поскольку любой пользователь домена по умолчанию имеет возможность завести в домен 10 устройств с установленным на них не контролируемым компанией ПО, в том числе вредоносным.
	Аудит управления группами безопасности	Успех, Отказ	4728	Добавление члена глобальной группы.
			4732	Добавление члена локальной группы.
			4756	Добавление члена универсальной группы.
	Аудит управления учетными записями пользователей	Успех, Отказ	4720	Создание учетной записи.
			4725	Отключение учетной записи.
			4740	Блокировка учетной записи.
			4723	Смена пароля.
			4724	Сброс пароля.
Подробное отслеживание	Аудит создания процессов	Успех	4688	При создании процесса.
			4689	При завершении процесса.
	Примечание: Для того чтобы для командного интерпретатора велась запись введенных команд, следует включить политику «Конфигурация компьютера - Конфигурация Windows - Административные шаблоны - Система - Аудит создания процессов -> Включать командную строку в события создания процессов». Примечание: Для того, чтобы велась запись выполняемых PowerShell-команд и загруженных PowerShell-модулей, следует включить в каталоге			

	«Конфигурация компьютера - Конфигурация Windows - Административные шаблоны - Компоненты Windows - Windows PowerShell» политики «Включить ведение журнала модулей» (в настройках политики указать все модули символом «*») и «Включить регистрацию блоков сценариев PowerShell» (в настройках политики отметить check-box «Регистрация начала или остановки вызова блоков сценариев»). Работа PowerShell-скриптов регистрируется с EventID=4104,4105,4106 в журнале Microsoft-Windows-PowerShell/Operational, а загрузка PowerShell-модулей регистрируется с EventID=800 в журнале Windows PowerShell.			
Вход/выход	Аудит выхода из системы	Успех	4634	Для неинтерактивных сессий.
			4647	Для интерактивных сессий и RDP-подключений.
	Примечание: При этом следует обращать внимание на код Logon Type, который показывает тип подключения (интерактивное, сетевое, с закэшированными учетными данными, с предоставлением учетных данных в открытом виде и т.д.).			
	Аудит входа в систему	Успех, Отказ	4624	При успешной попытке аутентификации. Создается на локальном ПК и на домен-контроллере при использовании NTLM и Kerberos-аутентификации.
			4625	При неуспешной попытке аутентификации. Создается на локальном ПК и на домен-контроллере при использовании NTLM аутентификации; при Kerberos-аутентификации на контроллере домена создается EventID=4771.
			4648	При попытке входа с явным указанием учетных данных, например, при выполнении команды runas, а также при работе «хакерской» утилиты mimikatz.
	Примечание: При этом следует обращать внимание на код входа (Logon Type), который показывает тип подключения (интерактивное, сетевое, с закэшированными учетными данными, с предоставлением учетных данных в открытом виде и т.д.). Целесообразно также обращать внимание на код ошибки (Status/SubStatus), который также сохраняется в событии аудита и характеризует причину неуспешного входа - несуществующее имя учетной записи, недействительный пароль, попытка входа с заблокированной учетной записью и т.д.			
	Аудит других событий входа и выхода	Успех, Отказ	4778	RDP-подключение было установлено.
			4779	RDP-подключение было разорвано.
	Аудит специального входа	Успех	4672	При входе с административными полномочиями.
Доступ к	Аудит сведений	Успех,	5145	При доступе к системных

объектам	об общем файловом ресурсе	Отказ		сетевым ресурсам, таким как \\C$\. Данное событие будет создаваться при работе ransomware, нацеленного на горизонтальное перемещение по сети.
	Аудит других событий доступа к объектам	Успех, Отказ	4698	При создании задания в «Планировщике задач», что часто используется злоумышленниками как метод закрепления и скрытия активности в атакованной системе.
Изменение политики	Аудит изменения политики аудита	Успех	4719	Изменение политики аудита.
			4906	Изменение настройки CrashOnAuditFail.
	Примечание: Изменить реакцию ОС на невозможность вести журнал аудита безопасности (настройка CrashOnAuditFail) можно в каталоге «Конфигурация компьютера - Конфигурация Windows - Параметры безопасности - Локальные политики - Параметры безопасности» в политике «Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности».			
Система	Аудит расширения системы безопасности	Успех	4610 4614 4622	При появлении в системе новых пакетов аутентификации, что не должно происходить несанкционированно.
			4697	При создании нового сервиса, что часто используется злоумышленниками как метод закрепления и скрытия активности в атакованной системе.

Кроме описанных выше настроек, имеет смысл также контролировать появление в журнале безопасности события с EventID=1102, которое формируется сразу после очистки журнала безопасности, что может говорить о вредоносной активности. Более того, разумно будет включить в каталоге «Конфигурация компьютера - Конфигурация Windows - Параметры безопасности - Локальные политики - Параметры безопасности» политику «Сетевая безопасность: ограничения NTLM: исходящий трафик NTLM к удаленным серверам» в значение «Аудит всего». После этого EventID=8001 в журнале Microsoft-Windows-NTLM/Operational будет содержать информацию об автоматической аутентификации на веб-ресурсах с учетной записью пользователя. Следующим шагом станет allow list с перечнем веб-ресурсов, которые легитимно могут запрашивать учетные записи, а указанную политику можно будет перевести в режим блокировки. Это не позволит вредоносным ресурсам получать NTLM-хэши пользователей, которые кликнули на ссылку из фишингового письма.

Обратим внимание и на то, что подсистема журналирования Windows весьма гибка и позволяет настроить аудит произвольных папок и веток реестра - следует лишь выбрать критичные для ИТ-инфраструктуры объекты аудита и включить данные опции.

Не лишним также будет обратиться к таким документам, как Microsoft Security Compliance Toolkit и CIS Microsoft Windows Benchmarks, в которых, в числе прочего, указаны рекомендуемые экспертами политики аудита.

Кроме задействования штатного функционала подсистемы журналирования, можно воспользоваться и официальной утилитой Sysmon из пакета Microsoft Windows Sysinternals, которая существенно расширяет и дополняет возможности мониторинга ОС. Данная утилита

позволяет проводить аудит создания файлов, ключей реестра, процессов и потоков, а также осуществлять мониторинг загрузки драйверов и библиотек, сетевых подключений, WMI-событий и именованных каналов. Из особо полезных функций отметим возможность утилиты показывать родительский процесс и командную строку процесса, отображать значение хэш-сумм при событиях создания процесса и загрузки драйверов и библиотек с указанием наличия и действительности цифровой подписи. Несложным путем можно автоматизировать сравнение полученных хэш-сумм с индикаторами компрометации (IoCs, Indicator of Compromise) из данных фидов CyberThreat Intelligence. Еще одной приятной опцией является возможность создания XML-конфигураций, в которых можно предельно четко указать объекты контроля и настройки работы Sysmon. Одними из наиболее продвинутых и детальных вариантов XML-конфигураций, с нашей точки зрения, являются конфиги https://github.com/ion-storm/sysmon-config и https://github.com/SwiftOnSecurity/sysmon-config.

Установка Sysmon предельно проста и также может быть легко автоматизирована:

1. Дистрибутив скачивается с https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Все исполняемые файлы подписаны.

2. Создается или скачивается по приведенным выше ссылкам xml-файл с конфигурацией Sysmon.

3. Установка sysmon для x64 производится командой:

C:\folder\sysmon64.exe -accepteula -i C:\folder\sysmonconfig-export.xml, где sysmonconfig-export.xml – файл конфигурации, sysmon64.exe – файл-установщик.

Поддерживается запуск установки с сетевой папки.

4. После установки создается журнал Microsoft-Windows-Sysmon/Operational, размер которого мы сразу рекомендуем увеличить как минимум до 100 Мб.

Перезапуск устройства не требуется. Sysmon работает в виде сервиса, его исполняемый файл находится в C:\Windows\sysmon64.exe. По нашим подсчетам, footprint на конечной системе даже при использовании максимально детального конфига Sysmon не превышает 5-10% ЦПУ и около 100 Мб ОЗУ.

Практическое занятие №22-23
Настройка контроля целостности и замкнутой программной среды.

Для контроля целостности компонентов ОС используется **IMA**. Компонент архитектуры измерения целостности (**IMA**) производит проверки целостности во время выполнения файлов с использованием хэшей, сравнивая их со списком допустимых хэшей.

Примечание.
Работает, начиная с версии **ядра 5.15.*** из репозитория РЕД ОС.

Для проведения контроля целостности необходимо перейти в сеанс пользователя **root**:

```
su -
```

и выполнить следующие действия:

1. Установить пакеты для работы с **IMA**:

```
dnf install ima-manage openssl-gost-engine keyutils
```

2. Включить ГОСТ в **openssl**:

```
openssl-switch-config gost
```

3. Сгенерировать пару ключей.

а) Создать файл **test-ca.conf** со следующим содержимым:

[req] distinguished_name = req_distinguished_name
prompt = no string_mask = utf8only
x509_extensions = v3_ca
[req_distinguished_name]
O = IMA-CA
CN = IMA/EVM certificate signing key
emailAddress = ca@ima-ca
[v3_ca]
basicConstraints=CA:TRUE
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer

Значения полей **O**, **CN**, **emailAddress** являются произвольными, можно заменить их на свои. Место расположения файла не играет роли, он нужен только для создания пары ключей один раз.

б) Сгенерировать ключевую пару:

```
openssl req -nodes -x509 -utf8 -days 10000 -batch -config test-ca.conf -newkey gost2012_512 -pkeyopt paramset:A -out x509_evm.der -outform DER -keyout privkey_evm.pem
```

4. Создать папку **/etc/keys** и скопировать в нее открытый ключ **x509_evm.der**.

```
mkdir /etc/keys

cp x509_evm.der /etc/keys/x509_evm.der
```

Секретный ключ «**privkey_evm.pem**» сохранить в каталоге, недоступном для всех пользователей, кроме администратора **root**, например:

```
mv privkey_evm.pem /root/privkey_evm.pem
```

5. В файл**/usr/lib/systemd/system/dracut-pre-mount.service** в секцию [**Service**] добавить строку **KeyringMode=shared**.

6. В файле **/usr/lib/dracut/modules.d/98ima/module-setup.sh** в функции **check()** изменить **255** на **0**:

called by Dracut check() {return 0}

7. Создать файл **/etc/sysconfig/ima-policy** со следующим содержимым:

PROC_SUPER_MAGIC
dont_measure fsmagic=0x9fa0
dont_appraise fsmagic=0x9fa0
SYSFS_MAGIC
dont_measure fsmagic=0x62656572
dont_appraise fsmagic=0x62656572
DEBUGFS_MAGIC
dont_measure fsmagic=0x64626720
dont_appraise fsmagic=0x64626720
TMPFS_MAGIC
dont_measure fsmagic=0x01021994
dont_appraise fsmagic=0x01021994
RAMFS_MAGIC
dont_appraise fsmagic=0x858458f
DEVPTS_SUPER_MAGIC
dont_measure fsmagic=0x1cd1
dont_appraise fsmagic=0x1cd1

```
# BINFMTFS_MAGIC
dont_measure fsmagic=0x42494e4d
dont_appraise fsmagic=0x42494e4d
# SECURITYFS_MAGIC
dont_measure fsmagic=0x73636673
dont_appraise fsmagic=0x73636673
# SELINUX_MAGIC
dont_measure fsmagic=0xf97cff8c
dont_appraise fsmagic=0xf97cff8c
# CGROUP_SUPER_MAGIC
dont_measure fsmagic=0x27e0eb
dont_appraise fsmagic=0x27e0eb
# CGROUP2_SUPER_MAGIC
dont_measure fsmagic=0x63677270
dont_appraise fsmagic=0x63677270
# NSFS_MAGIC
dont_measure fsmagic=0x6e736673
dont_appraise fsmagic=0x6e736673
appraise func=BPRM_CHECK appraise_type=imasig
appraise func=BPRM_CHECK appraise_type=imasig
appraise func=FILE_MMAP mask=MAY_EXEC appraise_type=imasig
appraise func=FILE_MMAP mask=MAY_EXEC appraise_type=imasig
#appraise func=MODULE_CHECK appraise_type=imasig
#appraise func=FIRMWARE_CHECK appraise_type=imasig
# this is only for newer kernels that support loading policies
# from file by writing the file path to the ima sysfs node
#appraise func=POLICY_CHECK appraise_type=imasig
```

8. Запустить утилиту **ima-manage** с ключом **init**:

```
ima-manage init
```

9. В файле **/etc/ima-manage.conf** изменить значение **HASHALGO="sha256"** на **HASHALGO="streebog512"**.

10. Запустить утилиту «**ima-manage**» с ключом «**signfs**» и указанием пути размещения секретного ключа:

```
ima-manage signfs /root/privkey_evm.pem
```

11. Запустить утилиту **ima-manage** с ключом «**enforce**»:

```
ima-manage enforce
```

Дождаться завершения работы утилиты и предложения перезагрузки. Дать согласие на перезагрузку системы.

Для проверки работы защиты от запуска неподписанных исполняемых файлов создайте копию существующего исполняемого файла, например:

```
cp /bin/ls ls.copy
```

Попробуйте его запустить, будет выведена ошибка:

```
./ls.copy
bash: ./ls.copy: Permission denied
```

При этом в логе аудита появится запись о запрете запуска неподписанного файла:

```
grep -i ima /var/log/audit/audit.log | tail -n 1
```

```
type=INTEGRITY_DATA msg=audit(1638974599.231:11315): pid=2800 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 op=appraise_data cause=IMA-signature-required comm="bash" name="/home/user/ls.copy" dev="dm-0" ino=946370 res=0 errno=0UID="user" AUID="user"
```

Для запуска сторонних файлов, не имеющих подписи, необходимо от имени администратора подписать файл:

```
evmctl ima_sign --hashalgo md_gost12_512 --key <путь_к_приватному_ключу_privkey_evm.pem> <путь_к_файлу>
```

Например:

```
evmctl ima_sign --hashalgo md_gost12_512 --key /root/privkey_evm.pem /home/user/ls.copy
```

Для включения режима журналирования (система не будет запрещать запуск неподписанных файлов, но будет записывать попытки их запуска) необходимо в файле **/etc/default/grub** изменить параметр **ima_appraise=enforce** на **ima_appraise=log**.

После этого обновите конфигурацию загрузчика ОС, для этого выполните в терминале команду:

- для систем, использующих **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- для систем, использующих **UEFI**:

```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Практическое занятие №24-25

Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.

Ход работы:

На сегодняшний день главной целью злоумышленников является не просто взлом сети или проникновение в систему, а извлечение прибыли.

И хотя для защиты своих информационных активов компании используют различные меры по обеспечению ИБ, тем не менее, инциденты, связанные с информационной безопасностью, и в первую очередь с кражей данных, все равно происходят.

Дело в том, что внедрение только средств защиты, как правило, не гарантирует высокую степень защищенности. В результате нет понимания, насколько полученный уровень информационной безопасности соответствует требуемому, а значит и насколько эффективна вся система обеспечения ИБ в целом. Внутренние и внешние аудиты не являются достаточными для решения данной задачи, поскольку носят периодический характер. Компании, внедряя основные элементы безопасности, зачастую не уделяют должного внимания такому важному элементу обеспечения ИБ, как мониторинг системы информационной безопасности.

В результате, затратив силы и средства на внедрение средств защиты, компании считают задачу выполненной, но на проверку оказывается, что:

- критичные системы уязвимы и доступны для злоумышленников;
- на рабочих станциях установлено неразрешенное ПО;
- конфигурации не соответствуют разработанным частным политикам;

- события, свидетельствующие об инциденте ИБ, остаются незамеченными;
- выявив инцидент ИБ, нет четко определенной процедуры, что с ним делать дальше и кто этим должен заниматься;
- у администраторов информационной безопасности нет полной и целостной картины о состоянии ИБ, есть только фрагментарные представления;
- и т.д.

Большинство таких фактов можно было бы избежать, если бы в компании был реализован комплексный мониторинг ИБ, своевременное выявление инцидентов, реагирование на них и эффективное разрешение.

Комплексный мониторинг ИБ подразумевает сбор и анализ событий безопасности от различных систем защиты, устройств и приложений, сбор конфигурационных данных, данных об уязвимостях и т.д. Это позволяет получить полную и достоверную информацию об имеющихся событиях и уязвимостях ИБ, текущих настройках, т.е. иметь целостную картину текущей защищенности компании. Осуществляя такой контроль, организации имеют возможность оперативного управления информационной безопасностью, исправляя выявляемые отклонения, своевременно разрешая инциденты ИБ, устраняя уязвимости, принимая меры по корректировке средств защиты и т.д.

Подтверждение важности и необходимости комплексного мониторинга нашло отражение в различных стандартах в области информационной безопасности, таких, как: PCI DSS, ISO/IEC 27001:2005, SOX, Basel II, СТО БР ИББС-1.0-2006, СТР-К.

Централизация оперативного управления ИБ

Собранная в ходе комплексного мониторинга информация поступает в единый центр, где она обрабатывается и представляется в наглядном и удобном виде. Здесь же осуществляется реагирование и разрешение инцидентов ИБ, устранение выявленных отклонений. Построение такого Центра оперативного управления ИБ (Security Operations Center, SOC (см. рис.1)) является непростой задачей.

Центр оперативного управления ИБ позволяет контролировать и оперативно управлять информационной безопасностью компании в режиме реального времени, быть уверенным в том, что требуемый уровень обеспечения ИБ достигнут и поддерживается, отслеживать выполнение заданных целевых показателей эффективности (KPI) обеспечения ИБ.

Центр оперативного управления ИБ позволяет отслеживать происходящие в информационной системе события, связанные с ИБ, анализировать и сопоставлять их с другими данными, представлять собранную информацию в наглядном и удобном виде, контролировать имеющиеся уязвимости, осуществлять контроль конфигураций, отслеживать степень выполнения требований законодательства, нормативных актов и корпоративных политик, а также оперативно реагировать на выявленные инциденты ИБ. То есть предоставляет полную картину текущего состояния информационной безопасности компании, что позволяет оперативно устранять выявляемые отклонения и обеспечивать заданный уровень ИБ.

Ключевыми факторами, обеспечивающими эффективность подобных центров, являются: внедрение процессов мониторинга, управления уязвимостями и инцидентами, правильное разграничение ответственности между сотрудниками внутри компании, разработка и внедрение регламентов реагирования на инциденты ИБ и их последующего разбора.

В многофилиальных компаниях с развитой ИТ-инфраструктурой и большим количеством разнообразных средств защиты без специализированных технических средств реализовать полноценный комплексный мониторинг ИБ весьма проблематично.

Рис. 1. Центр оперативного управления ИБ

Также многое зависит от качества настроек технических средств и квалифицированных действий обслуживающего персонала.

Внедряя Центр оперативного управления ИБ, компании одновременно реализуют часть процессов системы управления ИБ (СУИБ) в соответствии со стандартом ISO27001 (процесс управления инцидентами ИБ, управление уязвимостями, управление изменениями, контроль соответствия законодательным и отраслевым требованиям), а также выполняют часть требований стандарта PSI DSS (требования разделов 1, 6, 10, 11, 12).

Таким образом **Центр оперативного управления ИБ** представляет собой набор связанных и работающих процессов управления ИБ (мониторинг, управление инцидентами, управление уязвимостями, инвентаризация активов, управление изменениями, контроль политик безопасности) и автоматизирующих их технических систем:

- Мониторинга состояния ИБ:
  - мониторинг событий ИБ;
  - аудит действий пользователей;
  - управление уязвимостями/контроль конфигураций;
- Управления инцидентами ИБ;
- Контроля соответствия требованиям законодательства, международных и отраслевых стандартов, внутренних корпоративных политик.

Мониторинг состояния ИБ

Система управления (мониторинга) событиями ИБ (Security Information Management System, SIMS) – реализует комплексный подход к решению задач сбора, анализа (корреляции) и контроля событий ИБ от различных средств защиты, что позволяет в режиме реального времени эффективно идентифицировать инциденты информационной безопасности (с дальнейшей их передачей в систему управления инцидентами), получать реальные данные для анализа и оценки рисков, для принятия обоснованных и адекватных имеющимся рискам решений по обеспечению ИБ.

Система управления событиями ИБ помогает решить следующие задачи:

- управление большим объемом событий ИБ;
- получение полной картины происходящего в ИС;
- мониторинг текущего уровня обеспечения безопасности (контроль достижения заданных показателей эффективности (KPI) обеспечения ИБ);
- своевременное обнаружение инцидентов ИБ;

- получение реальных данных для анализа и оценки рисков;
- принятие обоснованных решений по управлению ИБ;
- выполнение требований законодательства и нормативных актов по мониторингу событий, связанных с ИБ (ISO/IEC 27001:2005, SOX, Basel II, PCI DSS, СТО БР ИББС-1.0-2006, Федеральный закон о персональных данных (№512-ФЗ), СТР-К, ГОСТ Р ИСО/МЭК 17799-2005).

На рынке систем управления событиями информационной безопасности представлены технические решения различных производителей, они отличаются по функционалу, спектру решаемых задач, сфере применения:

- Symantec Security Information Manager (SSIM);
- nFX SIM One (netForensics);
- ArcSight Enterprise Security Management (ArcSight ESM);
- Cisco Security Monitoring, Analysis and Response System (CS-MARS).

Система аудита действий пользователей обеспечивает регистрацию и анализ действий пользователей (прежде всего на уровне БД), рассылку уведомлений в режиме реального времени и подготовку отчетов о том, кто получает доступ, к какой именно информации, и как эти действия могут нарушить требования внешних регулирующих органов или внутренние правила по информационной безопасности компании.

Система аудита действий пользователей помогает решить следующие задачи:

- контроль злонамеренных действий пользователей;
- защита от утечки конфиденциальной информации;
- получение ответа на вопросы: «Кто? Что сделал? Когда? Где? Откуда? Куда? С помощью каких средств?»;
- подготовка отчетов различного уровня (от руководителя компании до администратора информационной безопасности).

Для контроля действий пользователей могут быть использованы решения компании Imperva, а также отлично зарекомендовавшие себя продукты nFX Data One (netForensics) и Oracle Audit Vault, первый из которых легко интегрируется с другими продуктами компании netForensics, а второй – разработан специально для одной из наиболее распространенных СУБД – Oracle.

Система управления уязвимостями/контроля конфигураций позволяет получать данные по имеющимся уязвимостям в режиме реального времени, отслеживать динамику их

устранения, контролировать производимые изменения, а также обеспечивает автоматизацию таких задач, как: инвентаризация ресурсов и контроль конфигураций. Поиск уязвимостей критичных ресурсов проводится на постоянной основе различными способами:

- сетевое сканирование;
- тест на проникновение;
- системные проверки;
- анализ защищенности СУБД;
- анализ защищенности Web-приложений.

Система реализуется на базе продукта MaxPatrol (Positive Technologies).

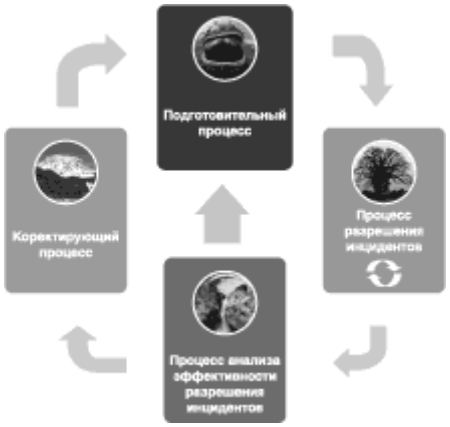
Управление инцидентами ИБ

Система управления инцидентами ИБ осуществляет регистрацию, оперативное реагирование и эффективное разрешение инцидентов ИБ, а также реализует полный цикл работы с инцидентами.

От того насколько быстро и грамотно компания среагирует и разрешит возникший инцидент информационной безопасности, зависит размер ущерба, наносимого ей в результате инцидента, поэтому подготовка к разрешению инцидентов приобретает особое значение.

Подготовительный этап включает планирование, определение ответственных, разграничение обязанностей, разработку планов по разрешению инцидентов и т. д. Далее осуществляется непосредственно регистрация инцидентов ИБ и реагирование на них с последующим разрешением.

Рис. 2. Управление инцидентами ИБ



В процессе управления инцидентами информационной безопасности важно не только разрешить эти инциденты, но и проанализировать, насколько эффективно осуществляется их

разрешение. Необходимо периодически тестировать разработанные планы для поддержания их в актуальном рабочем состоянии и для своевременного улучшения. Кроме того, необходимо проводить анализ произошедших инцидентов с целью дальнейшей корректировки текущих мер защиты и принятия мер проактивной защиты.

Если при анализе выявлены незначительные отклонения, то проводятся корректирующие действия. Если же выявлены системные ошибки, обнаружена неэффективность применяемых планов и т. п., то производится активация подготовительного этапа.

Общая схема управления инцидентами ИБ представлена на рис. 2.

Построение **Системы управления инцидентами ИБ** предполагает внедрение процесса управления инцидентами ИБ и (опционально) его автоматизацию.

Контроль соответствий

Система контроля соответствий позволяет выполнять регулярные технологические проверки соответствия информационных систем внутренним политикам безопасности компании, техническим стандартам, требованиям нормативных актов, международным стандартам и т. п. Результат проверки предоставляется в виде детального отчета.

Данная система предоставляет возможность определить внутренний стандарт на базе:

- международных стандартов (ISO 27001, PSI DSS и др.);
- рекомендаций производителя;
- «Best practice» NSA, NIST, CIS;
- внутренних требований,

а также постоянно контролировать соблюдение стандартов для:

- сетевого оборудования;
- прикладных систем (ERP, CRM);
- операционных систем UNIX и Windows;
- различных СУБД.

Система может быть реализована на базе продуктов MaxPatrol (Positive Technologies) и Control Compliance Suite (Symantec).

Построение Security Operation Center, SOC

Возможны различные варианты построения SOC в зависимости от степени зрелости и текущих задач компании: от внедрения отдельных систем до комплексных решений.

При реализации сложных масштабных проектов в ряде ситуаций оптимально поэтапное внедрение, когда на каждом этапе увеличивается область применения SOC как по территориальному охвату (например, сначала головной офис, затем регионы), так и по функциональным системам (например, сначала система управления событиями ИБ, а затем система управления уязвимостями).

Таб. 1. Использование Центра оперативного управления ИБ для решения задач бизнеса

Задачи бизнеса	Решение с помощью SOC
Сокращение расходов и потерь	Создание Центра оперативного управления позволят сократить расходы за счет централизации управления, а также снизить ущерб, наносимый в результате возникновения инцидентов ИБ, за счет своевременного и эффективного реагирования. Использование процессного подхода делает реагирование и разрешение инцидентов информационной безопасности более оперативным и позволяет использовать как собственный, так и мировой опыт по разрешению инцидентов ИБ.
Повышение стоимости компании	Центр оперативного управления ИБ повышает управляемость и стабильность компании, что ведет к увеличению ее стоимости. Это становится особенно актуально, когда речь идет о слиянии и поглощении. Потенциальный собственник предпочитает понимать, какие инструменты используются для оперативного управления ИБ, ценит использование комплексного и системного подхода для решения задач информационной безопасности.
Соответствие требованиям законов и нормативных актов как российских, так и международных	Наличие Центра оперативного управления свидетельствует о выполнении требований и рекомендаций по мониторингу и управлению инцидентами ИБ, прямо или косвенно присутствующих как в международных стандартах и нормативных актах (ISO/IEC 27001:2005, PCI DSS, Basel II, SarbanesQOxley Act), так и в российских (СТО БР ИББСQ1.0Q2006, Федеральный закон о персональных данных (№512QФЗ), СТРQК, ГОСТ Р ИСО/МЭК 17799Q2005).
Управление операционными рисками	Контроль операций и контроль конфигураций являются составляющими управления операционными рисками. Центры оперативного управления ИБ осуществляют мониторинг всех производимых действий, отслеживают факты изменений конфигурационных настроек,

	контролируют их соответствие установленным в компании требованиям, политикам. Центр оперативного управления может быть использован как средство автоматизации при анализе рисков, предоставляя реальные данные о текущих уязвимостях и угрозах.

Использование решений нескольких производителей позволяет учесть масштаб, ИТ-инфраструктуру и другие особенности каждой компании. Примеры использования SOC приведены в таб. 1.

Выгоды, получаемые компанией при внедрении SOC

• Непрерывное усовершенствование защитных мер для обеспечения безопасности: постоянный анализ текущих событий и инцидентов ИБ, выяснение причин их возникновения с привлечением различных подразделений, позволяет оценить эффективность текущих мер защиты, понять их недостатки и выработать предложения по их замене или корректировке.

• Снижение затрат: при небольшом штате сотрудников, когда «не хватает рук», SOC позволяет сократить ресурсы, требуемые при ручной обработке событий ИБ и при увеличении количества контролируемых средств защиты, не требует увеличения штата, а напротив, путем сведения данных на одну консоль и автоматизации проводимого анализа событий ИБ, позволяет оптимизировать работу сотрудников.

• Разделение полномочий контроля за ИТ-системами: средства защиты, их администрирование и эксплуатация, как правило, находятся в ведении подразделения ИТ, в то время как ИБ отводятся только функции контроля. SOC – это, пожалуй, единственный инструмент контроля в руках у подразделений ИБ, позволяющий им отслеживать действия в ИТ-системах, что объективно снижает влияние человеческого фактора и повышает уровень информационной безопасности компании.

• Оптимизация слияния компаний: SOC позволяет эффективно привести присоединяемую компанию в соответствие со стандартами ИБ, принятыми в головной компании. SOC дает возможность не только оперативно обнаружить расхождения, но и отследить их устранение с возможностью выставления и контроля соответствующих KPI ответственным за слияние подразделениям.

• Оптимизация затрат на обеспечение ИБ: данные, предоставляемые SOC, существенно уточняют оценку рисков, которая является основой в выборе тех или иных мер защиты. Кроме этого, формализация процедур снижает косвенные затраты компании, т. к. вопросы согласований без качественного обоснования занимают значительное количество рабочего времени сотрудников.

Построение Центра оперативного управления ИБ на базе продуктов компании Symantec

Для построения Центров оперативного управления ИБ используются решения нескольких производителей, что позволяет учесть масштаб, ИТ-инфраструктуру и другие особенности каждой компании.

Рассмотрим построение Центра оперативного управления ИБ на базе продуктов компании Symantec:

• Symantec Security Information Manager (Symantec SIM);

• Symantec Control Compliance Suite (Symantec CCS).

Symantec SIM используется для комплексного мониторинга и автоматизации процесса управления инцидентами ИБ, а Symantec CCS для контроля политик безопасности. Оба продукта хорошо интегрируются друг с другом и объединены в единое решение в 9-ой версии продукта Symantec Control Compliance Suite.

Эти продукты можно также использовать для закрытия соответствующих требований при выполнении проектов по PCI DSS и СТО БР ИББС-1.0.

Symantec Security Information Manager

Основные задачи, решаемые Symantec SIM:

• управление событиями ИБ;

• управление инцидентами ИБ;

• контроль активности пользователей;

• контроль состояния безопасности компании.

Основные возможности Symantec SIM представлены ниже.

Сбор данных и анализ безопасности в режиме реального времени

Продукт Symantec SIM осуществляет централизованный сбор событий ИБ от программно-технических средств более, чем 100 различных производителей. Для

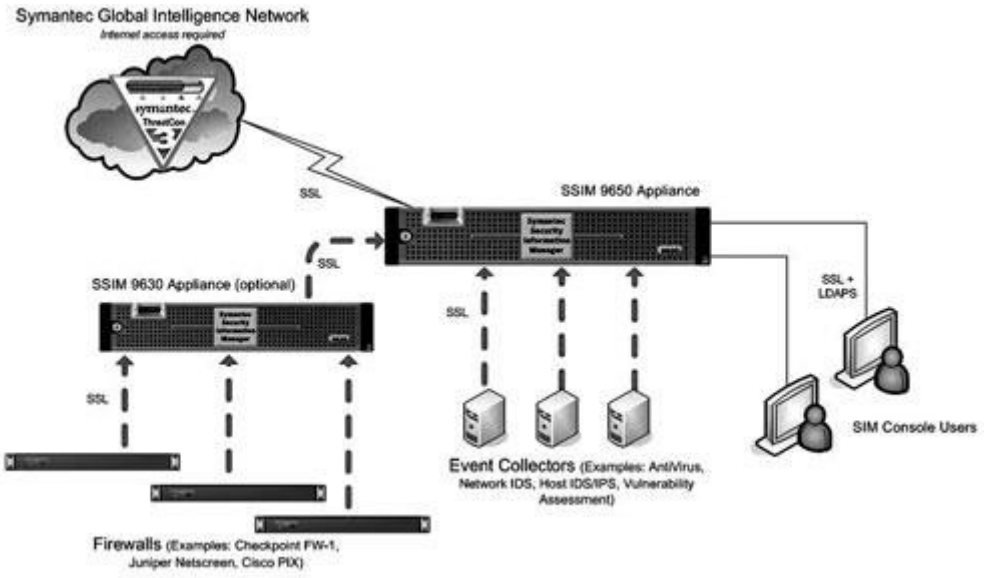
«неподдерживаемых» систем есть возможность разработки собственных коллекторов для сбора событий ИБ при помощи специализированного программного пакета Collector Studio.

На основе собранных данных Symantec SIM помогает выявлять угрозы безопасности, направленные на наиболее важные бизнес-приложения, определять их приоритеты, анализировать и устранять эти угрозы.

Сопоставление недостатков защиты сети и хостов в режиме реального времени с помощью службы Symantec Global Intelligence Network – это одно из ключевых преимуществ продукта Symantec SIM, делающее его системой оперативного реагирования на инциденты мирового класса с акцентом на обеспечение безопасности наиболее важных для бизнеса информационных ресурсов.

Symantec Global Intelligence Network – глобальная сеть, использующая ловушки для обнаружения злонамеренной активности по всему миру. Большое внимание уделяется анализу подозрительной активности по различным портам/протоколам. Исследуются приложения, использующие эти порты/протоколы, проверяется, не были/появлялись ли новые уязвимости в этих приложениях, анализируется вероятность использования приложений в злонамеренных целях. Также создается статистика наиболее атакующих и атакуемых систем. Вся эта информация перерабатывается в правила и используется в Symantec SIM при анализе и корреляции событий.

Рис. 3. Архитектура Symantec SIM



Анализ безопасности в режиме реального времени осуществляется с использованием внешнего стандарта выявления угроз безопасности – процесс, описанный в открытых стандартах Distributed Management Task Force (DMTF). Данный метод предусматривает

классификацию угроз и проблем безопасности с учетом степени воздействия события на среду, способа атаки и целевых ресурсов. Такая классификация, называемая «Эффекты, механизмы и ресурсы» (EMR), лежит в основе модуля анализа данных Symantec SIM. Благодаря гибкости интеллектуальных правил на основе шаблонов, отдельное правило может занять место нескольких более конкретных правил, применяемых в стандартных подходах.

В результате значительно упрощается процедура обслуживания и создания правил, которые могут охватывать множество условий.

В системе заведено большое количество предопределенных правил корреляции, есть возможность создавать свои собственные правила. Можно задавать правила отрицательного условия, которые срабатывают в случае отсутствия события в течение заданного времени. Это очень полезно для контроля поступления событий от определенного источника данных.

Управление инцидентами

На основе созданных правил формируются инциденты ИБ, которые могут быть объединены в иерархию инцидентов. Каждому инциденту назначается приоритет в соответствии с указанными сведениями о защищаемых активах.

В Symantec SIM реализована встроенная система управления инцидентами, позволяющая назначить ответственного за инцидент, эскалировать инциденты, автоматизировать процесс контроля разрешения инцидентов, передать инцидент во внешнюю службу Help Desk для обработки, получить результат его разрешения (обратная связь) и т.д.

Таким образом, продукт Symantec SIM также используется для автоматизации и документирования разрешения инцидентов.

Хранение данных

Кроме сбора данных компании должны соблюдать официальные требования по хранению архивов, обеспечивая надлежащую работу средств хранения и извлечения данных. Продукт превосходит стандартные продукты контроля информации о безопасности на основе реляционных баз данных, для которых характерны дополнительные начальные затраты и необходимость длительного администрирования баз данных. С продуктом Symantec SIM не требуется администрирование базы данных. Продукт сохраняет события в архивных файлах в указанном месте. Архив реализован в виде самостоятельного модуля. Он

отслеживает использование диска и срок хранения отдельных архивных файлов. При достижении указанного ограничения дисковой памяти или даты истечения срока действия файла Symantec SIM удаляет старые архивные файлы, чтобы освободить место для новых файлов. Для хранения файлов можно выбрать программно-аппаратный комплекс, напрямую подключенный диск (DAS), сетевое устройство хранения (NAS) или сеть хранения данных (SAN). Архивы Symantec SIM работают быстрее обычных баз данных, поскольку в отличие от нескольких сотен функций базы данных они оптимизированы для выполнения одной задачи – сохранения большого объема событий. Коэффициент сжатия в продукте Symantec SIM достигает 30:1. Нормализованные данные вместе с исходной информацией о событиях фиксируются и сохраняются для анализа происшествий.

Для обеспечения конфиденциальности и целостности архивы имеют электронную подпись.

Отчетность

Продукт Symantec SIM позволяет создавать отчеты для руководителей, технические отчеты и отчеты о контроле, содержащие наглядное представление уровней серьезности угроз и состояния безопасности компании. Предусмотрено более 400 готовых отчетов – от соблюдения требований до различных аспектов защиты.

При необходимости с помощью мастера запросов можно создать собственные отчеты. В состав Symantec SIM входят стандартные шаблоны оценки соблюдения требований PCI DSS, SOX и др.

При передаче собранных данных между компонентами Symantec SIM обеспечивается конфиденциальность и целостность передаваемой информации.

Продукт предоставляет возможность его внедрения в различных вариантах, в соответствии с потребностями компании, а также обеспечивает возможность построения резервируемого, распределенного и масштабируемого решения по его внедрению.

Общая архитектура Symantec SIM представлена на рис. 3.

Symantec SIM – PCI DSS

Компания «Инфосистемы Джет» использует продукт Symantec SIM в проектах по PCI DSS для закрытия требований стандарта по отслеживанию всех обращений к сетевым ресурсам и данным о держателях платежных карт (требования раздела 10).

Наличие в продукте возможности разработки собственных коллекторов для сбора событий ИБ, а также поддержка русского языка, позволяет собирать данные с АБС собственной разработки и «неподдерживаемых» на данный момент систем.

Symantec SIM, с одной стороны, является недорогим решением для небольшого отдела процессинга. С другой стороны, в последствие это решение может быть легко масштабировано до размеров всей компании.

Данный продукт уже использовался компанией «Инфосистемы Джет» в ряде банков и входит в состав типового решения в проектах по PCI DSS.

В частности, данное решение было использовано в проекте по приведению процессинговых систем ЗАО «Компания объединенных кредитных карточек» в соответствие с требованиями PCI DSS.

Symantec Control Compliance Suite

Продукт Symantec CCS осуществляет автоматический контроль отклонений от стандартов безопасности и обеспечивает полный охват жизненного цикла задач ИТ-соответствия, включая управление политиками безопасности, оценку технических и административных контролей, отчетность и устранение недостатков.

Подход компании Symantec по управлению соответствием состоит в следующем (рис. 4):

1. Обозначить риски и разработать политики безопасности.
2. Провести оценку инфраструктуры и процессов.
3. Отслеживать и демонстрировать соответствие.
4. Оценить риски и устранить проблемы.

Продукт состоит из 4-х логических элементов: Policy, Response Assessment (RAM), Standards и SIM (описание SIM см. выше).

Встроенный модуль Policy позволяет определить внутреннюю политику вручную или на базе:

- международных стандартов (ISO 27001, PCI DSS и др.);
- рекомендаций производителя;
- «Best practice» NSA, NIST, CIS;
- внутренних требований.

В дальнейшем созданными политиками можно управлять, проверять, утверждать, распространять через web-портал, привязывать к тем или иным стандартам, нормативным документам.

Оценка состояния безопасности и обеспечение соответствия созданным политикам осуществляется для следующих операционных систем и приложений: Windows®, UNIX®, Linux®, NetWare®, SQL Server, Oracle® и Exchange.

Рис. 4. Управление соответствием CCS

Поиск уязвимостей критичных ресурсов и несоответствия конфигурационных настроек проводится на агентной и безагентной основе (рис. 5). Продукт Symantec CCS позволяет качественно оценить и постоянно контролировать соблюдение стандартов с целью быстрого выявления отклонений (систем, не соответствующих требованиям). Оценка соответствия техническим стандартам посредством подсчета баллов «соответствует/не соответствует», позволяет избежать многочасовых ручных операций по выявлению и анализу отклонений. Ссылка на результаты проверки на соответствие отправляется администратору по электронной почте, так что он может их просмотреть из любой точки ИТ-инфраструктуры с помощью браузера Microsoft Internet Explorer. Благодаря выявлению тенденций на основе логической иерархической группировки и детальному анализу несоответствующих требованиям систем обеспечивается быстрое устранение отклонений. В результате уменьшается риск возникновения несоответствий, брешей в системы безопасности и нарушений в работе бизнеса. По выявленным проблемам создаются всеобъемлющие перечни необходимых мероприятий, например, встроенные рекомендации, списки исправлений, которые необходимо получить из базы данных исправлений Shavlik®. В продукте реализована интеграция с системами обработки запросов, предоставляется возможность задания автоматического исправления выявленных отклонений.

Встроенный модуль Entitlement Manager собирает действующие права доступа к данным по всему предприятию, преобразует их в согласованный и удобочитаемый формат, классифицирует данные и передает информацию о разрешениях для утверждения бизнес-

владельцам этих данных. Предоставляет детальные отчеты о правах, показывающих: «кто имеет доступ к определенной информации», «к какой информации имеет доступ данное лицо» и «кто является бизнес-владельцем этой информации».

Symantec CCS также осуществляет проверку как технических, так и НЕтехнических (административных) контролей. Встроенный модуль Response Assessment (RAM) автоматизирует оценку нетехнических контролей. Большинство объектов, о которых упоминается в нормативных актах и стандартах, представляют собой административные средства управления. Организации часто опираются на оценки на бумаге, составление которых требует больших трудозатрат и которыми трудно управлять. Модуль RAM управляет процессом ручной оценки от создания и распространения анкет до анализа собранных данных:

• Создание из встроенных шаблонов или импорт из документов или создание новых опросов.

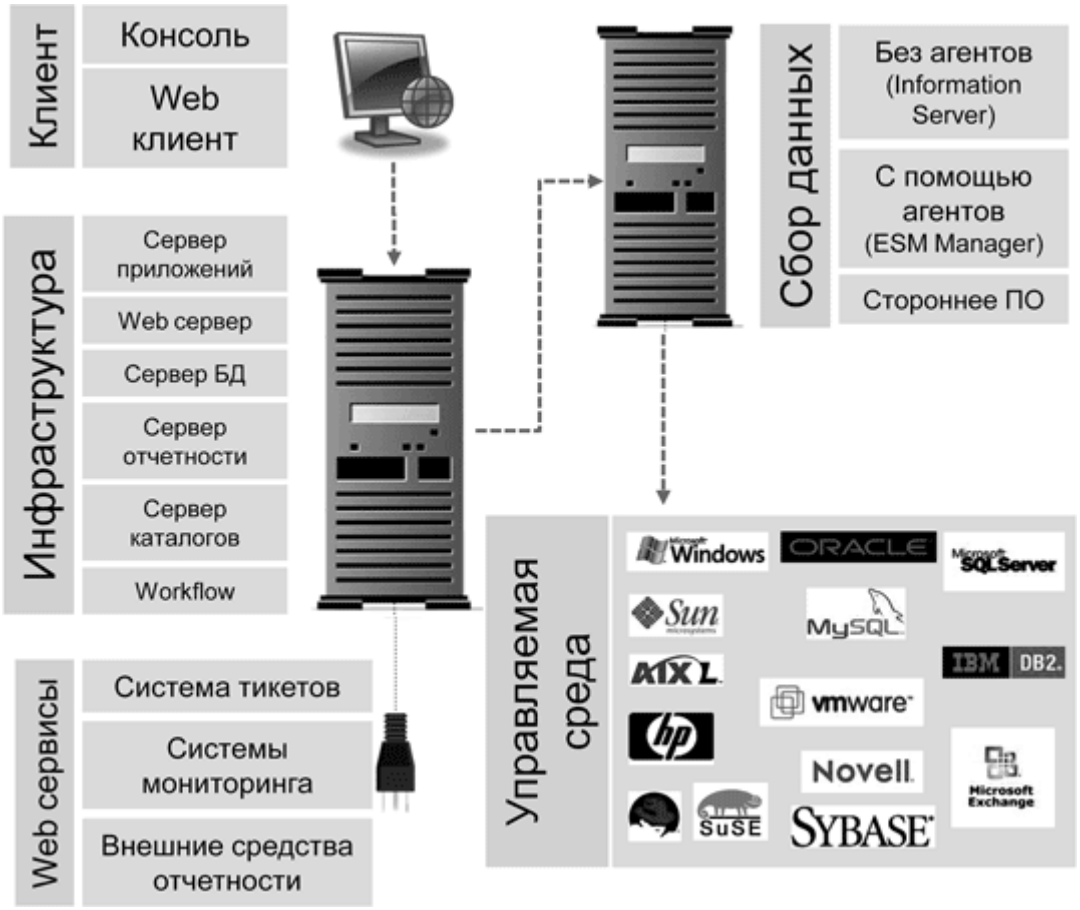
• Отслеживание ответов (принятие, запросы на пояснение.

• Создание списков заданий на исправление с указанием владельца задания и конкретных действий.

• и т.д.

При создании опросов есть возможность установить пороговые значения для успешного завершения опроса и количество попыток, а также оценивать результаты и отображать числовые значения в панели анализа. В качестве доказательств прикрепляются документы различных типов (до 3-х документов на вопрос) или даются ссылки. Имена документов и ссылки отображаются в панели анализа, сами документы хранятся в БД SQL, допускается их редактирование / удаление из БД.

Рис. 5. Общая архитектура CCS 9.0



В продукте Symantec CCS также реализовано немедленное всеобъемлющее устранение отклонений в виде процедуры с обратной связью, гарантирующей сведение уязвимостей к минимуму: автоматизация управления изменениями в организациях, использующих продукты Remedy® или HP® Service Desk, с возможностью подтверждения полноты и точности корректирующих действий. При проведении оценки соответствия автоматически (или полуавтоматически – требуется просмотр и утверждение пользователем) открываются «инциденты», в продуктах Remedy или HP Service Desk (с помощью встроенного интерфейса). По всем инцидентам, открытым с помощью Symantec CCS, подготавливаются соответствующие отчеты, включая просмотр заметок и состояния.

• Осуществляется контроль итогового статуса «fixed» или «closed» для открытых инцидентов, а также – корректного выполнения требуемых заданий.

Таким образом, продукты CCS и SIM, осуществляя консолидированный обзор текущего соответствия и данных конфигурации (CCS) и мониторинг ИТ-среды в реальном времени (SIM), реализуют комплексный мониторинг ИБ компании. И вместе с внедрением соответствующих процессов управления ИБ (управление инцидентами, управление уязвимостями, инвентаризация активов, управление изменениями, контроль политик

безопасности) позволяют построить эффективный Центр оперативного управления информационной безопасностью.

Практическое занятие №28-29
Оформление основных эксплуатационных документов на автоматизированную систему
Ход работы

Разработка эксплуатационной документации для конструкторских, программных изделий и автоматизированных систем. Рассмотрим основные виды ЭД, их коды и обозначения. Также указаны ссылки на стандарты в соответствии с которыми разрабатывается эксплуатационная документация.

1. ЕСКД

В соответствии с ГОСТ 2.102-2003 (Единая система конструкторской документации (ЕСКД). Виды и комплектность конструкторских документов), эксплуатационная документация - это документы, предназначенные для использования при эксплуатации, обслуживании и ремонте изделия в процессе эксплуатации. Разрабатываются такие документы на этапе рабочего проектирования. Номенклатуру и обязательность разработки определяет ГОСТ 2.601-2013 (ЕСКД. Эксплуатационные документы). Правила выполнения определенных ЭД приведены в ГОСТ 2.610-2006 (ЕСКД. Правила выполнения эксплуатационных документов). Общие требования к оформлению документации - по ГОСТ 2.105-95 (ЕСКД. Общие требования к текстовым документам).

В ГОСТ 2.601 приведено определение эксплуатационного документа:

Эксплуатационный документ – конструкторский документ, который в отдельности или в совокупности с другими документами определяет правила эксплуатации (например, руководство по эксплуатации) изделия и/или отражает сведения, удостоверяющие гарантированные изготовителем значения основных параметров и характеристик (свойств) изделия, гарантии и сведения по его эксплуатации в течение установленного срока службы (например, формуляр).

Где эксплуатация изделия – это стадия жизненного цикла изделия с момента принятия его потребителем от предприятия-изготовителя или ремонтного предприятия до отправки в ремонт или списания.

Сведения об изделии, помещаемые в ЭД, должны быть достаточными для обеспечения правильной и безопасной эксплуатации изделий в течение установленного срока службы. При необходимости, в ЭД приводят указания о требуемом уровне подготовке обслуживающего персонала.

Виды, комплектность и выполнение (электронное или бумажное) ЭД устанавливает разработчик, опираясь на требования ТЗ и ЕСКД.

Ниже представлена таблица, где определены виды и номенклатура эксплуатационных документов в соответствии с ЕСКД.

Вид документа	Код вида докумен-та	Определение	Степень обязатель-ности разработки документа	Дополнительное указание
Руководство по эксплуатации	РЭ	Документ, содержащий сведения о конструкции, принципе действия, характеристиках (свойствах) изделия, его составных частях и указания, необходимые для	о	–

		правильной и безопасной эксплуатации изделия (использования по назначению, технического обслуживания, текущего ремонта, хранения и транспортирования) и оценок его технического состояния при определении необходимости отправки его в ремонт, а также сведения по утилизации изделия и его составных частей		
Инструкция по монтажу, пуску, регулированию и обкатке изделия	ИМ	Документ, содержащий сведения, необходимые для монтажа, наладки, пуска, регулирования, обкатки и сдачи изделия и его составных частей в эксплуатацию на месте его применения	о	ИМ составляют на монтаж, пуск, регулирование и обкатку изделия на месте его применения и в случае, если эти требования нецелесообразно или невозможно изложить в РЭ
Формуляр	ФО	Документ, содержащий сведения, удостоверяющие гарантии изготовителя, значения основных параметров и характеристик (свойств) изделия, сведения, отражающие техническое состояние данного изделия, сведения о сертификации и утилизации изделия, а также сведения, которые вносят в период его эксплуатации (длительность и условия работы, техническое обслуживание, ремонт и другие данные)	+	Документ составляют на изделия, в период эксплуатации которых необходимо вносить сведения о значениях основных параметров и характеристиках (свойствах) изделия, отражающих техническое состояние данного изделия и/или данные о процессе эксплуатации (длительности и условиях работы, данные о проведении технического обслуживания, ремонта и другие данные)
Паспорт	ПС	Документ, содержащий сведения, удостоверяющие гарантии изготовителя, значения основных параметров и характеристик (свойств) изделия, а также сведения о сертификации и утилизации изделия	+	ПС составляют на изделия, для которых объем необходимых для эксплуатации данных и основных показателей незначителен и в период эксплуатации которого нет необходимости вносить сведения о значениях и/или

				подтверждении этих показателей
Этикетка	ЭТ	Документ, содержащий гарантии изготовителя, значения основных параметров и характеристик (свойств) изделия, сведения о сертификации изделия	+	ЭТ составляют на изделия, для которых данные, необходимые для эксплуатации, не превышают пяти-шести основных показателей, когда для подтверждения этих показателей нет необходимости составлять ФО (ПС) и технически их невозможно и/или нецелесообразно маркировать на изделии
Каталог изделий	КИ	Документ, содержащий перечень деталей, сборочных единиц и комплексов изделия с иллюстрациями и сведения об их количестве, расположении в изделии, взаимозаменяемости, конструктивных особенностях, материалах и др.	о	КИ составляют на изделия, для которых в течение времени эксплуатации предусмотрены неоднократный ремонт и замены составных частей
Нормы расхода запасных частей	НЗЧ	Документ, содержащий номенклатуру запасных частей изделия и их количество, расходуемое на нормируемое количество изделий за период их эксплуатации	о	Под НЗЧ на период эксплуатации одного изделия понимают среднее ожидаемое за этот период количество замен составных частей из-за отказов и выработки ресурсов
Нормы расхода материалов	НМ	Документ, содержащий номенклатуру материалов и их количество, расходуемое на нормированное количество изделий за период их эксплуатации	о	Под НМ на период эксплуатации понимают среднее ожидаемое за этот период количество расходуемых материалов
Ведомость комплекта запасных частей, инструмента и принадлежностей	ЗИ	Документ, содержащий номенклатуру, назначение, количество и места укладки запасных частей, инструментов, принадлежностей и материалов, расходуемых за срок службы изделия	о	ЗИ поставляют на изделия, с которыми совместно поставляют прилагаемые к ним комплекты ЗИП, а также наборы ЗИП, поставляемые отдельно от изделия, для эксплуатации которых предназначается ЗИП. Если количество наименований изделий и

				материалов незначительно, то ЗИ допускается не разрабатывать, а их номенклатуру перечислять в ФО или ПС
Учебно-технические плакаты	УП	Документы, содержащие сведения о конструкции изделия, принципах действия, приемах использования, техническом обслуживании, областях технических знаний с необходимыми иллюстрациями	о	УП выпускают по ГОСТ 2.605 (ЕСКД. Плакаты учебно-технические. Общие технические требования)
Инструкции эксплуатационные специальные	ИС	Документы, содержащие специальные требования, относящиеся к использованию по назначению, техническому обслуживанию, текущему ремонту, хранению, транспортированию и утилизации, оформленные в виде самостоятельных частей ЭД или в виде приложений к ним	о	Документы составляют на изделия, для которых в течение времени эксплуатации следует выполнять специальные требования, относящиеся к использованию по назначению, техническому обслуживанию, текущему ремонту, хранению, транспортированию и утилизации
Ведомость эксплуатационных документов	ВЭ	Документ, устанавливающий комплект эксплуатационных документов и места укладки документов, поставляемых с изделием и	+	ВЭ составляют на изделия, в комплект эксплуатационных документов которых входят два и более самостоятельных эксплуатационных документа
Условные обозначения: + – документ обязательный; о – необходимость разработки документа устанавливает разработчик (по согласованию с заказчиком). Примечание – В зависимости от назначения изделия, условий эксплуатации и объёма помещаемых сведений в обязательном порядке разрабатывают либо ФО, либо ПС, либо ЭТ, либо включают один из этих документов в объединённый ЭД.				

В зависимости от особенностей изделия и объёма сведений о нём, допускается разделять документ на части или разрабатывать объединённый ЭД.

2. Автоматизированные системы

При разработке решений в области информационных технологий стандарты ЕСКД применяются к документации на технические средства. Документация на автоматизированные системы разрабатывается по Комплексу стандартов на автоматизированные системы (КСАС, ГОСТ 34.*).

В соответствии с определением по ГОСТ 34.003-90 (Информационная технология. Комплекс стандартов на автоматизированные системы (КСАС). Автоматизированные системы. Термины и определения) эксплуатационная документация на автоматизированную систему (АС) – это часть рабочей документации на АС, предназначенная для использования при эксплуатации системы, определяющая правила действия персонала и пользователей системы при ее функционировании, проверке и обеспечении ее работоспособности. Перечень наименований разрабатываемых документов и их комплектность на систему и ее части должен быть определен в техническом задании на создание автоматизированной системы (подсистемы). Ниже приведена таблица, в которой приведены виды и номенклатура эксплуатационных документов в соответствии с КСАС.

Вид документа	Код вида документа	Часть проекта	Дополнительные указания
Чертеж формы документа (видеокадра)	С9	ИО	В документе должно быть приведено изображение формы документа или видеокадра в соответствии с требованиями государственных стандартов унифицированной системы документации, Р 50-77 и необходимые пояснения. На стадии ТП допускается включать в документы Описание постановки задач (комплекса задач) Описание информационного обеспечения системы
Ведомость эксплуатационных документов	ЭД	ОР	Документ содержит перечень эксплуатационных документов согласно ГОСТ 34.201. Ведомость заполняют по разделам - частям проекта АС
Ведомость машинных носителей информации	ВМ	ИО	Ведомость машинных носителей информации содержит обозначения, наименования документов, выполненных на машинных носителях. Запись документов осуществляется в порядке возрастания присвоенных обозначений
Массив входных данных	В6	ИО	Документ содержит перечень входных данных с указанием их наименований, кодовых обозначений и значности реквизитов, а также наименований и кодовых обозначений документов или сообщений, содержащих эти данные
Каталог базы данных	В7	ИО	Каталог базы данных содержит перечень объектов предметной области АС, информация о которых включена в базу данных
Состав выходных данных (сообщений)	В8	ИО	Документ содержит перечень выходных данных с указанием их наименований, кодовых обозначений и значности реквизитов, а также наименований и кодовых обозначений документов или сообщений, содержащих эти данные
Методика (технология)	И1	ОО	Документ описывает выбранные

автоматизированного проектирования			математические методы, используемые при проектировании, указывают состав и назначение проектных процедур, порядок взаимодействия проектных процедур в процессе выполнения
Технологическая инструкция	И2	ОО	Документ "Технологическая инструкция" разрабатывают на операцию или комплекс операций технологического процесса обработки данных. В документе указывают наименование технологической операции (операций), на которую разработан документ, и приводят сведения о порядке и правилах выполнения операций (операции) технологического процесса обработки данных. В инструкции приводят перечень должностей персонала, на которые распространяется данная инструкция. Номенклатуру технологических инструкций определяют, исходя из принятого процесса обработки данных. Структуру документа устанавливает разработчик в зависимости от содержания
Руководство пользователя	И3	ОО	Документ содержит полное описание системы, указания пользователю по подготовке к работе, освоению, эксплуатации системы, действиях при возникновении проблем в работе системы.
Инструкция по формированию и ведению базы данных (набора данных)	И4	ИО	Документ описывает правила подготовки данных, порядок и средства заполнения, процедуры изменения, порядок и средства восстановления базы данных
Инструкция по эксплуатации КТС	ИЭ	ТО	Документ содержит указания о порядок работы, проверке правильности функционирования, меры безопасности, действиях в разных режимах при работе с комплексом технических средств системы
Описание технологического процесса обработки данных (включая телеобработку)	ПГ	ОО	Документ описывает технологический процесс сбора и обработки данных на периферийных устройствах при децентрализованной обработки данных и технологический процесс обработки данных на вычислительном центре
Общее описание системы	ПД	ОР	Документ содержит сведения о системе, ее архитектуре, принципах функционирования и необходимых ресурсах
Формуляр	ФО	ОР	Определения – по ГОСТ 2.601
Паспорт	ПС	ОР	

Требования к содержанию документов приведены в РД 50-34.698-90 (Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы требования к содержанию документов).

Содержание документов является общим для всех видов АС и, при необходимости, может дополняться разработчиком документов в зависимости от особенностей создаваемой

АС. Допускается включать в документы дополнительные разделы и сведения, объединять и исключать разделы.

Общие требования к изложению текста документов – по ГОСТ 2.105-95 ЕСКД. Общие требования к текстовым документам.

3. ЕСПД

Сведения для обеспечения функционирования и эксплуатации программ (компонентов, комплексов) приводятся в эксплуатационной программной документации. Комплектность эксплуатационной документации на программные средства определяется по ГОСТ 19.101-77 (Единая система программной документации (ЕСПД). Виды программ и программных документов). Состав комплекта ЭД на программу зависит от её архитектуры, назначения и особенностей целевой аудитории. Необходимость составления того или иного документа определяется на этапе разработки и утверждения технического задания на программу. Ниже приведена таблица, в которой приведён перечень ЭД на программы.

Вид эксплуатационного документа	Код вида документа	Дополнительные указания
Ведомость эксплуатационных документов	20	В документе приводят перечень эксплуатационных документов на программу. Выполняется в соответствии с требованиями ГОСТ 19.507-79
Формуляр	30	В документе указывают основные характеристики программы, комплектность и общие сведения об эксплуатации программы. Выполняется в соответствии с требованиями ГОСТ 19.501-78
Описание применения	31	В документе приводят сведения о назначении программы, области применения, применяемых методах, классе решаемых задач, ограничениях для применения, минимальной конфигурации технических средств, входных и выходных данных. Выполняется в соответствии с требованиями ГОСТ 19.502-78
Руководство системного программиста	32	В документе приводят сведения для установки, проверки, обеспечения функционирования, интеграции в систему и настройки программы в определённых условиях применения ее, устранения аварийных ситуаций. Требования к содержанию и оформлению – по ГОСТ 19.503-79
Руководство программиста	33	В документе приводят сведения по эксплуатации (сопровождению) программы. Выполняется по ГОСТ 19.504-79
Руководство оператора	34	Документ содержит сведения о порядке действий оператора при использовании программы. Требования к содержанию и оформлению – по ГОСТ 19.505-79
Описание языка	35	Документ содержит описание синтаксиса и семантики языка, элементов и конструкций, встроенных функций. Выполняется по ГОСТ 19.506-79
Руководство по техническому обслуживанию	46	В документе приводят сведения для применения тестовых и диагностических программ при обслуживании технических средств.

Правила оформления программных документов для печатного способа выполнения установлены ГОСТ 19.106-78 (ЕСПД. Требования к программным документам, выполненным печатным способом).

В стандартах ЕСПД отсутствуют методические указания о том, как разработать документацию, они дают только перечень типов документов со списком разделов первого уровня для каждого и указания о том, какие сведения должны быть в нем изложены. Среди стандартов ИСО/МЭК есть ряд документов, касающихся процессов документирования при

разработках в сфере информационных технологий. В отличие от ЕСПД, они содержат минимум требований к составу и структуре документов, при этом в них дано множество указаний, направленных на получение документов высокого качества. Возможно, комплексное применение указанных нормативных документов при разработке эксплуатационной документации на программы позволит повысить качество, информативность и полезность таких документов.

Ниже приведена таблица, в которую включены стандарты ИСО/МЭК, касающиеся процессов разработки программной и системной документации.

Обозначение	Наименование
ГОСТ Р ИСО/МЭК 12207-99	Информационная технология. Процессы жизненного цикла программных средств
ГОСТ Р ИСО/МЭК ТО 15271-2002	Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 Процессы жизненного цикла программных средств
ГОСТ Р ИСО/МЭК 9126-93	Информационная технология. Оценка программной продукции. Характеристики качества и руководство по их применению
ГОСТ Р ИСО/МЭК 15910-2002	Информационная технология. Процесс создания документации пользователя программного средства
ГОСТ Р ИСО/МЭК ТО 9294-93	Информационная технология. Руководство по управлению документированием программного обеспечения
ГОСТ Р ИСО/МЭК 15288-2005	Информационная технология. Системная инженерия. Процессы жизненного цикла систем
ISO/IEC 15289	Системная и программная инженерия. Содержание информационных продуктов (документации) процессов жизненного цикла систем и программных средств
ISO/IEC 26514	Системная и программная инженерия. Требования для проектировщиков и разработчиков документации пользователя
ISO/IEC 26513	Системная и программная инженерия. Требования по экспертизе и тестированию документации пользователя
ГОСТ Р 51904-2002	Программное обеспечение встроенных систем. Общие требования к разработке и документированию
ISO/IEC 18019:2004	Программная инженерия. Руководство по разработке и подготовке пользовательской документации на прикладные программные средства
ISO 6592:2000	Обработка информации. Руководство по документации для вычислительных систем
ГОСТ Р ИСО 9127-94	Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов.

Критерии оценки

Процент результативности (правильных ответов)	**Качественная оценка индивидуальных образовательных достижений**	
	балл (отметка)	**вербальный аналог**
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	не удовлетворительно

Составитель: А.В. Винник
«31» августа 2022 г.