

УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра вычислительной техники и защиты информации

Выпускная квалификационная работа на тему:

«Система защиты персональных данных»

Выполнил: Мальцева М.А.
ст.гр.Зи-537

Консультант: Кудрявцева Р.Т.
доцент, к.т.н.

Уфа 2014

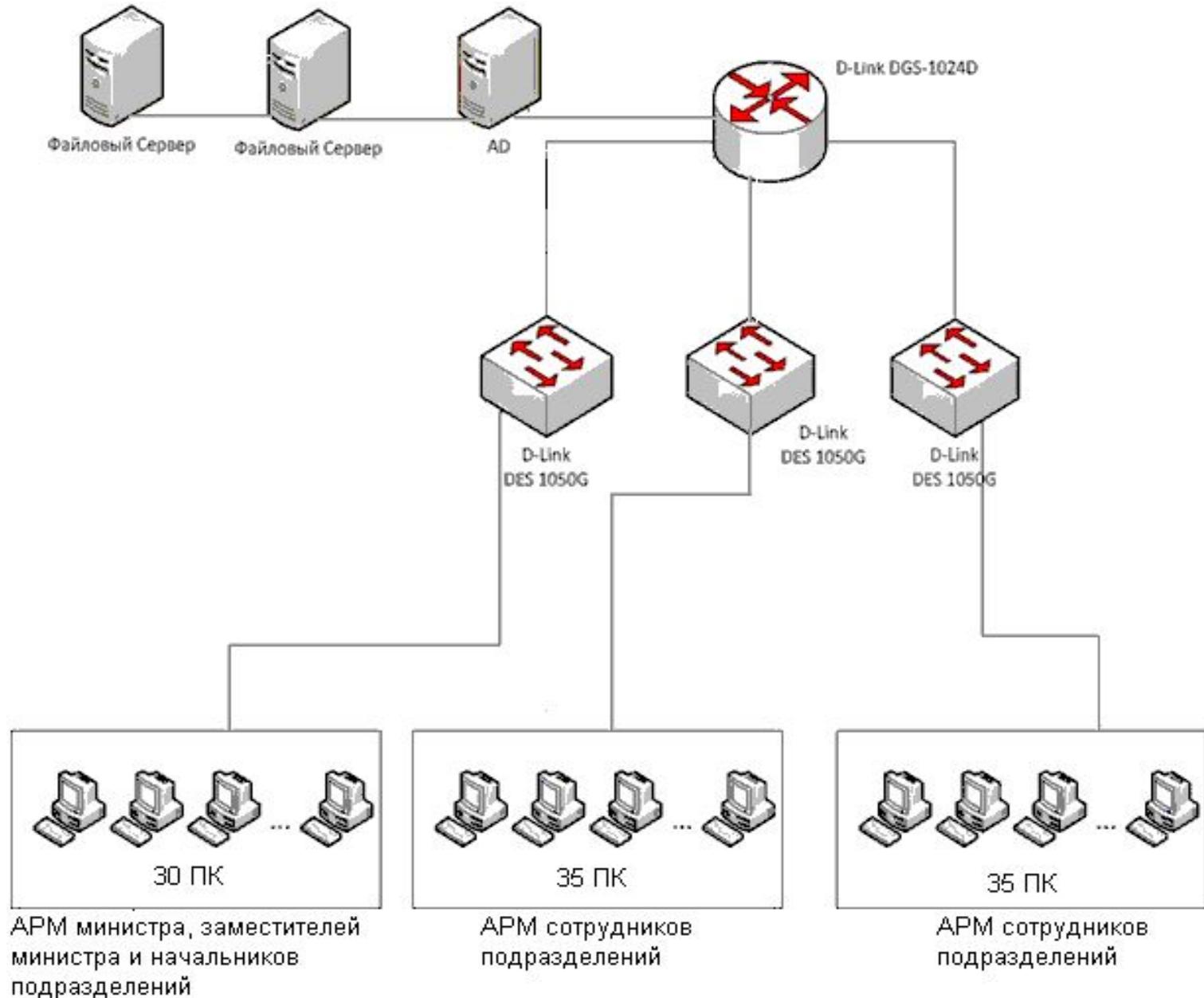
Цель дипломной работы

Разработка и приведение в соответствие с требованиями нормативной документации системы защиты, обеспечивающей информационную безопасность персональных данных в ИСПДн МВД по РБ.

Задачи дипломного проектирования

- Анализ существующих нормативных документов в области защиты персональных данных;
- Проведение обследования объекта защиты и формирование требований к проектируемой СЗПДн;
- Определение класса ИСПДн, построение модели актуальных угроз, разработка структуры СЗПДн, выбор необходимых подсистем,;
- Формирование критериев, выбор средств защиты для ИСПДн, описание настройки средств ЗИ от НСД;
- Расчет риска нарушения информационной безопасности;
- Расчет затрат на создание проекта СЗПДн.

Топология ИСПДн «Сотрудники МВД по РБ»



Исходные параметры ИСПДн «Сотрудники МВД по РБ»

Заданные характеристики безопасности персональных данных	специальная информационная система
Структура информационной системы	локальная информационная система
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	не имеется
Режим обработки персональных данных	многопользовательская система
Режим разграничения прав доступа пользователей	система с разграничением прав доступа
Местонахождение технических средств информационной системы	все технические средства находятся в пределах Российской Федерации

Актуальные угрозы ИСПДн

Наименование угрозы	Средство защиты
Угрозы, реализуемые после загрузки ОС	система защиты информации от НСД; средство криптографической ЗИ на ПК; система охранной сигнализации (в нерабочие часы); видеонаблюдение
Внедрение вредоносных программ	антивирусное ПО
Угрозы утраты ключей и атрибутов доступа	инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа
Установка ПО не связанного с исполнением служебных обязанностей	система защиты информации от НСД (обеспечивающая в т.ч. шифрование данных на съемных носителях), резервное копирование данных; наблюдение за действиями посетителей
Кража носителей информации	система защиты информации от НСД (обеспечивающая в т.ч. шифрование данных на съемных носителях), резервное копирование данных; наблюдение за действиями посетителей
НСД к информации при техническом обслуживании узлов ПЭВМ	система защиты информации от НСД, средство криптографической ЗИ на ПК, резервное копирование данных

Альтернативы подсистем СЗПДн

Анализ защищенности

- MaxPatrol
- Xspider 7.8

Обнаружение вирусов

- Kaspersky Endpoint Security 10 для Windows
- Dr.Web Enterprise Suite 6.0
- ESET NOD32 Platinum Pack 4.0
- Kaspersky 6.0 для Windows

Шифрование данных

- ViPNet SafeDisk 4.1

Разграничение доступа

- Аккорд NT/2000
- Аура 1.2.4
- Secret Net 6
- Соболь 3.0
- Страж NT 3.0

Резервирование

- Acronis Backup&Recovery 11 Advanced Server
- Acronis Backup & Recovery 11 Advanced Workstation

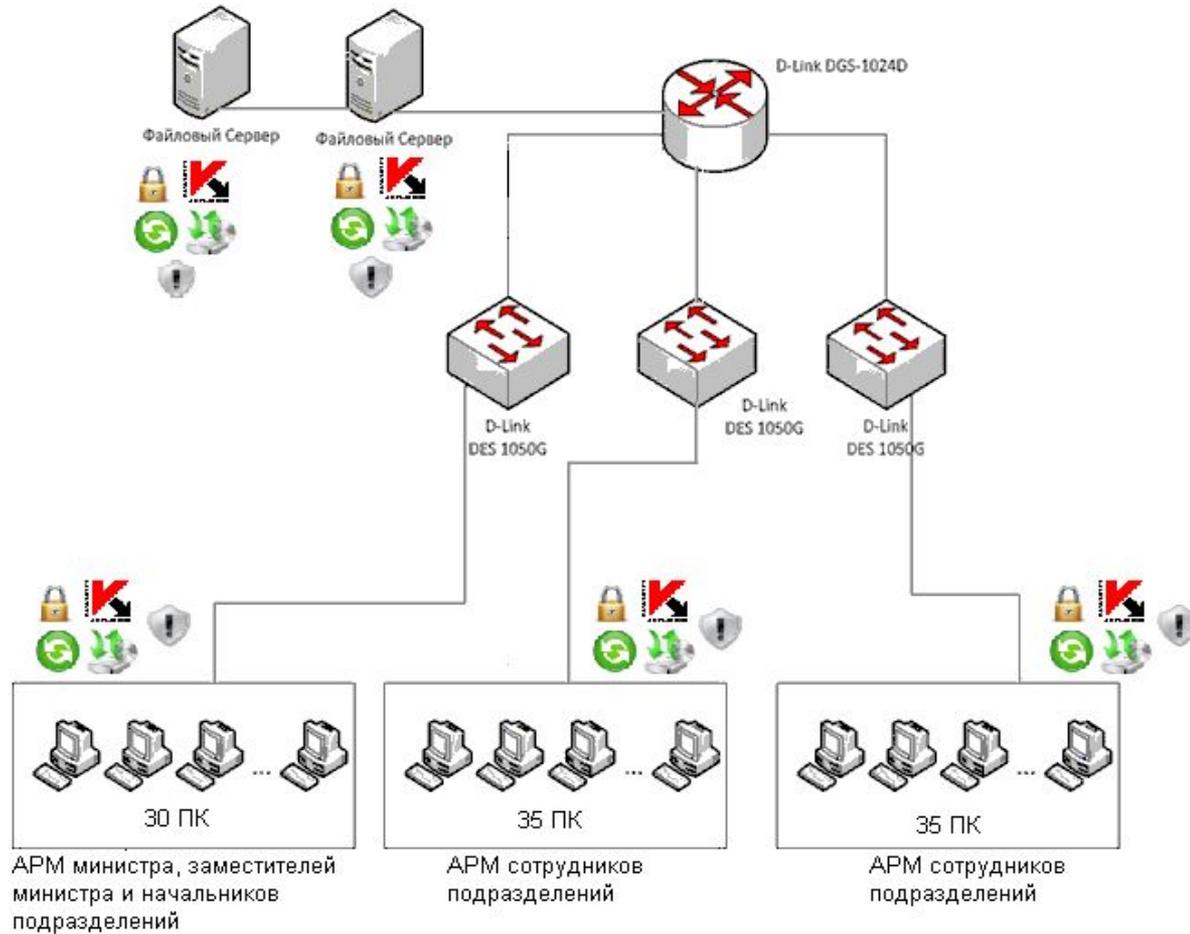
Выбор средств защиты информации от НСД методом линейной свертки

Альтернатива		Критерий					
		стоимость (C_1), руб.	наличие доверенной загрузки ОС (C_2)	возможность создания замкнутой программной среды (C_3)	гарантированное удаление данных (C_4)	механизмы разграничения доступа (C_5)	идентификация / аутентификация пользователей до загрузки ОС (C_6)
A_1	Secret Net 6	6650	да	да	да	Д, М (2)	нет
A_2	«Аккорд-N Т/2000» v.3.0	12889	да	да	нет	Д, М (2)	да
A_3	Страж NT v.3.0	7500	да	да	да	Д, М (2)	да
A_4	Аура 1.2.4	3000	нет	нет	да	Д (1)	нет
A_5	«Соболь» 3.0	4651	нет	да	да	Д, М (2)	нет

Результат выбора средств защиты ПДн

Подсистема СЗПДн	Выбранное средство защиты
контроля целостности, управления доступом, регистрации и учета (подсистема ЗИ от НСД)	Страж NT v.3.0
антивирусной защиты	Антивирус Касперского 6.0 для Windows Servers
	Антивирус Касперского 6.0 для Windows Workstations
анализа защищённости	XSpider 7.8
резервного копирования данных	Acronis Backup & Recovery 11 Advanced Server & Workstation
криптографической защиты информации	ViPNet SafeDisk 4.1

Топология ИСПДн после внедрения средств



 - система защиты от НСД

 - система антивирусной защиты

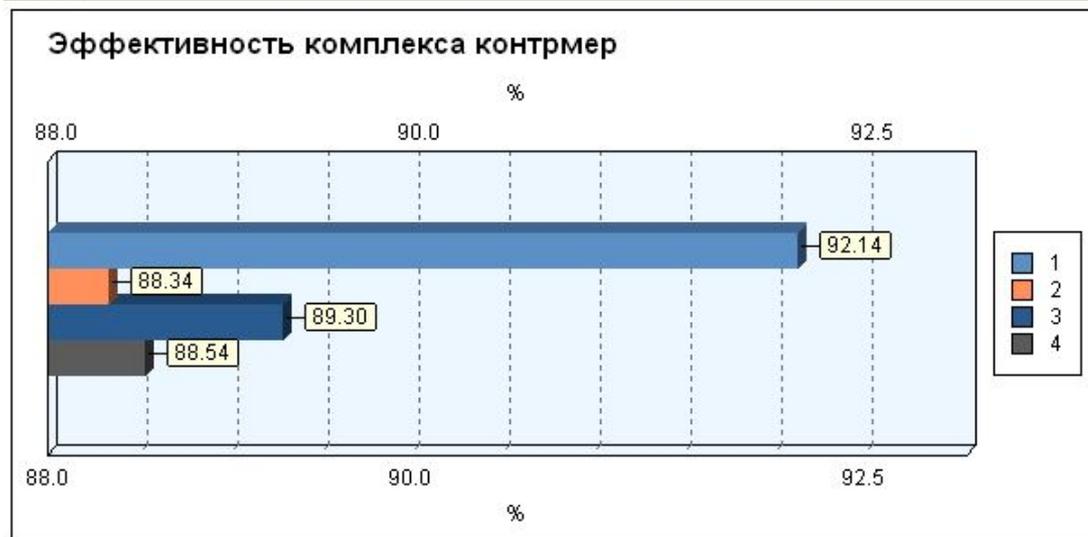
 - система анализа защищённости

 - система резервного копирования данных

 - система криптографическойЗИ

Расчет рисков ИБ с помощью «Гриф 2006»

Отчет 1



№	Ресурс	Значение риска до всех контрмер, %	Значение риска после всех контрмер, %	Эффективность комплекса контрмер, %
1	Сервер №1	2.11	0.17	92.14
2	Сервер №2	7.00	0.82	88.34
3	АРМ МВД	29.60	3.17	89.30
4	ИСПДн	35.91	4.11	88.54

Риск нарушения защищенности информационной системы до модернизации составляет 35,91 %, а после модернизации сокращается в 8,74 раз и составляет 4,11 %.

Расчет затрат на создание проекта СЗПДн

Средство защиты	URL на указание цены средства защиты	Дата обращения к URL	Цена за 1 лицензию, руб.	Кол-во необходимых лицензий	Итоговая стоимость продукта, руб.
Страж NT v.3.0	http://www.cbi-info.ru/groups/page-1090.htm	2.05.2014	7500	102	765000
Kaspersky 6.0 для Windows.	http://www.pointlane.ru/solutions/Kaspersky-vpn/price/		2800	102	285600
XSpider 7.8	http://www.ptsecurity.ru/xs7/rates/	2.05.2014	15040	1	15040
Acronis Backup & Recovery 11 Advanced Server & Workstation	http://www.acronis.ru/backup-recovery/advanced-workstation/		3465	102	353430
VipNet Safe Disk	http://www.dials.ru/product_manager/-/?ac=product&id=18		1357	102	138414
Итого:					1557484

Общие затраты на внедрение системы защиты ПДн составляют:

$C_{\text{ОБЩ}} = 1822929$ руб.

Выводы по проделанной работе

- Проанализированы существующие нормативные документы в области защиты персональных данных;
- Произведено обследование объекта защиты и сформированы требования к проектируемой СЗПДн;
- Разработана структура СЗПДн, выбраны необходимые подсистемы, построена модель актуальных угроз;
- Сформированы критерии, выбраны оптимальные средства защиты для ИСПДн, описаны настройки средств ЗИ от НСД;
- Рассчитаны риски нарушения информационной безопасности;

Спасибо за внимание.