МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Филиал в г. Славянске-на-Кубани

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(ДИПЛОМНАЯ РАБОТА)

Разработка организационно-технических решений по обеспечению защиты информации в компьютерной сети организации

Работу выполнил студент группы ДС-19-КС А.А.Галоян
Руководитель М.С.Бушуев

Защита информации в локальных вычислительных систем ООО «ВАРЯГ»

1) При проведении анализа защищенности информации на предприятии «ВАРЯГ», было установлено, что существует вероятность реализации следующих угроз несанкционированного доступа:

2) – осуществление несанкционированного доступа к защищаемым активам, используя штатные средства инфраструктуры ООО «ВАРЯГ»,

3) – использование бесконтрольно оставленных штатных средств инфраструктуры ООО «ВАРЯГ» или хищение нарушителями и утрата элементов инфраструктуры (в том числе распечаток, носителей информации)

Защита информации в локальных вычислительных систем ООО «ВАРЯГ»

–действия по анализу сетевого трафика, сканированию вычислительной сети, атаки, направленные на отказ в обслуживании, выявление парольной информации, подмена доверенного объекта сети, навязывание ложного маршрута сети с использованием нештатных технических и программных средств, доступных нарушителю,

–маскировка под администраторов инфраструктуры ООО «ВАРЯГ»,

–компрометация (просмотр, подбор и т.п.) парольной информации на доступ к информационным ресурсам ООО «ВАРЯГ»,

–осуществление перехвата управления загрузкой ОС.

№	Угроза безопасности ПДн	Степень актуальности	Меры по противодействию угрозе	
			Технические	Организационные
1	Кража носителей информации	актуальная		Инструкция для персонала
2	Кража паролей	актуальная		Инструкция пользователя, учет паролей
3	Кражи, модификации, уничтожения информации.	актуальная	Настройка средств защиты,политика безопасности	Резервное копирование и инструкция пользователя
4	Несанкционированное отключение средств защиты	актуальная	Настройка средств защиты	Инструкция администратора безопасности
5	Действия вредоносных программ (вирусов)	актуальная	Антивирусное ПО	Инструкция по антивирусной защите

6	Недекларированные возможности ПО	актуальная	Настройка средств защиты	Сертификация
7	Установка ПО не связанного с исполнением обязанностей	актуальная	Настройка средств защиты, политика безопасности	Инструкция пользователя, инструкция администратора безопасности
8	Непреднамеренная модификация (уничтожение) информации сотрудниками	актуальная	Настройка средств защиты, политика безопасности	Инструкция пользователя
9	Выход из строя аппаратно-программных средств	актуальная	Резервное копирование	Охрана, Инструкция для персонала
10	Сбой системы электроснабжения	актуальная	Использование ИБП, резервное копирование	Охрана
11	Разглашение информации, модификация, уничтожение сотрудниками	актуальная	Настройка средств защиты, политика безопасности	Инструкция для персонала, подписка о не разглашении

12	Перехват в пределах контролируемой зоны	актуальная	Средства криптографической защиты, физическая зашита канала	Охрана
13	Угрозы удаленного запуска приложений.	актуальная	Межсетевой экран, Антивирусное ПО	
14	Угрозы внедрения по сети вредоносного ПО	актуальная	Межсетевой экран, Антивирусное ПО	
15	Угрозы утечки видовой информации	актуальная		Инструкция пользователя
16	Кража ПЭВМ	неактуальная		Пропускной режим,охрана,видеонаблюдение
17	Вывод из строя узлов ПЭВМ, каналов связи	неактуальная		Пропускной режим, охрана, видеонаблюдение

Следовательно, по отношению к инфраструктуре ООО «ВАРЯГ» можно сделать следующие выводы:

–неактуальность кражи ПЭВМ. В здании введен круглосуточный контроль доступа в контролируемую зону, который осуществляется охраной, двери, закрываются на замок, вынос компьютерный техники за пределы здания возможен только по специальным пропускам,

–неактуальность вывода из строя узлов ПЭВМ, каналов связи. В здании введен контроль доступа в контролируемую зону, двери закрываются на замок,

–неактуальность действий, направленных на перехват ПЭМИН и акустической информации. Основной объем ПДн консолидировано хранится на сервере БД, сервер БД размещен в отдельном помещении внутри контролируемой зоны.

Ввиду того, что вероятность проникновения внешних нарушителей или физического уничтожения данных минимальна – необходимо дорабатывать программно-аппаратный комплекс средств защиты компьютерной информации по направлениям:

-обеспечить защиту сетевого периметра и выбрать межсетевой экран,

-выбрать криптографические средства защиты от НСД,

-определить средства обнаружения вторжений и антивируса

Одной из первых рекомендаций в ходе анализа защиты данных ООО «ВАРЯГ», является установка межсетевого экрана, которая является внешней защитой от НСД.

Межсетевые экраны предназначены в первую очередь для защиты компьютерных сетей или отдельных узлов от внешних атак Межсетевой экран делает возможной фильтрацию входящего и исходящего трафика, идущего через систему. Для корпоративной сети фирмы был выбран программный межсетевой экран UserGate Proxy & Firewall 5.2 F, который является эффективной альтернативой дорогостоящим программным и аппаратным межсетевым экранам и маршрутизаторам, используемым для защиты конфиденциальной информации и данных в защищенных системах.

СКЗИ «ViPNet CSP» предназначено не только для использования в программном обеспечении ViPNet производства ОАО «ИнфоТеКС», но и для встраивания в прикладное программное обеспечение других производителей и для поставки конечным пользователям и обеспечивает:

- создание ключей электронной подписи по алгоритму ГОСТ Р 34.10- 2001. Проверку электронной подписи по алгоритму ГОСТ Р 34.10-94, вычисление и проверку электронной подписи по алгоритму ГОСТ Р 34.10-2001,

- хэширование данных в соответствии с алгоритмом ГОСТ Р 34.11-94,

- шифрование и имитозащиту данных в соответствии с алгоритмом ГОСТ 28147-89. Генерацию случайных и псевдослучайных чисел, сессионных ключей шифрования,

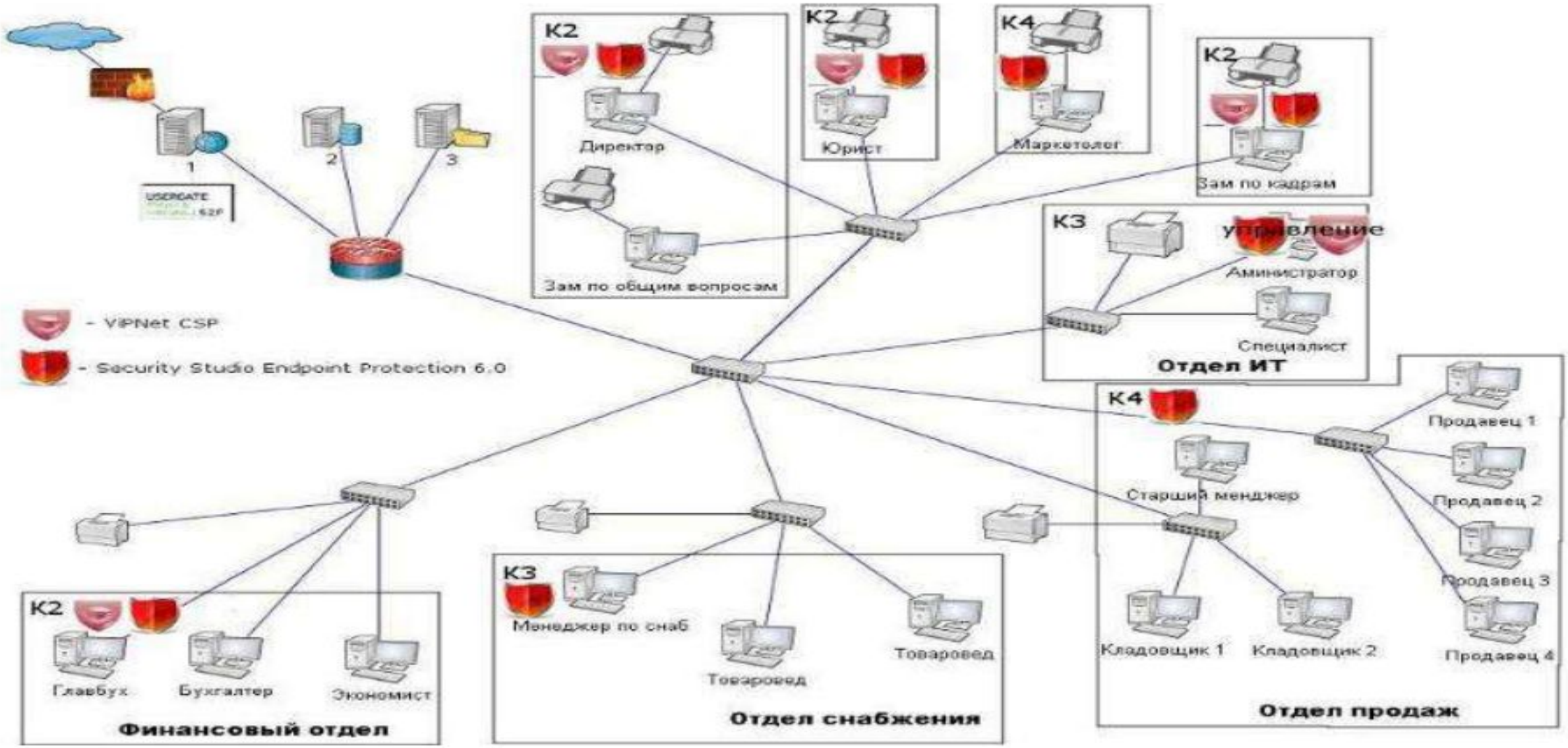
- аутентификацию и выработку сессионного ключа при передаче данных по протоколам SSL/TLS. Хранение сертификатов открытых ключей непосредственно в контейнере ключей,

поддержку различных устройств хранения ключей (eToken, ruToken, Shipka и др.)

Security Studio Endpoint Protection 6.0 обеспечивает защиту компьютера с применением межсетевого экрана, антивируса и средства обнаружения вторжений. Обеспечивает безопасную и комфортную работу с сетью Интернет, предотвращая любые попытки проникновения на компьютер вредоносного программного обеспечения и блокируя нежелательный трафик.

- безопасный доступ в сеть,
- защита от известных вирусов и программ-шпионов,
- защита от неизвестных угроз,
- безопасное использование сетевых ресурсов и защита от спама,
- централизованное управление.

Security Studio Endpoint Protection (SSEP) обеспечивает защиту компьютера с применением межсетевого экрана, антивируса и средства обнаружения вторжений. Обеспечивает безопасную и комфортную работу с сетью интернет, предотвращая любые попытки проникновения на компьютер вредоносного программного обеспечения и блокируя нежелательный трафик.


1
2
3
K2
Директор
Зам по общим вопросам
K2
Юрист
K4
Маркетолог
K2
Зам по кадрам
K3
Администратор
Специалист
Отдел ИТ
- ViPNet CSP
- Security Studio Endpoint Protection 6.0
K4
Старший менджер
Продавец 1
Продавец 2
Продавец 3
Продавец 4
Кладовщик 1
Кладовщик 2
Отдел продаж
K3
Менеджер по снаб
Товаровед
Товаровед
Отдел снабжения
K2
Главбух
Бухгалтер
Экономист
Финансовый отдел