Содержание

**Введение**…………………………………………………………………....3

**Глава 1. Общая характеристики и классификации систем HoneyPot**

* 1. Системы HoneyPot……………………………………………..…..5
  2. Классификация HoneyPot-систем…………….………………...…8
  3. Размещение HoneyPot приманок в сети брандмауэров .………..15
  4. Сбор и анализ информации……………………………………….25

**Глава 2. Анализ деятельности Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови»**

2.1 Общая характеристика Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови» ………………..……………………................................32

2.2 Локальная вычислительная сеть Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови» …………………….................44

**Глава 3. Рекомендации по внедрению и эксплуатации HoneyPot**

* 1. Внедрение коммерческого низкоинтерактивного KFSensor Honeypot IDS …………………………………………………………………….55
  2. Проект HoneyNet…………………………………………………...61
  3. Создание отвлекающей сети HoneyPot – ловушек……………..68

**Заключение**……………………………………………………………….70

**Список источников и использованной литературы**……………….72

**Приложения**

**Введение**

Курсовая работа направлена на внедрение технологии HoneyPot в локальную сеть Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови».

Системы HoneyPot на рынке ПО появились сравнительно давно. Но, к сожалению, их не оценивают должным образом и редко внедряют на предприятиях и в коммерческих структурах. Основные разработчики таких систем – энтузиасты. Основные пользователи таких систем – тоже энтузиасты. На рынке коммерческого ПО системы HoneyPot пока не получают должного развития. Возможно, это связано с низкой распространенностью такого рода ПО, и, как следствие, низким спросом. Но к счастью, существуют как минимум два OpenSource – программных продукта, заслуживающих внимания администратора безопасности любой квалификации – это низкоинтерактивный HoneyD и высокоинтерактивный HoneyNet Project. Эти продукты имеют наиболее развитые функциональные возможности и без существенных затрат могут быть развернуты в компьютерных сетях практически любого назначения.

Как и любой программный продукт, предназначенный для обеспечения информационной безопасности, система HoneyPot не может использоваться сама по себе. Внедрение в инфраструктуру сети подразумевает ее совместное использование с прочими средствами защиты: брандмауэрами, антивирусным ПО, системами IDS, системами обновления ПО, и прочими программами, предназначенными для повышения безопасности сетевой инфраструктуры. В дополнении к вышеперечисленным средствам, HoneyPot может оказаться новой по технологии и принципу работы системой, что может означать существенное повышение вероятности обнаружение попытки взлома или успешного проникновения.

Количество достоверной информации о противнике, его тактике, приемах, мотивации, инструментах и способах проникновения на защищенные узлы или в сеть влияет на процесс подготовки ко встрече с ним, к подготовке оборонительных действий, а, возможно, даже и наступательных.

**Актуальность выбранной темы** обусловлена необходимостью защиты существующей локальной сети объекта исследования, для предотвращения потери защищаемой информации.

**Целью работы является повышение уровня защиты локальной сети организации, определение возможных топологий использования HoneyPot.**

**Для достижения поставленной цели необходимо решить следующие задачи:**

* исследовать принципы работы систем HoneyPot;
* рассмотреть технологии внедрения HoneyPot в локальную сеть Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови». локальную сеть Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови»;
* разработать топологии для обеспечения безопасности локальной сети учреждения от внешних вторжений.

**Объект исследования:** Государственное бюджетное учреждение здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови».

**Предмет исследования** – локальная сеть Учреждения и система HoneyPot.

Структура работы определена ее целями и задачами, и включает введение, три главы, заключение, список используемых источников и литературы, а также приложения.

Во введении обоснована актуальность исследования, сформулирована цель работы и перечислены решаемые задачи.

В первой главе основной части рассматривается системы HoneyPot и их классификация.

Во второй главе приводится общая характеристика предприятия, анализируется деятельность и состояние локальной сети.

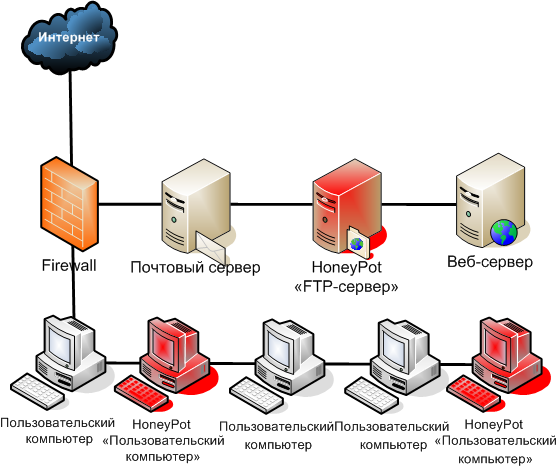
В третьей главе разработан комплекс мероприятий по совершенствованию сети Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови».

В заключение работы сформулированы общие выводы по содержанию каждой главы работы.

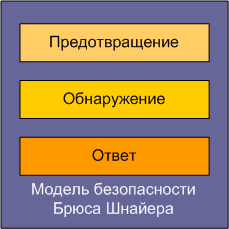
**Глава 1. Общая характеристика и классификация систем HoneyPot**

## 1.1 Системы HoneyPot

HoneyPot – программный комплекс, предназначенный для защиты сети от внешних вторжений и сбора информации о взломщике. Принцип работы заключается в том, что HoneyPot эмулирует на защищаемом компьютере, либо на компьютере(-ах) локальной сети сетевые службы, содержащие известные уязвимости, бэкдоры, трояны и т.д., т.е. все то, что способно позволить атакующему проникнуть на компьютер (рис. 1.1). Но на самом деле HoneyPot лишь эмулирует все те функции, что и та служба, за которую он себя выдает. Как правило, любая атака начинается со сканирования жертвы, поиска открытых портов и наличия уязвимых сервисов, находящихся за открытыми портами. HoneyPot обнаруживает сканирование, но в отличие от иных видов IDS(разновидностью которых он и сам является), он показывает атакующему “доступные” порты или даже целые компьютеры, которые он эмулировал сам. Все атаки будут направляться в HoneyPot, что может с большой степенью достоверности предположить, что происходит именно атака.

Рисунок 1.1 Общая схема расположения HoneyPot

Для описания принципа работы HoneyPot-а нужно воспользоваться моделью безопасности HoneyPot-а, предложенной известным специалистом по компьютерной безопасности Брюсом Шнайером (Bruce Schneier) [38]. Модель включает в себя три парадигмы представленные на рис. 1.2.

 Рисунок 1.2 Модель безопасности

HoneyPot можно задействовать на всех трех уровнях. На уровне предотвращения HoneyPot применяется для замедления или полной остановке автоматических вторжений. На уровне обнаружения HoneyPot применяется для того чтобы выявить неавторизованную активность. По сравнению с классическими IDS у HoneyPot-систем есть одно очень серьезное преимущество – количество информации предлагаемое администратору безопасности для анализа гораздо ниже, а точность и качество – выше. Классические IDS-системы и системы аудита способны генерировать огромный объем журнальных записей, хотя лишь проценты из них могут быть действительными атаками. Кроме того, IDS системы распознают атаки по сигнатурам, а это говорит о том, что они бессильны против неизвестных до настоящего момента атак. Любая активность, обращенная к HoneyPot может свидетельствовать о том, что производится либо сканирование сети, либо производится атака.1.2 Классификация HoneyPot-систем

Существует несколько классификационных признаков HoneyPot систем [35]:

* по степени интерактивности;
* по назначению;
* по размещению.

Основным классификационным признаком HoneyPot систем является степень их интерактивности. Под интерактивностью понимается уровень открытых сетевых сервисов, доступных злоумышленнику. HoneyPot системы бывают низкоинтерактивными и высокоинтерактивными.

Низкоинтерактивный HoneyPot, как правило, включает в себя один или несколько сетевых сервисов, являющихся объектами атаки [35]. Такими сервисами являются POP3, SMTP, IMAP, FTP, HTTP и т.д. Такой HoneyPot устанавливается на компьютер под управлением MS Windows или GNU/Linux как обыкновенный сетевой сервис. Этот сервис сразу закрепляет за собой порты для прослушивания сетевой активности. Число открытых портов определяется количеством эмулируемых сервисов. Если какой-либо сервис уже занял порт, необходимый HoneyPot-у, то прослушивание активности и анализ данных производиться по этому сервису не будет. В большинстве случаев, эмуляция сервисов происходит на поверхностном уровне – программы не реализуют все требования RFC, а лишь имитируют наиболее часто вызываемые команды. С одной стороны, это может показаться достаточным(как правило, так оно и есть), но с другой стороны, это может стать причиной возможного разоблачения HoneyPot-a, так как совершенно ясно, что сервис Microsoft Windows FTP server должен уметь выполнять все специализированные серверные директивы, задекларированные в RFC 959. По принципу работы низкоинтерактивные. HoneyPot и должен был бы называться Системной Обнаружения Вторжений, но исторически такой название закрепилось за системам с другим принципом работы.

Преимущества низкоинтерактивных HoneyPot:

1. Относительная простота реализации.
2. Простота установки и сопровождения.
3. Легкость настройки.
4. Работает поверх штатной операционной системы.
5. Может быть установлен на любой компьютер корпоративной сети.
6. Большое количество приманок, «разбросанных» по сети можно объединить в ферму – административную единицу.

Недостатки низкоинтерактивных HoneyPot:

1. Ограниченное количество эмулируемых сервисов.
2. Низкая скрытность от обнаружения
3. Зачастую выраженность именно в «прикладном уровне» работы
4. Низкая (по сравнению с высокоинтерактивными HoneyPot-ами) эффективность при отслеживании действий злоумышленника.

Высокоинтерактивным HoneyPot-ом называется программный комплекс предназначенный для эмуляции операционной системы целиком [35]. В отличии от низкоинтерактивного, высокоинтерактивный HoneyPot позволяет убедить хакера в том, что тот находится на взломанной машине, пользуется ее командной строкой или графическим интерфейсом, выполняет на ней команды и т.д. Такая система выглядит куда более реалистичной, чем просто эмуляция отдельных сервисов – хакер понимает, что частично достиг своей цели – один из компьютеров сети уже взломан. Если до этого основная информация, собираемая о хакере заключалась в основном в протоколах сеансов сетевой активности, то теперь хакер все свои действия производит на машине-приманке, что позволяет протоколировать его деятельность также на системном уровне либо средствами операционной системы, либо отдельными программами, которые собирают всю информацию об его действиях.

Высокоинтерактивные HoneyPot-ы реализуются различными способами:

1. Специальный дистрибутив ОС с модифицированным ядром.
2. Операционная система, содержащая в себе расширенные средства сбора данных, установленная на отдельном компьютере, либо на виртуальную машину (последний способ является наиболее предпочтительным).

### После развертывания высокоинтерактивные HoneyPot-ы требуют много внимания. На самом деле такие решения могут потребовать целой команды на их обслуживание. Эти люди должны обеспечивать безопасное обслуживание системы и гарантировать, что во время захвата информации, их не используют для атаки настоящих систем. Так как высоко интерактивные решения могут сохранять большое количество данных, администратор может утонуть в количестве информации, предоставляемой при попытке атаки. Если организация намерена производить полный анализ атакованных высокоинтерактивных HoneyPot, то этот анализ будет занимать порядка тридцати часов работы на каждые 30 минут, проведенные атакующим в системе. Можно представить, что будет, если развернуть десятки и сотни таких систем в рамках большой организации. Такой подход хотя и является очень мощным решением по обнаружению и сбору информации, но требует больших материальных и временных затрат.

Как уже было сказано, высокоинтерактивные ловушки представляют для взломщика гораздо более реалистичную и обширную среду, в которую он попадает. Вообще говоря, взламывая низкоинтерактивную приманку взломщик вообще никуда не попадает – сервиса просто нет как такового – есть просто сценарий поведения системы, есть механизм «запрос-ответ», который дает хакеру видимость того, что он взламывает какой-то ресурс, несмотря на то, что его нет на самом деле. В то время как хакер направляет на ловушку запросы и получает ответы, система протоколирует его действия, собирая о нем как можно больше информации. Но низкоинтерактивный HoneyPot – достаточно ограниченное средство. Их функция по большей части схожа с назначением классической IDS – системы, т.е. своевременно известить о проходящей атаке. Количество информации, которой он может собрать, значительно меньше, чем у высокоинтерактивных систем. Основное применение – промышленное использование в дополнении к IDS.

Можно понять, что высокоинтерактивный HoenyPot – гораздо более сложная система, которая представляет значительно больше способов взаимодействия со взломщиков, а, значит, и получить от него куда больше информации о том, как происходит взлом систем, определить его тактики, мотивы и инструменты.

Высокоинтерактивный HoneyPot должен представлять из себя систему, которая осуществляет эмуляцию на всех уровнях операционной системы, всех уровнях стека сетевых протоколов(а не только на верхних, как в случае низкоинтерактивных ловушек) и т.д.

На настоящее время мне известен только один проект, связанный с исследованием в области высокоинтерактивных HoneyPot – систем. Это – The HoneyNet Project, открытый проект, поучаствовать в котором может любой желающий. Над этим проектом работает несколько десятков высококлассных специалистов в области информационной безопасности. Среди них – Лэнс Спицнер, Эрик Коул, Нильс Провос и другие. Про этот проект будет подробнее рассказано далее. Сейчас я вынесу только ключевые моменты.

Разработчики из HoneyNet Project решили не разрабатывать новую среду, представляющую высокий уровень эмуляции, что является очень сложной задачей. Для использования в качестве высокоинтерактивных ловушек они решили взять самые обыкновенные операционные системы, такие как FreeBSD, Linux, Microsoft Windows. От «коробочных» версий их отличает лишь дополнительный драйвер Sebek, работающий как руткит уровня ядра (англ.- kernel level rootkit). Этот драйвер «скрыт» из операционной системы и работает по принципу перехвата всех системных вызовов. Очевидно, что у такого драйвера возможностей для отслеживания информации о происходящем в системе предостаточно. Всю запротоколированную информацию Sebek отправляет по сети, используя TCP/IP, на специальный компьютер – Roo HoneyWall, который журналирует всю пришедшую информацию и, по сути, является удаленным источником хранения информации о взломе.

Важным является умение проводить различие между низкоинтерактивными и высокоинтерактивными HoneyPot системами. Можно сказать, что отличия между ними фундаментальны. Они используют принципиально различный способ работы, хотя и предназначены для решения схожих задач. Поэтому классификация по степени интерактивности представляется мне наиболее важным критерием сравнения различных HoneyPot-систем.

Однако, не все специалисты видят грань различия между этими системами. Порой даже специалисты по ИБ, публикуя свои работы по системам HoneyPot на таких уважаемых порталах, как SecurityLab.ru, не делают различия между этими типами систем, зачастую смешивая эти понятия и путая терминологию.

Преимущества высокоинтерактивного HoneyPot-а:

1. Наибольшее количество информации о взломщике.
2. Трудно отличить высокоинтерактивный HoneyPot от обыкновенного узла.
3. Возможность установки любых программ, содержащих реальные уязвимости.
4. Возможность обнаружить ранее неизвестные уязвимости системы.

Недостатки высокоинтерактивного HoneyPot-а:

1. Трудность установки и сопровождения.
2. Трудность анализа данных после взлома HoneyPot-a.

По назначению HoneyPot системы подразделяются на промышленные и исследовательские.

Исследовательские системы предназначены для изучения действий хакеров, способов взлома компьютерных систем и сетей, инструментов, которые они используют для взлома, тактических приемов и т.д. Наблюдая за происходящем во взломанной системе, можно определить и локализовать проблемы, связанные с безопасностью, определить, как взломщик проник в систему, что в ней происходит после того, как она оказалась взломанной и какие действия выполняет взломщик для того, чтобы со взломанной системы атаковать другие системы. HoneyPot – единственное средство, которое позволяет с высокой степенью достоверности изучить все приемы хакеров. Так, разработчики HoneyNet Project позиционируют свой продукт именно как инструмент для исследования действий и мотивов хакеров.

Промышленные HoneyPot предназначены для защиты корпоративных сетей от атак хакеров и сетевых червей. Защита производится по трем направлениям:

1. Предотвращение атаки.
2. Обнаружение атаки.
3. Организация ответных действий.

Основная цель такого HoneyPot-a – ввести хакера в заблуждение, отнять его время, изучить мотивы и инструменты, отвести его внимание от реальных серверов, информировать администратора безопасности об угрозе, собрать информацию о хакере для того чтобы приготовиться к нападению. Использование таких HoneyPot-ов в комплексе с другими системами обеспечения безопасности, такими как IDS/IPS систем, брандмауэрами, комплексами антивирусной защиты, позволяет серьезно увеличить уровень безопасности сети по сравнению с комплексами безопасности, которые не включают в себя HoneyPot.

Промышленные HoneyPot позволяют:

1. Отслеживать компьютеры, с которых происходит сканирование узлов сети.
2. Отслеживать компьютеры, с которых производится доступ к несуществующим узлам сети, что говорит о разведывании доступных ресурсов.
3. Отслеживать компьютеры, с которых осуществляется DoS или DDoS атаки на внутренние или внешние узлы сети.
4. Отслеживать компьютеры, с которых производится несанкционированная отправка почты (SMTP Relays).

## По размещению и в зависимости от назначения HoneyPot системы могут находиться:

1. На серверах в Интернете (НИ\*, ВИ\*).
2. На внешних брандмауэрах (НИ).
3. В сети внешних брандмауэров (ВИ.)
4. В демилитаризованной зоне (ВИ).
5. На серверах, расположенных в демилитаризованной зоне (НИ).
6. В сети внутрикорпоративных серверов (ВИ).
7. На внутрикорпоративных серверах (НИ).
8. В пользовательском сегменте сети (ВИ).
9. На пользовательских компьютерах (НИ).
10. Комбинирование различных схем размещения.

Так как приманки могут отличаться по интерактивности, то располагаться они могут как в составе программного обеспечения штатных серверов, так и на специально предназначенных выделенных серверах [35].

Низкоинтерактивные приманки, как правило, не требовательны к вычислительным ресурсам компьютера, и поэтому могут располагаться как на компьютерах обыкновенных пользователей, так и на серверах сети, выполняющих собственные функции. Такие приманки запускаются как отдельные программы, не влияющие на работу других программ, и поэтому могут вполне с ними сосуществовать.

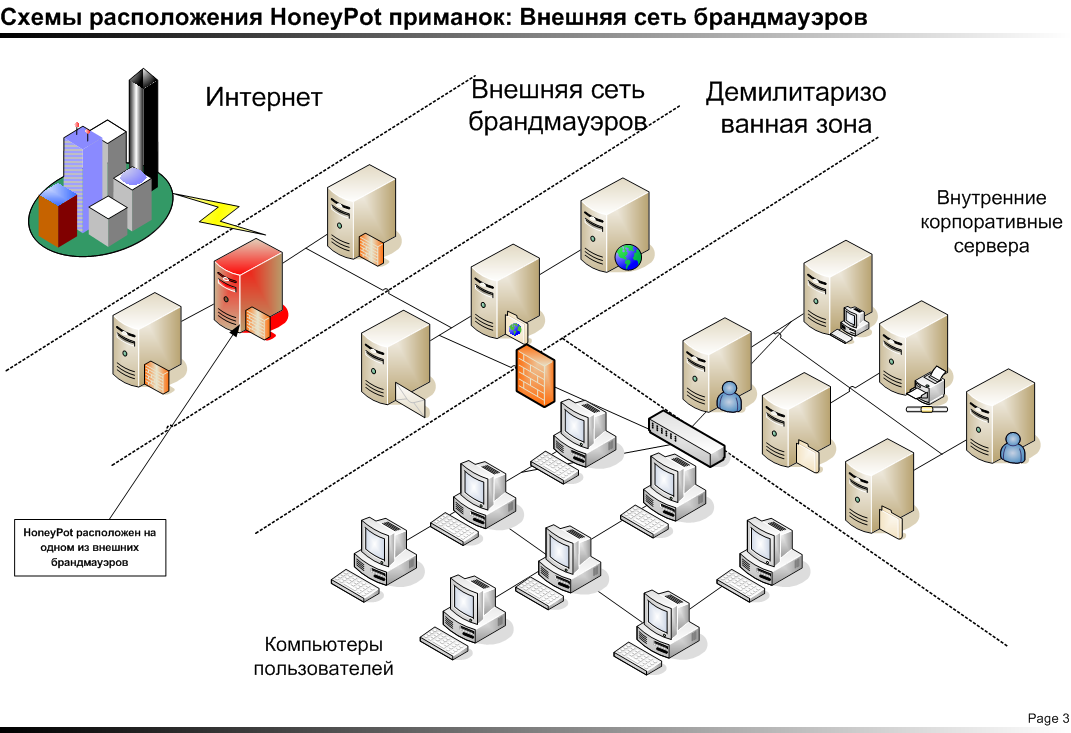
Высокоинтерактивные приманки работают как отдельные операционные системы, поэтому для их работы необходимы отдельные компьютеры и сервера. Для работы высокоинтерактивных HoneyPot-ов подходят и виртуальные машины, которые возможно создавать с помощью таких программных комплексов, как VMWare Server, Microsoft Virtual Server 2005, Parallels Workstation, Bochs, Qemu и т.д. Возможность использования виртуальных машин для построения виртуальных HoneyPot-ов будет исследована далее в выпускной работе.

**1.3 Размещение HoneyPot приманок в сети брандмауэров**

Размещение приманок на внешних брандмауэрах и в сети внешних брандмауэров.

### Такой способ размещения приманок предназначен для выявления атак, которые производятся из Интернета. Так как в большинстве случаев хакер пытается проникнуть в корпоративную сеть именно из внешней сети, такой как Интернет, или ближайшие сети провайдеров, то размещение приманок таким способом является необходимым.

### В данном случае работа HoneyPot напоминает работу обыкновенной IDS системы, но специфика работы HoneyPot позволяет открыть новые возможности для обнаружения и исследования сетевых атак: (рисунок 1.3.)

Рисунок 1.3 Схема расположения HoneyPot приманок: внешняя сеть брэндмауэра

### Размещение приманок в демилитаризованной зоне. DMZ (демилитаризованная зона)— технология обеспечения защиты информационного периметра, при которой сервера, отвечающие на запросы из внешней сети, или направляющие туда запросы, находятся в особом сегменте сети (который и называется DMZ).

При этом для DMZ осуществляется раздельная защита файрволлами, соединенными со внешней средой и с основной внутренней сетью.

Основное назначение DMZ - минимизировать последствия взлома сети, при этом взломщик получает (полный или частичный) контроль над серверами DMZ, но не имеет доступа к внутренним серверам или рабочим станциям.

Как правило, в DMZ сети размещаются сервера электронной почты (SMTP, POP3, IMAP, MAPI), файловые сервера (FTP), веб-сервера (HTTP), сервера регистрации и доступа к виртуальной частной сети (VPN).

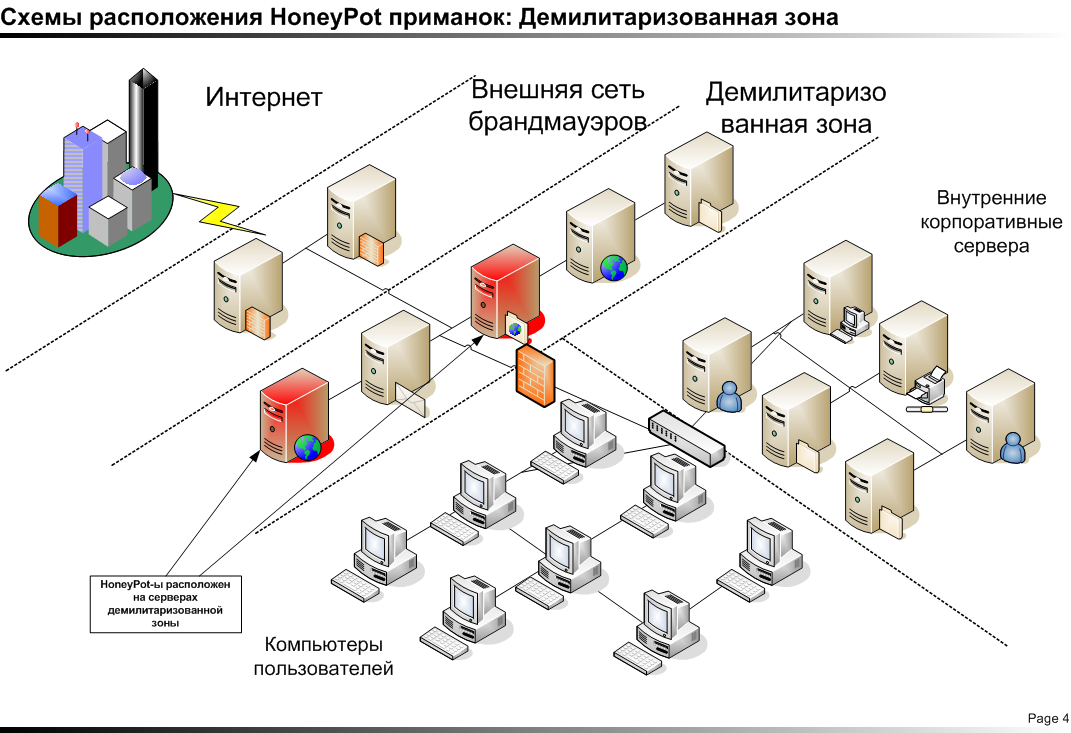
Такие сервера становятся объектами хакерских атак. Поэтому целесообразно разместить в DMZ сети одну или несколько приманок HoneyPot (рис. 1.4).

Рисунок 1.4 Схема расположения HoneyPot приманок: демилитаризованная зона

Нападение на одну или несколько приманок в DMZ скажет о том, что производится атака на сервера.

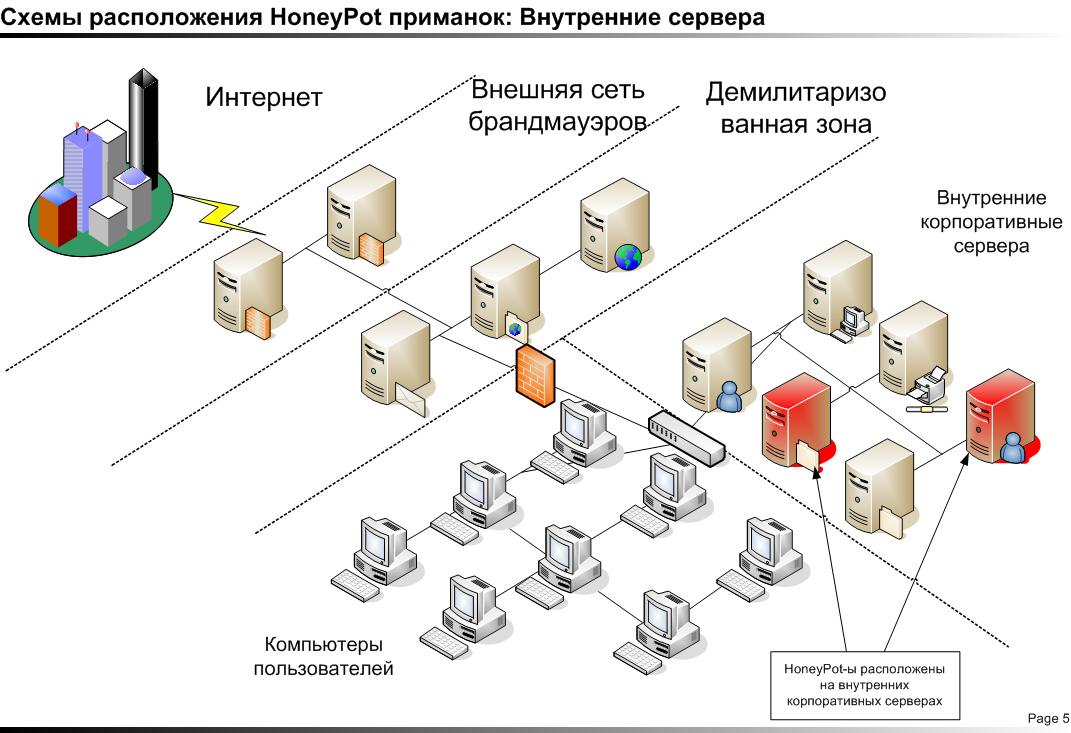
Размещение приманок в зоне внутренних корпоративных серверов

Не все сервера целесообразно размещать именно в DMZ. Часть серверов должна быть недоступна для пользователей Интернета, так как предназначены они именно для внутрикорпоративного использования. Такими серверами как правило являются внутренние файловые NFS, SMB и FTP сервера, хранящие конфиденциальную информацию, внутрикорпоративные документы и прочие другие материалы, не предназначенные для опубликования. Хранение такой информации на серверах, расположенных в DMZ, чревато попытками доступа к ней снаружи, так как даже использование различных механизмов защиты, таких как защита по паролю, по диапазону IP-адресов, не может обеспечить высокой степени защищенности информации. Такие методы защиты возможно обойти, используя ошибки и уязвимости в ПО серверов. Кроме того, усложняется доступ к информации от самих корпоративных пользователей. Поэтому в настоящее время большинство ИТ-специалистов предпочитают раздельное размещение таких серверов от DMZ-зоны (рисунок 1.5).

Также, в зоне внутренних корпоративных серверов размещаются контроллеры домена, сервера печати,сервера терминалов, DHCP и DNS сервера, сервера потоков мультимедиа(поддерживающие видеоконференции, интранет-радио) внутренние корпоративные порталы, сервера обмена документами, сервера новостей, коммуникационные сервера и т.д.

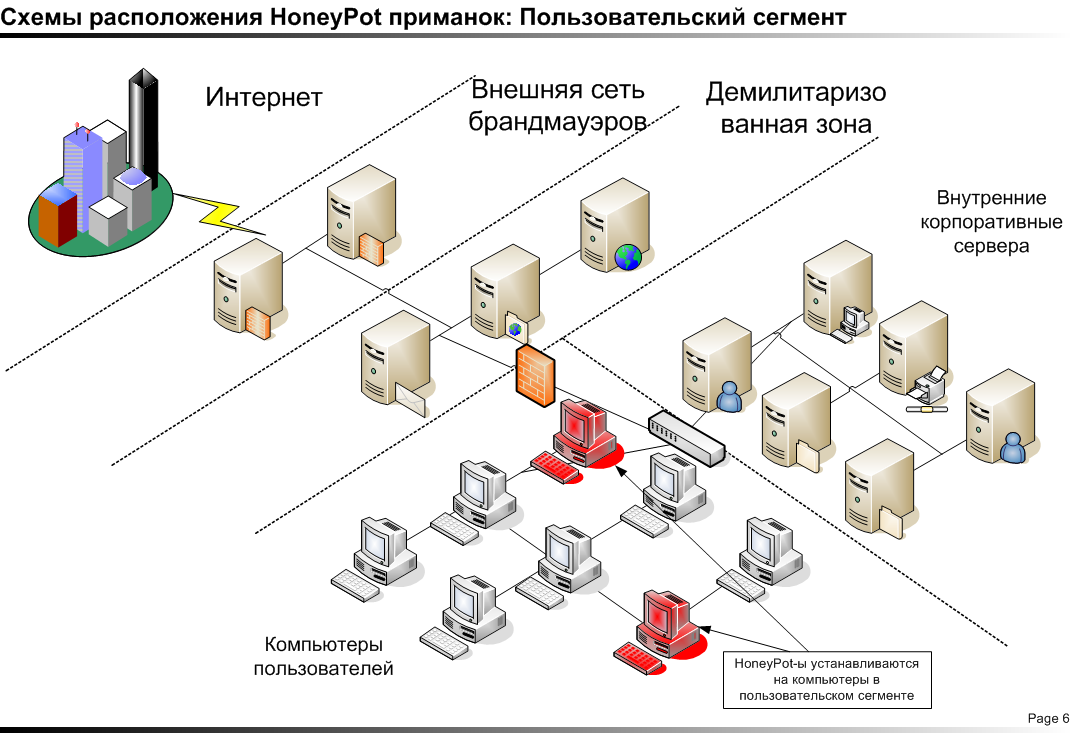
Но вместе с этим появляется другая очень важная проблема: всем известно, что в большинстве случаев политика доступа ко внутренним корпоративным ресурсам для внутренних пользователей не обладает должными мерами безопасности. Зачастую пренебрегаются даже базовые механизмы безопасности – аутентификация и авторизация. К сожалению, администраторы безопасности делают больший упор на защиту внешнего периметра – усиливают защиту брандмауэров, не защищая ресурсы внутренней сети.

Проникнуть на компьютеры пользователей можно большим количеством способов. Среди доступных способов – трояны, находящиеся в почтовых вложениях, уязвимости браузеров, через которые могут устанавливаться вредоносные программы на компьютер пользователей, методы социальной инженерии, трояны, распространяемые через программы мгновенного общения (ICQ, Jabber, Skype, Mail.ru агент, Windows Messenger и т.д.), по шифрованным каналам, которые не могут фильтроваться на антивирусном ПО на брандмауэре. Такая вредоносная программа, установленная на компьютер пользователя может обеспечить доступ взломщику, установив соединение с его компьютером изнутри. Компьютер пользователя становится завербованным. Взломщик автоматически получает все те же права, которыми обладает пользователь. Взломщик станет сканировать сервера сети на наличие доступных ресурсов.

Рисунок 1.5 Схема расположения HoneyPot приманок: Внутренние сервера

В сети корпоративных серверов могут располагаться как низкоинтерактивные приманки, работающие в качестве отдельных сервисов на штатных серверах, так и высокоинтерактивные HoneyPot-ы, которые выглядят как самостоятельные сервера.

Размещение приманок на компьютерах, находящихся в пользовательском сегменте.

 Рисунок 1.6 Схема расположения HoneyPot приманок: Пользовательский сегмент

Когда в корпоративной сети пользовательских компьютеров несколько сотен, то в таком случае невозможно отслеживать ни сетевую активность, ни активность самих программ. Стандартные средства сбора информации будут заваливать специалистов огромным объемом данных, которые очень сложно анализировать как машинным способом, так и простым анализом, производимым администратором безопасности. Поэтому необходимо искать кардинально новые подходы к обнаружению нелегитимных действий. HoneyPot системы позволяют решить этот вопрос (рис. 1.6).

Размещение ловушек в корпоративной сети, замаскированных под компьютеры обыкновенных пользователей будут выдавать минимальный объем информации по сравнению с классическими IDS системами [35]. Эта информация будет свидетельствовать именно о наличии взломщика.

### Смешанное размещение приманок. Наиболее часто используемым способом размещения приманок является смешанный способ. Суть его заключается в том, что приманки размещаются во всех сегментах сети. Этот метод эффективен тем, что зона покрытия, и, соответственно, вероятность обнаружения максимальны. При таком способе размещения могут использоваться десятки HoneyPot-ов, размещенных по всей сети (рис 1.7).

Здесь целесообразным является использование разных типов приманок, комбинирование низкоинтерактивных и высокоинтерактивных HoneyPot-ов, применение всего спектра сервисов.

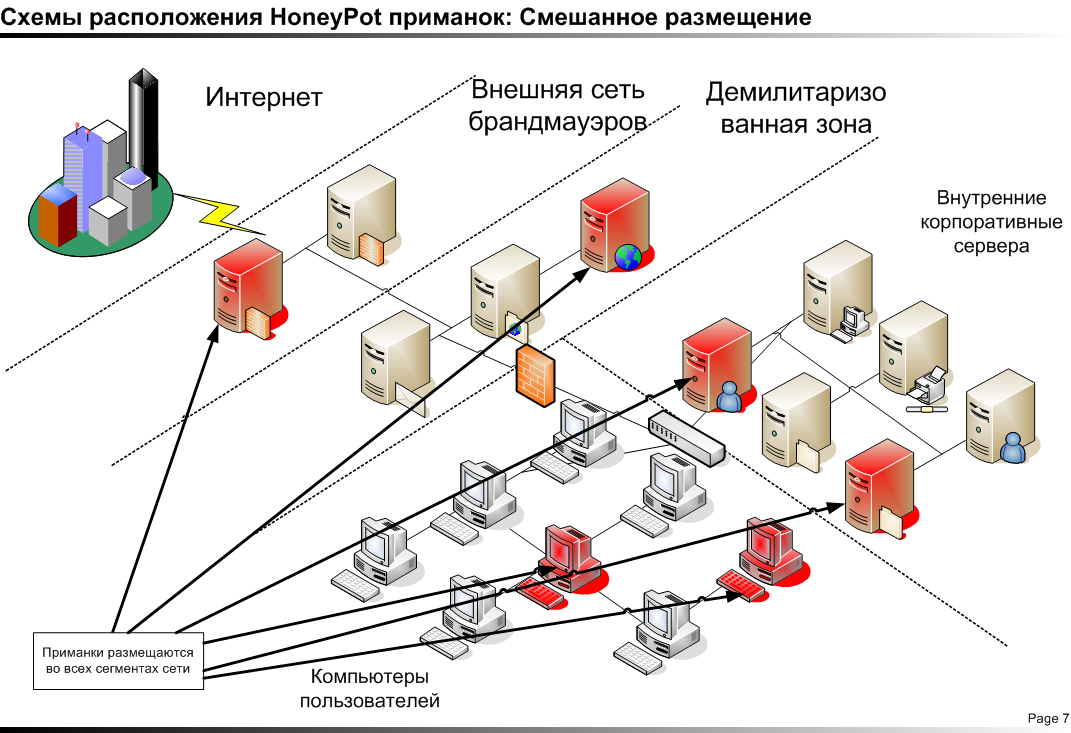
Одной из наиболее трудных проблем, с которой приходится справляться в случае использования большой HoneyPot инфраструктуры с разным типом приманок – это централизованный сбор системных сообщений в гетерогенной сети.

Рисунок 1.7 Схема расположения HoneyPot приманок: Смешанное размещение

Размещение приманок в Интернете. Возможность использования HoneyPot-а заключается в том, что будучи размещеннми на случайных серверах Интернета, они доступны для пересылки через себя почтового трафика. Особенность заключается в том, что пересылка почты через эти хосты осуществляется исключительно спамерами, так как обыкновенным пользователям эти SMTP-relay неизвестны. Спамеры узнают об этих хостах сканируя диапазоны сетей на наличие открытого 25-го порта. После того, как такие хосты обнаружены, проверяется, есть ли возможность пересылать через них почту. Так как HoneyPot-ы и предназначены для этого, то спамеры включают эти сервера в списки SMTP Relay серверов.

Проходящий трафик является исключительно незаконной рассылкой. Таким образом, с большой степенью достоверности можно вычислить спамеров, почтовые адреса, с которых производится рассылка, состав сообщений, IP-адреса хостов, с которых осуществляется доставка писем до HoneyPot-ов. Такая информация будет очень полезной при составлении списков адресов отправителей спама, локализации спамеров, сбора текстов спам-сообщений для настройки адаптивных спам-фильтров, работающих по Байесовому алгоритму, который анализирует спам-сообщения для выявления признаков, отличающих спам от легитимных сообщений.

Кроме того, HoneyPot-ы используются для замедления спам-рассылки. Например, HoneyD может быть настроен на прием сообщений на 25-й порт. 25-му порту ассоциируется выполняемый скрипт, который начинает работать при выполнении подключения на этот порт.

Спамер будет пытаться отправить почту через этот HoneyPot. Он будет думать, что спам пересыается, однако HoneyPot не станет этого делать. Для того чтобы одурачить спамеров с помощью технологии HoneyPot существует специальная программа BubbleGum ProxyPot. Единственной ее возможностью(с которой она весьма неплохо справляется), является именно обман спамеров с помощью симуляции открытого почтового прокси.

### Размещение приманки на веб-сервере. Почти у каждой организации (коммерческой или некоммерческой) есть свой веб-сервер, что может находиться на веб-сервере:

1. Сайт-визитка (набор статических страниц).
2. Корпоративный портал.
3. Система новостей.
4. Форум.
5. Календарь.
6. Корпоративные блоги.
7. Опросы.
8. Гостевые книги и т.д.
9. Интернет-магазин.

В настоящее время сложно найти успешный ресурс, который для своей работы не использует технологий динамических страниц, таких как PHP или ASP. Кроме этих, существуют и другие технологии, такие как Perl, Java Server Pages, Ruby on Rails, CGI-приложения и т.д. Но наиболее часто используются PHP и ASP. Причем, по популярности выигрывает все-таки PHP, так как язык является открытым, интерпретаторы PHP работают почти под всеми существующими серверными платформами. Разумеется, он отлично работает и под GNU/Linux и \*BSD. Напротив, ASP – куда более привередливая технология в плане поддержки платформ, и работает только на Microsoft Windows Server. Это обеспечивает более широкое распространение именно технологии PHP.

На языке программирования PHP написано много коммерческих и OpenSource CMS(Content Management System) – систем управления содержимым. Такие CMS, как Joomla, E107, Drupal, PHPNuke, Bitrix, MediaWiKi, DataLife Engine и пр. позволяют быстро и просто создать веб-портал. Большинство таких систем являются гибкими и масштабируемыми, что позволяет наращивать функциональность таких систем за счет применения сторонних модулей и расширений.

Но удобство и гибкость оборачиваются уменьшением безопасности таких систем. Современные CMS-системы могут содержать сотни тысяч строк кода. Учитывая статистику, что на каждую тысячу строк содержится в среднем 17 ошибок, то можно представить, какое количество ошибок может содержаться в большом портале.

Атаки хакера на веб-сервер заключаются во взломе защиты:

1. Операционной системы.
2. Дополнительных сервисов на веб-сервере.
3. Сервиса веб-приложений (Apache, IIS и т.д).
4. Служб серсивов веб приложений (PHP, ASP - интерпретаторы).
5. СУБД.
6. Использование уязвимостей CMS веб-сайта.

Защита ОС заключается в своевременной установке обновлений. Защита от уязвимостей дополнительных сервисов заключается переносом этих сервисов на другой сервер(разнесение). Защита от атак на сервисы веб-приложений также заключается в их своевременном обновлении. Защита от атак на службы сервиов веб-приложений заключается в ограничении функционала интерпретатора, использовании безопасных режимов и т.д. Защита СУБД заключается в аудите SQL-запросов на наличие возможности осуществления SQL-иньекций, ограничении прямого доступа к СУБД извне. Защита от использования хакером уязвимостей CMS-оболочки заключается в постоянном обновлении, ограничения доступа в админпанель и применении стандартных методов защиты веб-сервера.

Однако, взломы веб-сайтов наиболее часто происходят именно при взломе CMS-системы. В настоящее время хакеры при взломе веб-сайтов постоянно пользуются поисковыми машинами для сбора информации о взламываемом сайте. Поисковые роботы, индексируя сайт, собирают всю информацию с веб страниц, учитывая даже техническую. Кроме того, от поисковых машин не скрыть информации, которая может появиться в результате неправильной работы скрипта. Такой информацией может быть отчеты об ошибках интерпретатора языка, конфигурационные параметры веб-сервера, куски неинтерпретированного кода, файлы журналов доступа или даже файлы, содержащие пароли пользователей. Зачастую, CMS системы для увеличения своей популярности на каждой странице дают информацю о себе: какая CMS установлена и какая у нее версия. Таким образом, хакеру достаточно просто можно узнать об уязвимостях, связанных с работой какой-то конкретной CMS-системы, которые содержит в себе сервер.

Сравнительно недавно появился даже термин GoogleHack, который означает осуществление взлома с использованием информации, полученной от поисковых машин [35].

Для защиты таких ресурсов сложно применять обычный HoneyPot, потому как тот предназначен для обнаружения атак на цели, которые он сам же и эмулирует. Но веб-сервер – ресурс, который физически существует, и к которому обращаются легитимные пользователи.

Но разработчики HoneyPot-ов придумали, как использовать один из инструментов взломщиков против них самих. Идея заключается в создании подложных страниц, эмулирующих работу каких-либо CMS(например, форума phpBB) [35]. Посещение такой странцы будет свидетельствовать о том, что посетил ее либо злоумышленник, либо паук поисковой машины. Поведение паука достаточно предсказуемо – с посещением этой страницы он обязательно посетит и все остальные, причем промежуток времени между запросами других страниц с сервера будет очень коротким. Кроме того, паук обязательно «представляется»: в поле «User-Agent» http-запроса содержится имя паука, отличное от представления веб-браузера. Например, у Google – это будет GoogleBot. Таким образом, не представляет труда обнаружить взломщика, который производит разведывание возможных уязвимостей сервера, проинформировать об этом администратора безопасности и дать ему отпор.

Одним из таких HoneyPot-ов является «GoogleHack HoneyPot». Он представляет собой набор PHP файлов эмулирующих какую-либо уязвимость [33].

**1.4 Сбор и анализ информации**

Запись данных – это сбор и фиксация всей доступной информации связанной с атакой на HoneyPot (рисунок 1.8). Правильная запись данных крайне важна для успеха всех HoneyPot-мероприятий.

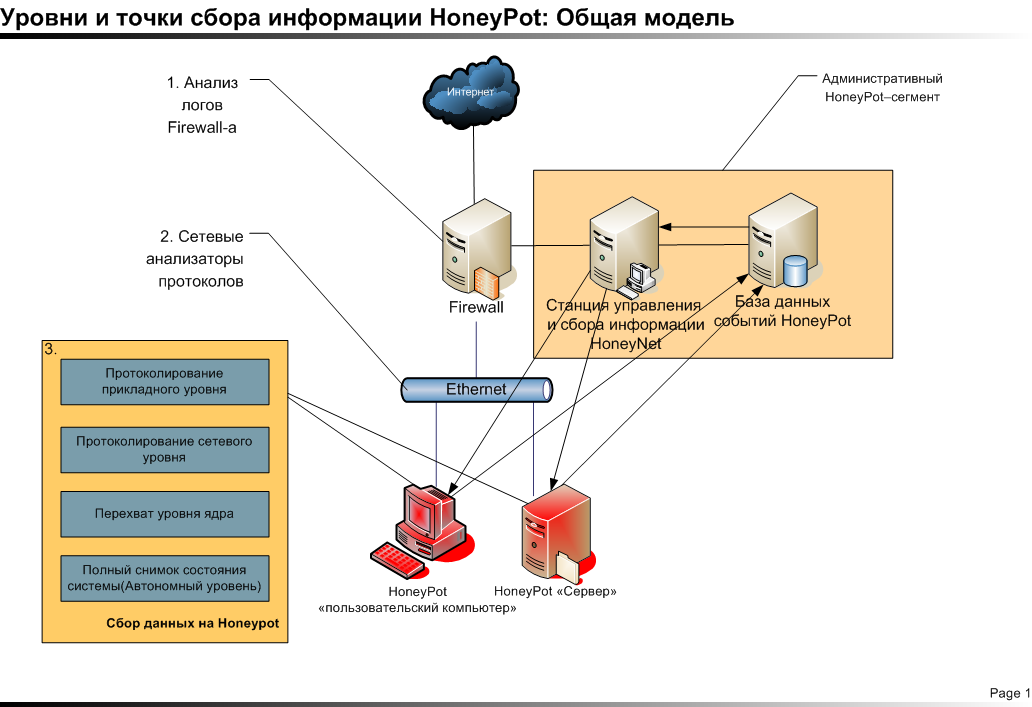
Доступным является большое количество разнообразных способов и методов сбора и агрегации информации. Не нужно зависеть от единственного способа. Зачастую очень сложно предугадать, как поведет себя хакер в этой системе, и как будет работать сама система в данный момент времени. Необходимо располагать средствами, позволяющими осуществлять сбор и протоколирование данных на разных уровнях системы и в разных точках сети.

Рисунок 1.8 Уровни и точки сбора информации HoneyPot: Общая модель

При сборе данных необходимо опираться именно на многоуровневую модель, так как только в таком случае можно быть уверенным, что имеем дело с наиболее полной и достоверной информацией. Хакер обязательно предпримет попытки затереть свои следы и уничтожить доказательства своего пребывания в системе. Поэтому необходимо иметь возможность хранить данные на удаленной системе и защищенным образом в локальной системе. С другой стороны, у локального хранения собранных данных существует опасность другого рода: если она будет обнаружена взломщиком, то у того будут все основания понять, что он находится на HoneyPot системе.

По-настоящему хорошим является лишь тот HoneyPot, который не может быть обнаружен. Если он будет обнаружен, то взломщик может попытаться нарушить целостность работы всей HoneyNet сети – HoneyPot системы, базы данных HoneyPot и станции управления HoneyPot(напр., Roo HoneyWall). Еще одна проблема, связанная с обнаружением – взломщик может попытаться подменить записываемую информацию, что, несомненно, отрицательно скажется на последующем анализе взлома.

Первым уровнем контроля доступа HoneyPot системы, является точка входа в сеть – маршрутизатор и брандмауэр. Вся информация, проходящая в систему первым делом должна контролироваться на брандмауэре, поэтому брандмауэр является отличным средством сбора первичной информации. Хотя, многие ИТ-специалисты и специалисты в области защиты информации считают журналы регистрации брандмауэра бесполезным средством, так как он за несколько часов работы может накопить десятки и сотни мегабайт информации. С другой стороны, многие современные брандмауэры являются гибкими средствами, поэтому можно настроить их под свои нужды. Совсем не обязательно собирать информацию о всех пакетах, проходящих через него. Так как правило и происходит, после чего информация от брандмауэра признается бесполезной. Для анализа работы HoneyPot вполне достаточно лишь той информации, которая обращена именно к нему. В таком случае информации будет совсем немного. Особенно, если учесть, что «по умолчанию» вся активность, обращенная к HoneyPot является подозрительной, то вся информация будет ценной для последующего анализа.

Кроме того, у брандмауэра есть еще несколько полезных качеств, которые обязательно необходимо использовать для успешного внедрения и сопровождения систем HoneyPot [35].

Первое полезное качество – ограничение внешней активности самого HoneyPot-а. Взломав HoneyPot, хакер может начать использовать его для своих нужд – атаки других серверов Интернета, рассылки спама и т.д. Таким образом, мы начинаем нести ответственность, связанную с тем, что HoneyPot установлен в нашей организации. Таким образом, претензии по поводу взлома внешних серверов Интернета в первую очередь будут предъявлять компании, в которой HoneyPot был установлен. Чтобы избежать лишних неприятностей, следует использовать политики безопасности брандмауэра, которые позволят ограничить внешнюю активность с HoneyPot-а в другие сети. Такой политикой может служить запрет на большое количество соединений, запрет рассылки почты, контроль распространения вредоносных программ, осуществляемый антивирусным модулем брандмауэра и т.д. С другой стороны, при создании политик следует учитывать, что слишком жесткие правила могут насторожить взломщика, дав ему возможность догадаться, что он находится в HoneyPot системе, а слишком мягкие правила предоставят ему излишнюю и опасную свободу действий.

Второе полезное качество – возможность извещения администратора безопасности о том, что появилась сетевая активность у HoneyPot системы, которая может говорить о появлении взломщика в сети. Обязательно должна существовать возможность вовремя известить о наличии опасности. Есть несколько способов, каждый из которых имеет свои преимущества и недостатки.

Звуковой сигнал на брандмауэре. Один из самых простых в реализации способов. При обнаружении опасности систем подает один или несколько звуковых сигналов на звуковую карту или в системный динамик. Звук может продолжаться до тех пор, пока его не отключит сам администратор безопасности, что будет свидетельствовать о том, что система смогла успешно проинформировать об угрозе. Наряду с очевидными преимуществами, есть столь-же очевидные недостатки – далеко не всегда администратор безопасности будет находиться рядом с брандмауэром, и если ему не сообщит о сигнале кто-то другой, кто его услышал, то угроза какое-то время будет оставаться необнаруженной. Особенно это неэффективно в нерабочее время, в выходные и праздничные дни (когда, кстати, и существует большой риск взлома систем).

Уведомление, содержащееся в почтовом сообщении. Такое уведомление может содержать в себе достаточно много первичной полезной информации. Но оно в первую очередь предназначено все-таки для информирования именно о факте взлома, а не о деталях, так как все равно не сможет содержать всю необходимую информацию о взломе. Для того чтобы получить информацию таким способом, у администратора безопасности должен быть постоянно запущен почтовый клиент, а он сам постоянно должен находиться на своем рабочем месте. Недостатки, в основном те же, что и у первого способа оповещения. Хотя, пользоваться почтой администратор безопасности может и в нерабочее время.

Уведомление с помощью клиентов мгновенного общения. Такие клиенты, как ICQ, Jabber, Yahoo IM, позволяют мгновенно передавать текстовые сообщения, в которых содержится информация о факте взлома. Преимущества и недостатки как у электронной почты.

Уведомление с помощью SMS. Мобильный телефон стал неотъемлемой частью нашей жизни. Почти у каждого человека он всегда он всегда с собой. Таким образом, можно сказать, что оповещение с помощью SMS является одним из наиболее эффективных способов. В настоящее время существуют провайдеры SMS сообщений, которые могут предоставлять услуги рассылки сообщений на телефоны абонентов различных операторов. Такие провайдеры предоставляют API, используя который можно реализовывать собственные программные механизмы оповещения о каких-либо системных событиях. За символическую плату можно завести аккаунт у такого провайдера и пользоваться таким способом оповещения об атаках.

Каждый способ оповещения имеет свои преимущества и недостатки. Лишь комбинация различных способов сможет достаточно эффективно информировать об опасности. Очевидно, что оповещение с помощью SMS является наиболее эффективным, поэтому нужно исследовать возможность использования этого способа. Хотя, вместе с тем, на следует пренебрегать и другими способами оповещений.

Для низкоинтерактивных HoneyPot-систем сбор информации осуществляется либо на компьютере с самим модулем приманки, либо на удаленном компьютере. В отличии от высокоинтерактивного HoneyPot, для низкоинтерактивного в плане безопасности нет никаких проблем, связанных с тем, что данные могут быть скомпрометированы. Но, зачастую низкоинтерактивные HoneyPot-ы снабжают функционалом, позволяющим собирать информацию удаленно на специальные выделенные сервера. Но это скорее связано с тем упрощением администрирования и сопровождения таких систем, а также более эффективному и быстрому информированию о проходящей атаке. Это особенно актуально в масштабах предприятия, где HoneyPot – сенсоров может стоять несколько десятков.

Для высокоинтерактивного HoneyPot-а необходимо искать возможности именно удаленной регистрации событий, а также удаленного хранения информации о взломе и происшествиях в системе. Это связано именно с тем, что будучи взломанным, HoneyPot не сможет должным образом защитить информацию, которую он собирает о процессе взлома системы. Также, существует большой риск того, что информация будет модифицирована самим взломщиком, что сделает последующий анализ атаки бесполезным. Помимо этого, запись данных на локальный жесткий диск может быть сравнительно легко обнаружена, что позволит взломщику заметить, что он находится в ловушке. Такой HoneyPot-системе доверять нельзя. Высокоинтерактивные приманки должны обеспечивать возможность удаленного протоколирования событий.

Виртуальная машина, или, иначе, VM - это программа, которая эмулирует настоящий физический компьютер, притом таким образом, что на этот компьютер можно установить операционную систему и приложения, которые будут работать, не подозревая о том, что работают они не на физическом компьютере, а в программной среде [35]. При этом виртуальная машина может создавать различные аппаратные конфигурации (в некоторых пределах) - например, можно определить, сколько памяти получит та или иная виртуальная машина. Сама программа эмуляции, равно как и работающая на ней операционная система, называется виртуальной машиной, в то время как основная операционная система и физическая машина называются хост-системой. Задействованные виртуальной машиной ресурсы или "вырезаются" из основного пула ресурсов (как, например, происходит с оперативной памятью), или раздельно используются и хост, и виртуальной системами - как это происходит с процессором и съемными носителями.

HoneyPot системы требуют для себя мало ресурсов – по сути они работают только тогда, когда на них производится нападение. Таким образом, они находятся в состоянии ожидания.

Целесообразность использования виртуальных машин для размещения на них HoneyPot-ловушек заключается в большом числе факторов [35]:

1. Экономия – для установки десятка высокоинтерактивных HoneyPot-ов достаточно одного сервера.
2. Простота сопровождения – гораздо проще отслеживать аппаратное состояние одной физической машины, чем десятка, разнесенных территориально
3. Удобство развертывания – для развертывания HoneyPot систем можно подготовить эталонный образ с системой и развернуть его на большое количество машин
4. Механизмы снимков(snapshot) – позволяют за несколько минут «откатить» систему до первоначального состояния
5. Снижение полной стоимости обслуживания(TCO) – простота управления такой системой позволит уменьшить число задействованного персонала.
6. Возможность совместного использования – сервера с HoneyPot-ами можно устанавливать параллельно обыкновенным серверам – так как HoneyPot потребляет мало ресурсов, то он почти не будет оказывать влияния на производительность целевого сервера.
7. Изоляция – виртуальные машины на физическом сервере никак не могут вторгаться в адресное пространство других машин.
8. Интероперабельность – многие компании уже используют технологии виртуализации для обыкновенных серверов, поэтому внедрение виртуальных HoneyPot произойдет очень легко.
9. Тестирование – перед внедрением можно удобно протестировать HoneyPot на виртуальной машине. После тестирования образ можно легко перенести на сервер.

В настоящее время существует несколько технологий виртуализации. Выделив наиболее часто используемые системы, можно отметить следующие типы виртуальных машин, которые можно использовать для создания HoneyPot – систем и построения HoneyPot – инфраструктуры. К таким типам можно отнести:

**Глава 2. Анализ деятельности Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови»**

**2.1 Общая характеристика Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови»**

Государственное бюджетное учреждение здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови», именуемое в дальнейшем «Учреждение», является государственным бюджетным учреждением здравоохранения Республики Адыгея, финансовое обеспечение выполнения функций которого, осуществляется за счет средств республиканского бюджета Республики Адыгея, а также иных, предусмотренных действующим законодательством, источников.

Учреждение создано 2 апреля 1992 года в соответствии с приказом Министерства здравоохранения Республики Адыгея № 94 «О переименовании областных ЛПУ».

В соответствии с [постановлением](garantF1://6292330.1147) Кабинета Министров Республики Адыгея от 09.07.2007 г. № 117 Учреждение находится в ведении Министерства здравоохранения Республики Адыгея.

Учредителем Учреждения является Республика Адыгея. Учреждение подведомственно Министерству здравоохранения Республики Адыгея, которое осуществляет от имени Кабинета Министров Республики Адыгея функции и полномочия учредителя Учреждения (далее - Учредитель) в соответствии с законодательством Российской Федерации и законодательством Республики Адыгея.

Собственником имущества Учреждения является Республика Адыгея. Функции и полномочия собственника имущества Учреждения осуществляет Комитет Республики Адыгея по имущественным отношениям (далее – Собственник).

Учредитель действует в рамках своей компетенции, осуществляет координацию деятельности и оказывает организационно-методическую и практическую помощь Учреждению.

Учредитель в отношении Учреждения является главным распорядителем бюджетных средств.

Учреждение в своей деятельности руководствуется [Конституцией](garantF1://10003000.0) Российской Федерации и Республики Адыгея, федеральными законами, актами Президента Российской Федерации, Правительства Российской Федерации, законодательством Республики Адыгея, иными нормативными правовыми актами, а также настоящим уставом.

Учреждение является юридическим лицом - бюджетным учреждением (некоммерческой организацией), созданным в соответствии с [законодательством](garantF1://10064072.120) Российской Федерации и Республики Адыгея для выполнения работ и оказания услуг в целях обеспечения реализации предусмотренных законодательством Российской Федерации полномочий органов государственной власти Республики Адыгея в сфере здравоохранения, обладает на праве оперативного управления обособленным имуществом, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде в соответствии с законодательством Российской Федерации.

Учреждение имеет самостоятельный баланс, лицевой счет, открытый в территориальных органах Федерального казначейства, по учету средств республиканского бюджета Республики Адыгея и средств, полученных от приносящей доходы деятельности в валюте Российской Федерации, круглую печать с изображением Государственного герба Республики Адыгеи со своим полным наименованием на русском и адыгейском языках и наименованием Учредителя, собственную эмблему, а также печати, штампы, бланки со своим наименованием.

Учреждение самостоятельно формирует свою структуру, в которую входят:

- общеучрежденческий медицинский персонал;

- организационно-методический отдел;

- отдел комплектования и медицинского освидетельствования доноров;

- отдел заготовки крови и ее компонентов;

- отдел подготовки материалов и растворов;

- клиническая лаборатория;

- иммунологическая лаборатория;

- бактериологическая лаборатория;

- отдел контроля качества;

- административно-хозяйственный персонал.

Наименование Учреждения:

полное:

- на русском языке: Государственное бюджетное учреждение здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови»;

- на адыгейском языке: Адыгэ Республикэм псэуныгъэм икъэухъумэнкIэ къэралыгъо бюджетнэ IофшIапIэу «Лъыр зыщатырэ Адыгэ Республикэ станциер».

Сокращенное:

- на русском языке: ГБУЗРА «АРСПК»

Место нахождения Учреждения: Республика Адыгея, г.Майкоп, ул. 12 Марта, 163.

Устав Учреждения, все изменения и дополнения к нему утверждаются Учредителем после предварительного согласования с Собственником и подлежат регистрации в установленном порядке.

Целью создания Учреждения является организация службы заготовки и переливания крови в Республике Адыгея. Предметом деятельности Учреждения является: отбор и обследование доноров крови и ее компонентов, заготовка донорской крови и переработка на компоненты, обеспечение безопасности крови, хранение компонентов крови и их перевозку, изготовление диагностических сывороток.

Для достижения целей, определенных в Уставе, Учреждение осуществляет следующие виды деятельности, выполняемые за счет средств республиканского бюджета Республики Адыгея (средств обязательного медицинского страхования):

Доврачебная помощь

- работы и услуги по специальности – лабораторная диагностика;

- работы и услуги по специальности – сестринское дело.

Амбулаторно-поликлиническая помощь, в том числе в условиях дневного стационара и стационара на дому:

- работы и услуги по специальности - клиническая лабораторная диагностика;

- работы и услуги по специальности – терапия;

- работы и услуги по специальности – трансфузиология.

Стационарная помощь, в том числе в условиях дневного стационара:

- работы и услуги по специальности – трансфузиология.

Прочие работы и услуги:

- работы и услуги по заготовке, производству, транспортировке и хранению донорской крови, ее компонентов и препаратов;

- работы и услуги по специальности - организация сестринского дела;

- работы и услуги по предрейсовым медицинским осмотрам водителей транспортных средств;

- работы и услуги по специальности – бактериология.

Учреждение для достижения основных целей, предусмотренных в настоящем Уставе, может осуществлять по договорам, контрактам с юридическими и физическими лицами, в том числе заключенным в рамках реализации федеральных, отраслевых, региональных, ведомственных программ, на возмездной основе следующие виды приносящей доходы деятельности:

- оказание платных медицинских услуг за рамками объемов, устанавливаемых Учредителем;

Учреждение выполняет работы и оказывает услуги по ценам, установленным в соответствии с законодательством Российской Федерации и Республики Адыгея.

Видами деятельности согласно [разделу 2](#sub_1200) в случаях, установленных [законодательством](garantF1://12023874.17), Учреждение может заниматься только на основании специального разрешения (лицензии).

Перечень видов деятельности, перечисленный в настоящем уставе, является исчерпывающим.

В целях обеспечения уставной деятельности за Учреждением закрепляется на праве оперативного управления государственное имущество Республики Адыгея.

Учреждение вправе приобретать за счет средств от приносящей доход деятельности имущество в порядке, установленном [законодательством](garantF1://10064072.296) Российской Федерации и Республики Адыгея.

Земельные участки, необходимые для выполнения Учреждением своих уставных целей и задач, предоставляются ему на праве постоянного (бессрочного) пользования.

Объекты культурного наследия (памятники истории и культуры) народов Российской Федерации, культурные ценности, природные ресурсы (за исключением земельных участков), ограниченные для использования в гражданском обороте или изъятые из гражданского оборота, закрепляются за бюджетным учреждением на условиях и в порядке, которые определяются [федеральными законами](garantF1://12027232.800) и иными нормативными правовыми актами Российской Федерации.

Имущество Учреждения является государственной собственностью Республики Адыгея. Учреждение несет ответственность за сохранность, целевое и эффективное использование закрепленного за ним имущества, обеспечивая в установленном [законодательством](garantF1://10036812.3) Российской Федерации и Республики Адыгея порядке учет указанного имущества, включая имущество, приобретенное за счет средств, полученных от приносящей доходы деятельности, а также обязано представлять сведения об имуществе, приобретенном Учреждением за счет доходов, полученных от приносящей доходы деятельности, в исполнительный орган государственной власти Республики Адыгея, осуществляющий ведение реестра государственного имущества Республики Адыгея.

Учреждение реализует право владения, пользования и распоряжения в отношении закрепленного за ним на праве оперативного управления имущества в порядке, установленном [законодательством](garantF1://10064072.296) Российской Федерации и Республики Адыгея и настоящим Уставом.

Учреждение отвечает по своим обязательствам тем своим имуществом, на которое по законодательству Российской Федерации может быть обращено взыскание. Собственник имущества не несет ответственности по обязательствам Учреждения.

Учреждению запрещается совершать сделки, возможными последствиями которых является отчуждение или обременение имущества, закрепленного за Учреждением, или имущества, приобретенного за счет средств, выделенных этому Учреждению из республиканского бюджета Республики Адыгея или бюджета государственного внебюджетного фонда Российской Федерации, если иное не установлено законодательством Российской Федерации.

Источники формирования имущества Учреждения:

- имущество, закрепленное за Учреждением на праве оперативного управления в порядке, установленном [законодательством](garantF1://10064072.296) Российской Федерации и Республики Адыгеи;

- имущество, приобретенное Учреждением за счет средств республиканского бюджета Республики Адыгеи и средств, полученных от приносящей доходы деятельности;

- иные источники получения имущества, предусмотренные законодательством Российской Федерации.

Источники финансирования Учреждения:

- субсидии из республиканского бюджета Республики Адыгеи на финансовое обеспечение выполнения государственного задания на оказание услуг (выполнение работ);

- субсидии на иные цели;

- бюджетные инвестиции;

- средства, полученные от приносящей доход деятельности;

- средства, полученные при возмещении затрат на эксплуатационные, коммунальные и административно-хозяйственные услуги от арендаторов;

- средства, полученные от сдачи помещений в аренду;

- средства, полученные в виде безвозмездных благотворительных поступлений и добровольных пожертвований;

- средства, полученные от участников конкурсов на размещение заказов на поставку товаров (выполнение работ, оказание услуг) для государственных нужд;

- средства, поступающие в счет оплаты медицинских услуг, в том числе по договорам добровольного и обязательного медицинского страхования;

- средства, полученные в виде грантов на осуществление научной деятельности;

- иные источники, предусмотренные законодательством Российской Федерации.

Финансовое обеспечение функций Учреждения до принятия Учредителем решения о предоставлении Учреждению субсидий в соответствии со [статьей 78.1](garantF1://12012604.781) Бюджетного кодекса Российской Федерации осуществляется за счет средств республиканского бюджета Республики Адыгея на основе бюджетной сметы.

Права Учреждения на объекты интеллектуальной собственности, созданные им в процессе осуществления деятельности, регулируются в соответствии с [законодательством](garantF1://10064072.40700) Российской Федерации.

Учреждение без согласия собственника не вправе распоряжаться особо ценным движимым имуществом, закрепленным за ним собственником или приобретенным Учреждением за счет средств, выделенных ему собственником на приобретение такого имущества, а также недвижимым имуществом.

Остальным находящимся на праве оперативного управления имуществом бюджетное учреждение вправе распоряжаться самостоятельно, если иное не предусмотрено действующим законодательством.

Учреждение не вправе размещать денежные средства на депозитах в кредитных организациях, а также совершать сделки с ценными бумагами, если иное не предусмотрено федеральными законами.

Финансовое обеспечение выполнения государственного задания осуществляется с учетом расходов на содержание недвижимого имущества и особо ценного движимого имущества, закрепленных за бюджетным учреждением учредителем или приобретенных бюджетным учреждением за счет средств, выделенных ему учредителем на приобретение такого имущества, расходов на уплату налогов, в качестве объекта налогообложения по которым признается соответствующее имущество, в том числе земельные участки и других расходов, которые несет Учреждение при выполнении государственного задания.

В случае сдачи в аренду с согласия учредителя недвижимого имущества и особо ценного движимого имущества, закрепленного за бюджетным учреждением учредителем или приобретенного бюджетным учреждением за счет средств, выделенных ему учредителем на приобретение такого имущества, финансовое обеспечение содержания такого имущества учредителем не осуществляется.

Контроль за использованием имущества, находящегося в оперативном управлении Учреждения, осуществляет Учредитель и Собственник.

Право оперативного управления имуществом Учреждения прекращается по основаниям и в порядке, предусмотренным действующим [законодательством](garantF1://10064072.299) для прекращения права собственности.

Учреждение вправе передавать некоммерческим организациям в качестве их учредителя или участника денежные средства (если иное не установлено условиями их предоставления) и иное имущество, за исключением особо ценного движимого имущества, закрепленного за ним или приобретенного за счет средств, выделенных ему собственником на приобретение такого имущества, а также недвижимого имущества только по предварительному согласованию с Учредителем.

Решение об одобрении крупных сделок, а также сделок, в совершении которых у Учреждения имеется заинтересованность, определяемая в соответствии с критериями, установленными в [статье 27](garantF1://10005879.27) Федерального закона от 12.01.1996 N 7-ФЗ «О некоммерческих организациях» принимается Учредителем.

Под крупной сделкой признается сделка или несколько взаимосвязанных сделок, связанная с распоряжением денежными средствами, отчуждением иного имущества (которым в соответствии с федеральным законом бюджетное учреждение вправе распоряжаться самостоятельно), а также с передачей такого имущества в пользование или в залог при условии, что цена такой сделки либо стоимость отчуждаемого или передаваемого имущества превышает 10 процентов балансовой стоимости активов бюджетного учреждения, определяемой по данным его бухгалтерской отчетности на последнюю отчетную дату.

Учреждение имеет (не имеет) филиалов и представительств.

Учреждение строит свои отношения с государственными органами, другими юридическими и физическими лицами во всех сферах на основе настоящего Устава, договоров, соглашений, контрактов.

Для выполнения уставных целей Учреждение имеет право в установленном порядке:

- планировать свою деятельность и определять перспективы развития по согласованию с Учредителем;

- заключать договоры с юридическими и физическими лицами в целях осуществления приносящей доходы деятельности;

- получать и использовать доходы от разрешенной настоящим Уставом приносящей доходы деятельности;

- участвовать в научно-практических мероприятиях, съездах, научных и научно-практических конференциях, симпозиумах по проблемам медицины по профилю деятельности Учреждения;

- осуществлять права и обязанности субъекта интеллектуальной деятельности, в том числе правовую охрану и использование результатов интеллектуальной деятельности, в соответствии с [законодательством](garantF1://10064072.40700) Российской Федерации;

- устанавливать для своих работников дополнительные отпуска, сокращенный рабочий день и иные социальные льготы в соответствии с [законодательством](garantF1://12025268.116) Российской Федерации;

- осуществлять внешнеэкономическую деятельность по согласованию с Учредителем;

- в установленном порядке определять размер средств, направляемых на оплату труда работников Учреждения и их поощрение, на производственное и социальное развитие;

***-*** выполнять функции государственного заказчика по проектированию, реконструкции, расширению и техническому перевооружению, капитальному ремонту объектов капитального строительства, находящихся у Учреждения на праве оперативного управления с 01.01.2012 г.;

- осуществлять организацию капитального ремонта и проводить текущий ремонт зданий, строений, сооружений, находящихся в оперативном управлении Учреждения;

- получать лицензии (разрешения), необходимые для осуществления видов деятельности, предусмотренных настоящим Уставом;

- командировать работников Учреждения, в том числе за границу Российской Федерации, для изучения имеющегося опыта работы в сфере деятельности Учреждения в порядке, установленном действующим законодательством;

- принимать и увольнять работников в соответствии с [законодательством](garantF1://12025268.1011) Российской Федерации;

- осуществлять размещение заказов на поставку товаров, выполнение работ и оказание услуг для государственных нужд, необходимых для осуществления деятельности Учреждения за счет бюджетных ассигнований республиканского бюджета Республики Адыгея и иных источников финансового обеспечения;

- участвовать в соответствии с [законодательством](garantF1://10005879.11) Российской Федерации в работе ассоциаций, союзов и иных общественных организаций по профилю деятельности Учреждения на территории Российской Федерации и за границей Российской Федерации.

4.3. Учреждение обязано:

- обеспечивать исполнение своих обязательств в соответствии с государственным заданием, планом финансово-хозяйственной деятельности и в пределах денежных средств, полученных в установленном порядке от приносящей доход деятельности;

- нести ответственность в соответствии с [законодательством](garantF1://10064072.393) Российской Федерации за нарушение обязательств;

- отчитываться перед Учредителем за состояние и использование имущества и денежных средств и представлять необходимую сметно-финансовую документацию в полном объеме утвержденных форм и по всем видам деятельности;

- возмещать ущерб, причиненный нерациональным использованием земли и других природных ресурсов, загрязнением окружающей среды, нарушением правил безопасности производства, санитарно-гигиенических норм и требований по защите здоровья работников, населения и потребителей продукции, за счет результатов своей деятельности;

- платить налоги и производить иные обязательные отчисления, предусмотренные [законодательством](garantF1://10800200.3001) Российской Федерации;

- обеспечивать своевременно и в полном объеме выплату заработной платы работникам в соответствии с [законодательством](garantF1://12025268.136) Российской Федерации;

- обеспечивать своим работникам безопасные условия труда и нести ответственность в установленном порядке за вред, причиненный работнику увечьем, профессиональным заболеванием либо иным повреждением здоровья, связанным с исполнением им трудовых обязанностей;

- обеспечивать сохранность документов (управленческих, финансово-хозяйственных, по личному составу и других);

- обеспечивать передачу на государственное хранение документов, имеющих научно-историческое значение, в архивные фонды;

- осуществлять организацию и ведение бюджетного, налогового, статистического учета и представление бюджетной отчетности Учредителю в порядке, установленном федеральным органом исполнительной власти, осуществляющим выработку единой государственной финансовой, кредитной, денежной политики для бюджетных учреждений;

- не допускать нарушений [бюджетного законодательства](garantF1://12012604.20001) Российской Федерации;

- представлять сведения об имуществе, в том числе, приобретенном за счет средств, полученных от приносящей доходы деятельности, в исполнительный орган государственной власти, осуществляющий ведение реестра государственного имущества Республики Адыгея;

- выполнять государственные мероприятия по гражданской обороне и мобилизационной подготовке в соответствии с законодательством Российской Федерации.

Учреждение в своей деятельности использует формы первичных учетно-отчетных документов и бланков строгой отчетности, утверждаемых в установленном порядке.

Учреждение обеспечивает сохранность государственной тайны в соответствии с возложенными целями и в пределах своей компетенции.

Проверку по всем видам деятельности Учреждения осуществляют Учредитель, другие уполномоченные федеральные органы государственной власти и органы государственной власти Республики Адыгея в пределах их полномочий, установленных законодательством Российской Федерации.

**2.2** **Локальная вычислительная сеть Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови»**

Объект информатизации «Автоматизированная информационная система Государственного учреждения здравоохранения «Адыгейская республиканская станция переливания крови»(далее - АИС РИЦ) предназначен для сбора, хранения и обработки информации Службы крови России.

В соответствии с Перечнем защищаемых ресурсов АИС РИЦ, эта информация относится к конфиденциальной, содержащей сведения, относящиеся к служебной тайне и сведения, содержащие персональные данные.

АИС РИЦ Службы крови России реализует следующие функции:

* регистрацию и ввод данных о донорах в базу данных (персональные данные);
* предоставление информации о донорах и кроводачах в Федеральный информационный центр по защищенным каналам связи;
* создание и предоставление статистических отчетов.

Контролируемая зона размещения Автоматизированной информационной системы: Контролируемой зоной размещения АИС РИЦ являются все помещения и коридоры здания, где размещаются рабочие станции, серверное оборудование и линии связи АИС РИЦ, приведённые на рисунке 2.1.

Схема размещения Автоматизированной информационной системы с указанием коммутационного оборудования и линий связи приведена на рисунке 2.1.

Рисунок 2.1 Локальная вычислительная сеть

Структурно-функциональная схема Автоматизированной информационной системы приведена на рисунке 2.2.



Рисунок 2.2 Структурно-функциональная схема объекта информатизации

Пользователи АИС РИЦ работают с различными правами доступа к различным видам информации, хранящейся и обрабатываемой в АИС РИЦ и техническим ресурсам АИС РИЦ. Разграничение прав доступа пользователей к защищаемым ресурсам приведено в документе «Таблица разграничения доступа к защищаемым ресурсам АИС РИЦ». Учётные записи пользователей могут быть включены в разные группы Active Directory. Это допускается для разграничения прав к различным компонентам базы данных и ресурсам домена. На каждом АРМ пользователей присутствует встроенная учётная запись локального администратора, необходимая для устранения ответственным специалистом по защите информации нештатных ситуаций.

Работа пользователей на средствах вычислительной техники АИС РИЦ осуществляется по утвержденному «Списку пользователей, допущенных к обработке конфиденциальной информации на объекте информатизации «Автоматизированная информационная система Государственного учреждения здравоохранения «Адыгейская республиканская станция переливания крови» (приложение).

Распределение IP-адресов в АИС РИЦ осуществляется средствами DHCP за исключением серверного и коммутационного оборудования.

Для обеспечения возможности удаленного централизованного администрирования и управления оборудованием РИЦ из ФИЦ ФМБА в АИС РИЦ применяются коммутаторы KVM (клавиатура, видео, мышь) серии Avocent DSR совместно с программным комплексом DSView 3.0. Коммутатор с помощью специализированных кабельных окончаний (KVM) подключается к портам клавиатуры, видео и мыши серверов и передает потоки данных на удаленные консоли операторов (служба системных администраторов ФИЦ). Кроме того коммутатор серии Avocent DSR с помощью специализированных кабельных окончаний (RS-232) подключается к консольным портам основного сетевого оборудования, и тем самым обеспечивает внешнее управление оборудованием. Доступ к управляющей консоли осуществляется через использование TCP/IP, протоколов Telnet или SSH. В серверах и АРМ для мониторинга используется технология Intel vPRO.

Кроме того в системе централизованного управления и мониторинга серверным оборудованием ФМБА используется ПО LANDesk Server Manager, которое предназначено для инвентаризации серверного оборудования, АРМ, их компонент и периферийных устройств, а также учета и сбора статистики по использованию установленного на ПЭВМ ПО. Управление данным ПО производится удаленно администратором ФИЦ ФМБА.

Для начала работы на персональной электронной вычислительной машине (далее ПЭВМ) пользователь подсоединяет свой персональный eToken ключ к USB-входу ПЭВМ, вводит идентификационные и аутентификационные данные (логин и PIN-код). Средствами установленного на каждом АРМ и сервере ПО (eToken и Windows) проводится идентификация и аутентификация пользователей, после чего пользователь (в случае успешной идентификации и аутентификации) получает доступ к запрашиваемым информационным ресурсам. Если пользователю не был выдан персональный eToken ключ, то процедура идентификации и аутентификации производится только средствами ОС Windows (пользователь вводит логин и пароль).

При работе с ПО «АИСТ» пользователь вводит дополнительные идентификационные и аутентификационные данные, которые могут не совпадать с идентификационными и аутентификационными данными его учетной записи в Active Directory домена АИС РИЦ.

В АИС РИЦ применяются сканеры штрих кодов для контроля идентификационных марок пакетов с кровью для создания идентификационного изображения донора.

В АИС РИЦ используется ПО контроля доступа к устройствам DeviceLock. Настройки ПО DeviceLock обеспечивают ограничения использования съёмных носителей, устройств и ведение журнала учета.

Пользователям домена АИС РИЦ разрешён доступ только к жестким дискам ПЭВМ и локальным принтерам (в том числе термотрансферным принтерам). Доступ к USB портам запрещен, за исключением электронных ключей eToken, учтенных соответствующим образом съёмных носителей информации, сканеров штрих кодов, Web камер, локальных принтеров. На группу администраторов ограничений по использованию сменных носителей и устройств не накладывается.

Для регистрации действий пользователя используются средства регистрации операционной системы Microsoft Windоws XP, Microsoft Windows Server 2003 R2 и ПО DeviceLock.

В АИС РИЦ на каждом АРМ и сервере ответственным специалистом по защите информации установлен пароль на BIOS, также произведена настройка BIOS разрешающая загрузку только с локального жесткого диска ПЭВМ.

Процедура подключения новых пользователей и предоставления им прав на использование данных из БД в АИС РИЦ выполняется в соответствии с «Инструкцией ответственному специалисту по защите информации».

После внесения изменений в списки пользователей администратор АИС РИЦ должен обеспечить настройки рабочих станций и настройки используемых на АРМ и серверах АИС РИЦ специализированных средств защиты от НСД.

В качестве устройства вывода информации на «твердую копию» (на бумагу) могут использоваться принтеры. Печать может осуществляться следующим образом:

* печать конфиденциальной информации выполняется на листы, учтенные установленным порядком. Учет листов ведется в «Журнале учета печати конфиденциальной информации»;
* печать открытой информации осуществляется на неучтенные листы.

Пользователь несет полную ответственность за соблюдение правил вывода информации на печать. Контроль вывода информации на печать осуществляет Ответственный специалист по защите информации АИС РИЦ.

Вся информация, хранящаяся и обрабатываемая в АИС РИЦ, проверяется на отсутствие вирусов с использованием антивирусного ПО Kaspersky Business Space Security Russian Edition. Обновление баз вирусных описаний проводится администратором еженедельно. Регламент обновления антивирусного ПО определен в документах «Инструкция Ответственного специалиста по защите информации». Управление антивирусным ПО Kaspersky Business Space Security Russian Edition в АИС РИЦ осуществляется централизованно из Федерального информационного центра ФМБА России.

Для обеспечения работоспособности АИС РИЦ и сохранения защищаемых данных в АИС РИЦ предусмотрено резервное копирование и восстановления данных на системных разделах серверов с помощью программного комплекса Acronis Backup & Recovery 10 Server for Windows / Acronis Backup & Recovery 10 Advanced Server. Процедуры создания и восстановления образа системного диска определены в документе «Инструкция ответственному специалисту по защите информации». Образ системного диска обновляется ежемесячно и хранится на установленном «Инструкцией Ответственному специалисту по защите информации» dc0102 в каталоге d:\backup, так же допускается хранение образов на учтенных МНД (внешний жесткий диск) в сейфе у ответственного специалиста по защите информации. Резервирование системных разделов пользовательских АРМ производится посредством ПО «Aquarius System Recovery». Процедуры резервирования системного диска АРМ и серверов определены в документе «Инструкция Ответственного специалиста по защите информации».

Для обеспечения контроля целостности СЗИ в АИС РИЦ на АРМ и серверах устанавливается ПО «ФИКС». Для настройки средства контроля целостности ПО «ФИКС» должен быть выполнен вход на сервер под учетной записью Администратора и проведено контрольное суммирование (формирование эталонных контрольных сумм) директорий с установленными программными средствами защиты информации.

Для серверов АИС РИЦ должно быть проведено формирование эталонных контрольных сумм и последующий контроль целостности следующих каталогов (включая подкаталоги):

* C:\Program Files\Acronis
* C:\Program Files\Kaspersky Lab
* C:\Program Files\fix202

Для АРМ пользователей АИС РИЦ должно быть проведено формирование эталонных контрольных сумм и последующий контроль целостности следующих каталогов (включая подкаталоги), в случае их наличия:

* C:\Program Files\Kaspersky Lab\
* C:\Program Files\DeviceLock
* C:\Program Files\fix202

Для ноутбуков выездных бригад должно быть проведено формирование эталонных контрольных сумм и последующий контроль целостности следующих каталогов (включая подкаталоги), в случае их наличия:

* C:\Program Files\Kaspersky Lab\
* C:\Program Files\DeviceLock
* C:\Program Files\fix202
* C:\Program Files\Secret Disc

Контрольные суммы указанных каталогов хранятся на локальном диске «С» в директории (в случае отсутствия директория должна быть предварительно создана администратором) \fix202\.

Контрольное суммирование выполняется по алгоритму ГОСТ 34.11-94. После проведения обновления, либо внесение иных санкционированных изменений в контролируемые программные средства должно быть произведено повторное формирование эталонных контрольных сумм измененных средств. Сверка контрольных сумм контролируемого ПО должна осуществляться не реже чем раз в неделю.

Все помещения объекта информатизации АИС РИЦ расположены в пределах контролируемой зоны. Вскрытие помещений могут выполнять только сотрудники, указанные в документе «Список работников Государственного учреждения здравоохранения «Адыгейская республиканская станция переливания крови» имеющих право вскрывать помещение».

Для защиты информации от несанкционированного доступа используются встроенные средства защиты сертифицированных операционных систем Microsoft Windows XP Professional Service Pack 2, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition. Настройку встроенных СЗИ от НСД для идентификации и аутентификации пользователей, регистрации их действий, контроля целостности системных файлов, и файлов СрЗИ НСД, а также контроль работы встроенных СрЗИ НСД осуществляет Ответственный специалист по защите информации. Обязанности и порядок работы Ответственного специалиста по защите информации и пользователей (операторов) на средствах вычислительной техники АИС РИЦ регламентируется следующими документами: «Инструкция ответственному специалисту по защите информации», «Руководства оператора», «Инструкция пользователя».

Управление всем коммутационным оборудованием происходит удаленно из АС ФИЦ, если же необходимо, то ответственный специалист по ЗИ в АИС РИЦ может физически подключиться к коммутатору через порт управления. Всё коммутационное оборудование управляется централизованно. Если выходит из строя канал связи, то АИС РИЦ продолжает работу с донорами без связи с АС ФИЦ. Это режим работы АС РИЦ допускается в течение 60 суток, за это время канал необходимо восстановить.

В АИС РИЦ пользователи имеют полный доступ ко всем защищаемым ресурсам и техническим ресурсам АРМ, за исключением доступа к интерфейсу настройки и контроля доступа встроенных средств защиты информации операционной системы Microsoft Windows XP. Доступ пользователей домена к защищаемым ресурсам серверов АИС РИЦ определяется документом «Таблица разграничения доступа к защищаемым ресурсам».

Перечень средств обработки защищаемой информации, системного программного обеспечения представлен в табл. 2.1.

Таблица 2.1 Перечень средств обработки защищаемой информации, системного программного обеспечения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Наименование и тип технического средства | Заводской  Номер или номер лицензии | Сведения о сертификате | Место установки |
|  | Microsoft Windows XP Professional SP2 Russian | 2M5\_818883\_130407\_0314\_013871  2M5\_818883\_130407\_0314\_014106  2M5\_818883\_130407\_0314\_013614  2M5\_818883\_130407\_0314\_014011  2M5\_818883\_130407\_0314\_014309  2M5\_818883\_130407\_0314\_013543  2M5\_818883\_130407\_0314\_014065  2M5\_818883\_130407\_0314\_014008  2M5\_818883\_130407\_0314\_013699  2M5\_818883\_130407\_0314\_014108  2M5\_818883\_130407\_0314\_013639  2M5\_818883\_130407\_0314\_014286  2M5\_818883\_130407\_0314\_013635  2M5\_818883\_130407\_0314\_013904  2M5\_818883\_130407\_0314\_014022  2M5\_818883\_130407\_0314\_013556  2M5\_818883\_130407\_0314\_014157 | Сертификат соответствия ФСТЭК № 1636  Выдан 04.07.08  Действителен до 04.07.2011  В832114  B832344  B795182  B832249  B832499  A795253  B832303  B832246  B831955  B832346  A795119  B832476  A795115  B832081  B832260  A795240  B832401 | Все пользовательские ПЭВМ |
|  | Microsoft Windows XP Professional SP3 Russian | 2M5\_818883\_13407\_0314\_014258  2M5\_818883\_13407\_0314\_014238 | Сертификат соответствия ФСТЭК № 884/3  Выдан 3.12.08  Продлён до 3.12.2011  B831336  B831359 | oper  registratura |
|  | Windows XP Professional XP\_Check | --------- | --------- | --------- |

Ответственный специалист по защите информации АИС РИЦ имеет полный доступ ко всем ресурсам АИС РИЦ.

Операции входа пользователей в систему документируются средствами регистрации и учета операционной системы Microsoft Windows XP и Microsoft Windows Server 2003.

Для пользователей в качестве штатных средств доступа в АИС РИЦ предусмотрены:

* стандартные средства операционной системы Microsoft Windows XP Professional Service Pack 2 и Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition;
* интерфейс настройки и контроля функций встроенных средств защиты операционной системы Microsoft Windows XP Professional Service Pack 2 и Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition.

Как известно, сети подвержены атакам, которые можно условно разделить на внешние и внутренние. Если от внутренних атак локальная сеть Учреждения имеет должную защиту: firewall-ы, антивирусы, то от внешних атак этих средств будет недостаточно. Именно поэтому предлагается использовать в сети организации системы HoneyPot.

**Глава 3. Рекомендации по внедрению и эксплуатации HoneyPot**

## 3.1 Внедрение коммерческого низкоинтерактивного KFSensor Honeypot IDS

Для того чтобы обнаружить злоумышленников предлагается KFSensor. KFSensor – коммерческий низкоинтерактивный HoneyPot. Разработчики позиционируют свой продукт, как ПО, совмещающее в себе функции системы обнаружения вторжений(IDS), и, собственно, самого HoneyPot-а в одном флаконе. Он работает по классической для низкоинтерактивных HoneyPot схеме – администратору безопасности предоставляется набор сервисов, которые может реализовать программа. Программа имеет 77 преконфигурированных сервисов, из них 58 TCP и 19 UDP портов. Эти сервисы подразделяются на несколько групп. Она выступает в качестве приманки для привлечения и выявления хакеров, моделируя уязвимые системы услуг и троянов. Система легко конфигурируется и имеет подробное протоколирование, анализ атак и предупреждения системы безопасности. Этот подход дополняет другие формы обеспечения и добавляет еще одну защиту от растущей угрозы безопасности, с которыми сталкиваются все организации.

Каждый сервис имеет свой сценарий поведения, который определяет поведение системы при произведении подключения на соответствующий порт. Для разных служб этот сценарий может подразделяться на следующие типы:

* просто открытый сокет;
* баннер приветствия;
* набор поддерживаемых команд и ответов на них

эмуляция реального хост-соединения.

Целью исследования данной ловушки является анализ программных возможностей данного продукта, степень безопасности, которую он может обеспечить, исследование наиболее эффективных точек размещения приманок в сети, анализ средств сбора информации, имеющийся в наличии, типы атак, от которых внедрение данного типа HoneyPot поможет защититься.

Для установки такой системы будет достаточно одного компьютера, но при построении распределенных систем рекомендуется использовать дополнительный компьютер, на котором работает SysLog Server. KFSensor поддерживает механизм удаленного хранения данных об атаке в SysLog сервере, который представляет из себя специализированную базу данных, предназначенную для сбора информации с датчиков различных сетевых устройств и программ. Использование такой базы данных очень удобно, а в отдельных случаях даже необходимо с точки зрения безопасности хранения данных. Данные со скомпрометированного HoneyPot-а нельзя использовать для дальнейшего исследования, так как они могли быть подвергнуты модификации взломщиком.

При проводимом исследовании использовалась операционная система Microsoft Windows XP SP2 со всеми выпущенными на данный момент обновлениями. Приманка HoneyPot расположена на компьютере, имеющем два сетевых интерфейса: один подключен к локальной сети провайдера, а второй – к маршрутизатору с доступом в Интернет

При тестировании этого HoneyPot-а была создана конфигурация, в которую были включены все доступные для использования сервисы. Для реального использования такой подход, естественно, неприменим, так как для атакующего сразу будет понятно, что сервисы Linux и Windows, размещенные на одной машине, обязательно окажутся HoneyPot-ом. Но просто для исследовательских целей такой подход годится.

При старте программа запрашивает у операционной системы сокеты. Если сокет уже занят каким-либо другим сервисом, то для эмуляции эта служба будет недоступна. Ее можно перенести на другой свободный порт. В реальном применении необходимо использовать лишь несколько эмулируемых сервисов из всего многообразия предлагаемых служб. Кроме того, очень важно грамотно их сочетать. Нельзя смешивать сервисы разных ОС на одной машине. Гораздо лучше будет использовать в сети несколько машин с индивидуальным набором сервисов на каждой. Кроме того, не стоит «запускать» серверные сервисы на машинах, эмулирующих работу рабочих станции пользователя. Иначе, несоблюдение этих правил обязательно наведет злоумышленника на мысль о том что это ловушка.

В программе поддерживаются сценарии – это наборы задействованных эмулируемых сервисов. Для разных целей могут быть заданы различные сценарии. В каждый момент времени работать может только один сценарий.

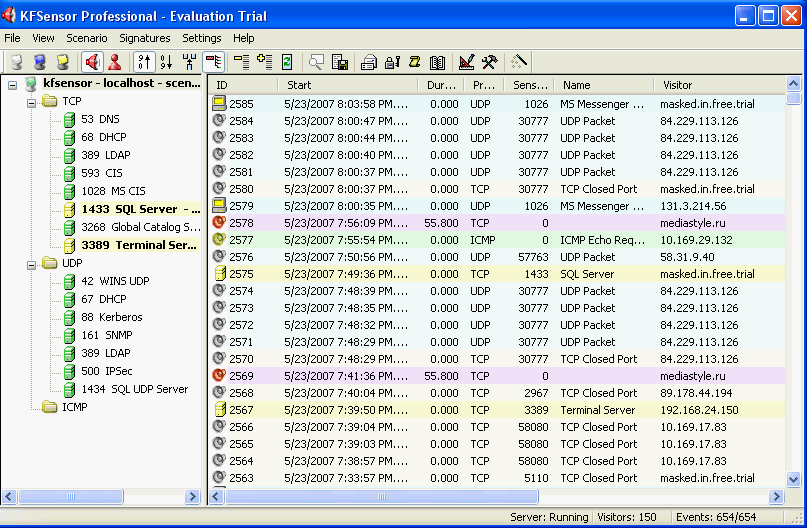
Конфигурирование KFSensor заключается в создании и настройке сценариев поведения.

Рисунок 3.1 KFSensor Professional

Для эмуляции работы различных компьютерных сред были созданы несколько различных сценариев. Каждому сценарию определяется набор используемых им сервисов. Сценарии были поделены на классы, определяющие эмулируемую программную среду. Таковыми сценариями стали: (рис 3.1).

На рисунке видны сервисы, которые эмулирует KFSensor HoneyPot. Таковыми сервисами являются DNS, DHCP, LDAP, MSSQL Server, SNMP, RDP Server и прочие.

Эта конфигурация реализует среднестатистический Windows Server. Отдельные сервисы можно добавлять или удалять, добиваясь недетерменированности системы, что снижает вероятность её разоблачения.

Аналогичным образом создаются прочие конфигурации, которые могут выдавать HoneyPot - это:

* рабочая станция Microsoft Windows;
* Linux;
* веб сервер, использующий Microsoft Internet Information Services;
* компьютер, зараженный вирусами.

На стадии сбора данных, необходимых для атаки использовались такие программные средства как Tenable Nessus и Positive Technologies Xspider. При обнаружении работающего компьютера производится опрос открытых портов, после чего на сервисы, расположенные за этими портами начинает производиться атака на доступ к ресурсам сервиса или взлом системы авторизации.

Проведение атаки заключалось в сканировании сети, некоторые узлы которой представляли HoneyPot ловушки с целью обнаружить наиболее привлекательные для взлома системы. Установленный HoneyPot сразу стал извещать о попытках подсоединения к наблюдаемым портам. Атаки, зафиксированные системой как правило делились на:

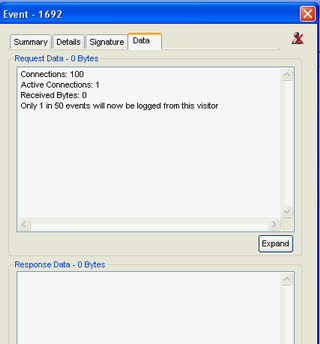
DoS атаки – за короткое время происходит установка большого количества сессий (рис. 3.2).

Рисунок 3.2 DoS атаки

Спам – HoneyPot выступал либо в виде промежуточного релея для пересылки SMTP сообщений, либо целевой системой для доставки спама через службу MS Messenger.

Атаки на системы авторизации сетевых служб – атаки в основном заключаются в грубом переборе паролей (bruteforce) (рис. 3.3).

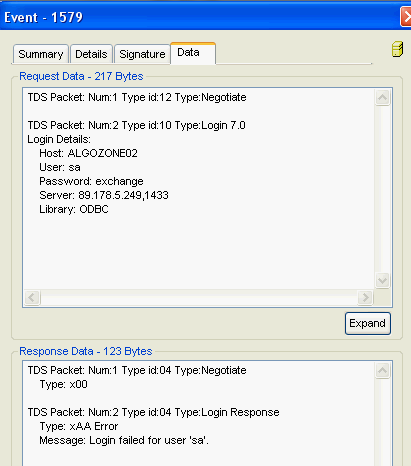


Рисунок 3.3 Bruteforce

KFSensor – HoneyPot, по большей части предназначенный для отвлечения злоумышленников. Одним из отличительных свойств является то что этот продукт умеет эмулировать очень большое количество сервисов. По этому параметру он явно отрывается вперед от своих конкурентов. Также, к преимуществам следует отнести то, что он разработан для запуска на операционной системе Microsoft Windows и обладает простым и наглядым графическим интерфейсом, позволяющим администратору легко конфигурировать ловушки, отслеживать происходящее с системой, задавать дополнительные конфигурационные параметры и многое другое. Несомненным плюсом следует считать то, что установка, настройка и запуск программы не составляют большого труда(в отличии от подавляющего большинства его конкурентов) и позволяют быстро разворачивать такие системы. Также важным свойством является наличие механизма удаленного протоколирования информации на Syslog сервер. Это делает систему масштабируемой в рамках предприятия и позволяет собирать информацию от приманок, находящихся в разных точках сети. Простота установки позволяет без труда развернуть эту систему на множестве станций в сети.

К его недостаткам можно отнести работу исключительно на прикладном уровне. В отличии от, например, HoneyD, который работает также и на сетевом уровне, KFSensor работает только на уровне приложений. Из этого следует, что сетевой отпечаток операционной системы(os fingerprint) не находится у него под контролем, и, как следствие, злоумышленник может определить тип реальной операционной системы. Количество информации им собираемой не всегда бывает достаточно для того чтобы определить все детали произошедшего нападения. Это происходит еще и потому, что KFSensor не собирает информацию сетевого уровня. Низкоинтерактивность программы очень затрудняет, а, зачастую и не позволяет использовать систему в исследовательских целях. Это происходит потому, что взаимодействие со взломщиком происходит по большей части именно по сценарию, заложенному в эмитируемый сервис, т.е, весь контакт с системой происходит на уровне запросов и ответов, которые заложены разработчиками. Также очень серьезным недостатком является сложность противодействия эмитируемых сервисов эвристическим средствам сетевых анализаторов. Из-за этого может произойти разоблачение HoneyPot-а. Кроме этого KFSensor не поддерживает виртуальных хостов и откликается только на один IP адрес – адрес того компьютера, на который он установлен. Также стоит обратить внимание на отсутствие Linux-версии программы и ее высокую стоимость.

## 3.2 Проект HoneyNet

Honeynet Project — это научная организация, занимающаяся исследованиями в области систем безопасности и специализирующаяся на изучении инструментария, используемого злоумышленниками, их тактики и мотивов. Затем полученная информация и сделанные выводы предлагаются для ознакомления всем желающим. В состав организации входят специалисты по вопросам безопасности из разных стран, которые на добровольной основе предоставляют свои ресурсы для развертывания и изучения сетей-приманок, основное назначение которых — стать объектом атаки хакеров. После каждого зарегистрированного инцидента собранная информация тщательно анализируется.

Проект был инициирован в 1999 году небольшой группой специалистов как неформальный список рассылки. Однако в скором времени стало понятно, что ни один специалист сам по себе не обладает всем опытом, необходимым для анализа собранных сведений об атаках. Ряды участников проекта постепенно расширялись, и в июне 2000 года он получил официальное название Honeynet Project.

Целью исследования является рассмотрение наиболее оптимальных технологий внедрения сетей HoneyNet, исследования их функциональных возможностей, способов противодействия хакерам, типу, количеству и качеству информации, им собираемой, а также способов развертывания таких систем с использованием технологий виртуальных машин.

Программный комплекс HoneyNet состоит из следующих обязательных составляющих (рис. 3.4.):

Roo HoneyWall(HoneyPot FireWall) – линукс-система, работающая в режиме моста для всех проходящих соединений(кроме eth2, который предназначен для подключения станции управления)

Станция управления системой HoneyNet – практически любая ОС, имеющая браузер, способный работать по протоколу SSL. Опционально, может содержать поддержку SSH соединений, например, клиент SSH в Linux, либо PuTTY в Windows. SSH соединения предназначены для поддержки терминальных подключений удаленного управления.

Системы HoneyPot – представляют собой обыкновенные компьютеры, с операционными системами типа Microsoft Windows либо GNU/Linux, поверх которых работает низкоуровневый драйвер Sebek, обеспечивающий перехват системной информации.

Также в исследовании проводится рассмотрение работы высокоинтеративных HoneyPot-ов на виртуальных машинах, а именно на платформах VMWare Server, Workstation, GSX.

HoneyNet – очень гибкое программное средство. Но одним из его серьезных недостатков является необходимость установки перед самими

HoneyPot-ами специального программного комплекса, предназначенного для управления сетью HoneyPot, сбора и анализа данных и фиксирования сетевых атак. Этот программный комплекс называется Roo HoneyWall и представляет собой дистрибутив ОС Linux Fedora Core 3. Далее приведена базовая топология развертывания системы HoneyNet (рис. 3.5.):

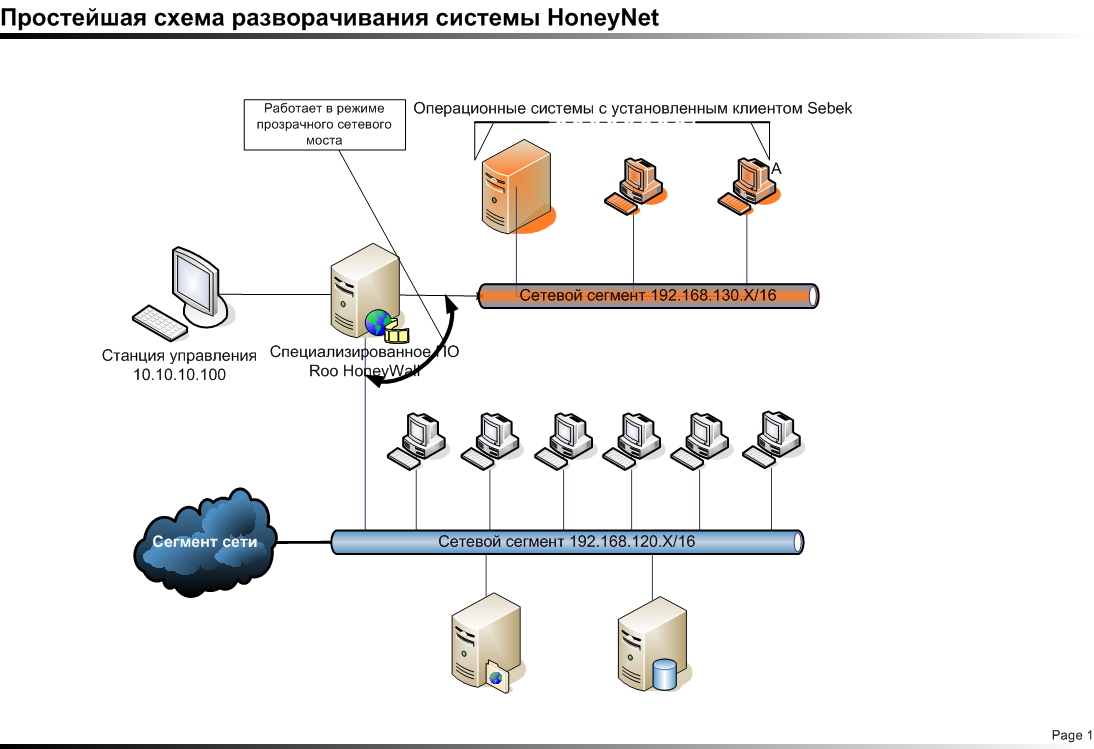
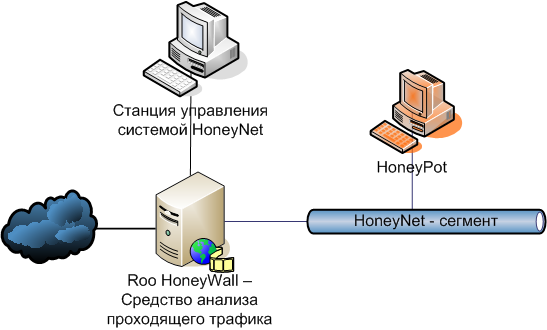


Рисунок 3.4 Программный комплекс HoneyNet

Рисунок 3.5 Базовая топология системы HoneyNet

Для системы HoneyNet отводится отдельный сегмент сети, который связан с обыкновенной сетью посредством компьютера, на котором установлен Roo HoneyWall. Специфика работы Roo HoneyWall заключается в том, что он работает в режиме прозрачного сетевого моста, что позволяет объеденять различные сетевые сегменты, а, точнее, наоборот их разделять – отделять HoneyPot сеть от обыкновенной сети и контролировать их по-отдельности. Это важное свойство позволяет вести контроль соединений устанавливаемых хакером при взломе систем, расположенных в этом сегменте. Таким образом существенно повышается безопасность такой ловушки в плане предотвращения осуществления атак с нее на внешние системы, например системы Интернета или критические сервера локальной сети.

Для своей работы Roo Honeywall должен иметь три сетевых интерфейса – два из них, eth0 и eth1 предназначены для связывания сегментов сети и работают в режиме моста, а третий, eth2, предназначен для подключения к административному сегменту сети, либо напрямую к компьютеру администратора системы HoneyNet. Выделение отдельного сегмента сети, по словам разработчиков, предназначено для повышения безопасности административных консольных соединений, отсутствия такого трафика в основных сегментах сети, использование адресации, отличной от общепринятой в данной сети. Кроме того, этот интерфейс также необходим еще и потому, что сам Roo HoneyWall работает в режиме прозрачного моста, поэтому иметь собственных соединений он не может.

В качестве систем-приманок такой сети выступают обыкновенные физические (либо виртуальные) компьютеры. В зависимости от типа внедряемой приманки (рабочая станция или сервер), на компьютер устанавливаются соответствующие операционные системы и программное обеспечение, предназначенное для работы такой системы в реальной жизни. Поддерживаемыми операционными системами являются Microsoft Windows XP, операционные системы семейства Linux и FreeBSD. После этого в систему устанавливается и настраивается драйвер Sebek, который отвечает за низкоуровневый перехват системных вызовов и сбора прочей информации, которая позже отсылается на Roo HoneyWall для последующего анализа. Для того чтобы остаться незамеченным, сетевой трафик, отправляемый клиентом Sebek, маскируется под широковещательный NetBIOS трафик.

При разработке конфигурации HoneyPot исследована возможность разворачивания HoneyNet на одном высокопроизводительном компьютере (рис 3.6). Был создан отдельный сетевой сегмент, в котором была развернута сеть приманок, эмулирующих работу обыкновенной производственной сети. Это необходимо для того, чтобы взломщик, попав в такую сеть был уверен, что находится в производственной сети, которую он и взламывал. Сеть-ловушка предназначена для того, чтобы отвлечь взломщика, дав ему уверенность в том, что он находится в реальной сети.

Для решения этой задачи использовались технологии виртуализации, а именно, VMWare Workstation v 5.5. VMWare Workstation использует виртуализацию уровня операционной системы. Это означает, что гипервизор устанавливается поверх основной операционной системы. В качестве основной операционной системы был выбран Microsoft Windows 2003 Server. Компьютер имеет два сетевых подключения, одно направлено в интернет, а другое – в корпоративную сеть Учреждения. На компьютер установлен программный фаирволл Kerio WinRoute Firewall v6.2.3.

Этот фаирволл имеет функцию прямой трансляции пакетов из локальной сети в интернет (NAT) и обратной трансляции пакетов из интернета в локальную сеть(Port Mapping). Первая функция позволяет использовать компьютер для обеспечения общего выхода в интернет. Вторая функция позволит осуществлять переадресацию пакетов, пришедших на шлюз на любой другой компьютер локальной сети. Причем, можно осуществлять трансляцию двумя способами: либо транслируя все пакеты на один компьютер, либо транслируя на различные компьютеры в зависимости от портов назначения в приходящих пакетах.

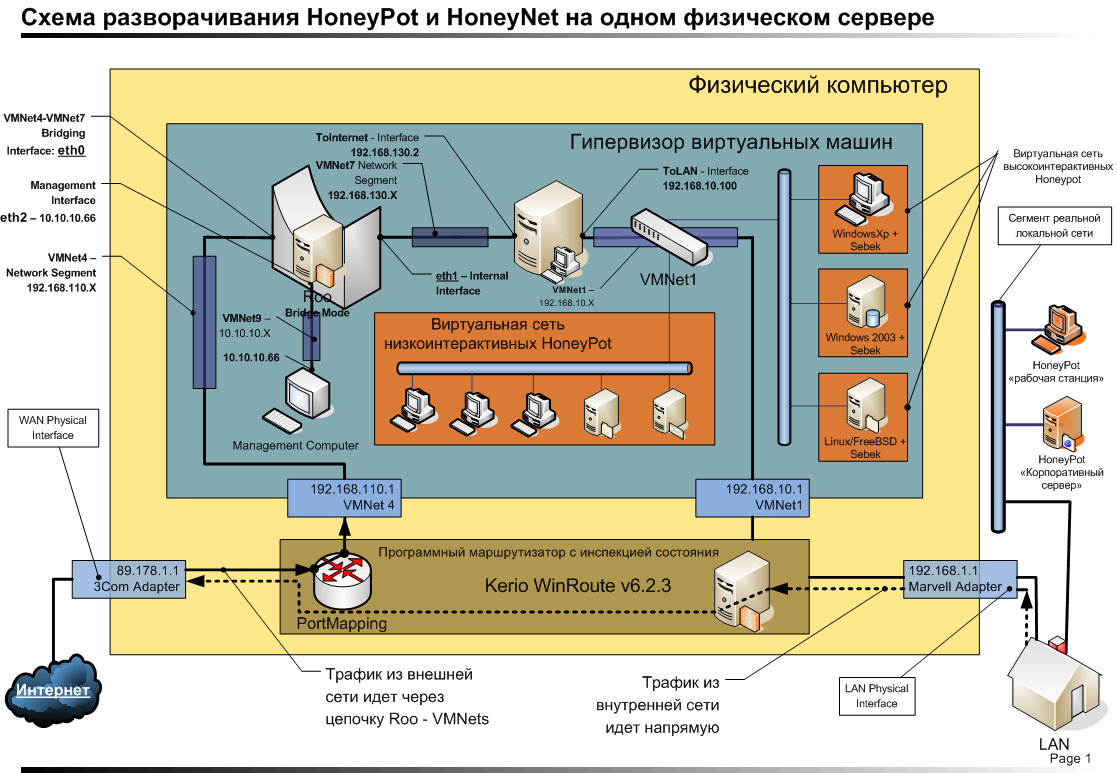


Рисунок 3.6 Схема разворачивания HoneyPot и HoneyNet на одном компьютере

В данной схеме будет использоваться метод полной обратной трансляции. Для создания отвлекающей сети была создана следующая конфигурация. Сеть-приманка состоит из Roo HoneyWall, из фаирволла-ловушки с также установленным Microsoft Windows 2003 Server и Kerio WinRoute Firewall v.6.2.3. Фаирволл-ловушка играет роль обыкновенного корпоративного фаирволла, имеющего функцию шлюза общего доступа. Он имеет два сетевых интерфейса, один из которых связан с Интернетом, посредством прямой трансляции NAT через физический компьютер, а второй – в виртуальную локальную сеть, которая состоит из высокоинтерактивных и низкоинтерактивных ловушек.

На фаирволл-ловушку будут транслироваться ВСЕ пакеты, приходящие из Интернета. Это сделано для того, чтобы при сканировании сети снаружи, сканировался не реальный, а именно виртуальный компьютер, играющий роль приманки, которая предназначена для взлома. По сценарию, при попытке взлома, злоумышленник проникает на подставной фаирволл, и задействует какую-либо уязвимость. После этого он получает доступ в локальную сеть и имеет прямую связь с компьютерами сети. Теперь взломщик имеет возможность атаковать сервера и компьютеры локальной сети (которые, разумеется, также являются системами HoneyPot).

Вся сеть является полностью контролируемой. Все виртуальные машины выполняются на одном физическом компьютере. При необходимости отдельные компьютеры можно останавливать и запускать. Таким образом, можно реализовать практически любую сетевую инфраструктуру.

Применение такой системы может резко повысить безопасность сети от внешних вторжений, переадресовывая все входящие соединения на сеть ловушек. Кроме того, с ее помощью можно достаточно детально наблюдать за всеми действиями злоумышленника в этой сети. Реализованная конфигурация отделяет реальную сеть от виртуальной, поэтому проникновение взломщика из виртуальной сети в реальную практически невозможно.

Roo HoneyWall представляет из себя законченную самодостаточную систему. Это дистрибутив, основанный на ОС FedoraCore 3, в котором оставлены только необходимые дистрибутивы. Roo HoneyWall имеет встроенный веб-интерфейс, предназначенный для администрирования системы и отслеживания атаки.

При умелом использовании этот программный комплекс – действительно необходимый инструмент в руках специалиста по информационной безопасности.

### 3.3 Создание отвлекающей сети HoneyPot – ловушек

В ходе исследования работы систем HoneyPot предлагается новая топология развертывания и использования таких систем. Идея заключается в том, чтобы параллельно обыкновенной корпоративной сети развернуть похожую сеть HoneyPot приманок, как низкоинтерактивных, так и высокоинтерактивных типов. Основные задачи, решаемые такой системой:

1. Отвлечение злоумышленника на подставные компьютеры.
2. Исследование приемов, тактик и инструментов, используемых злоумышлнником
3. Задерживание распространения сетевых червей из Интернета

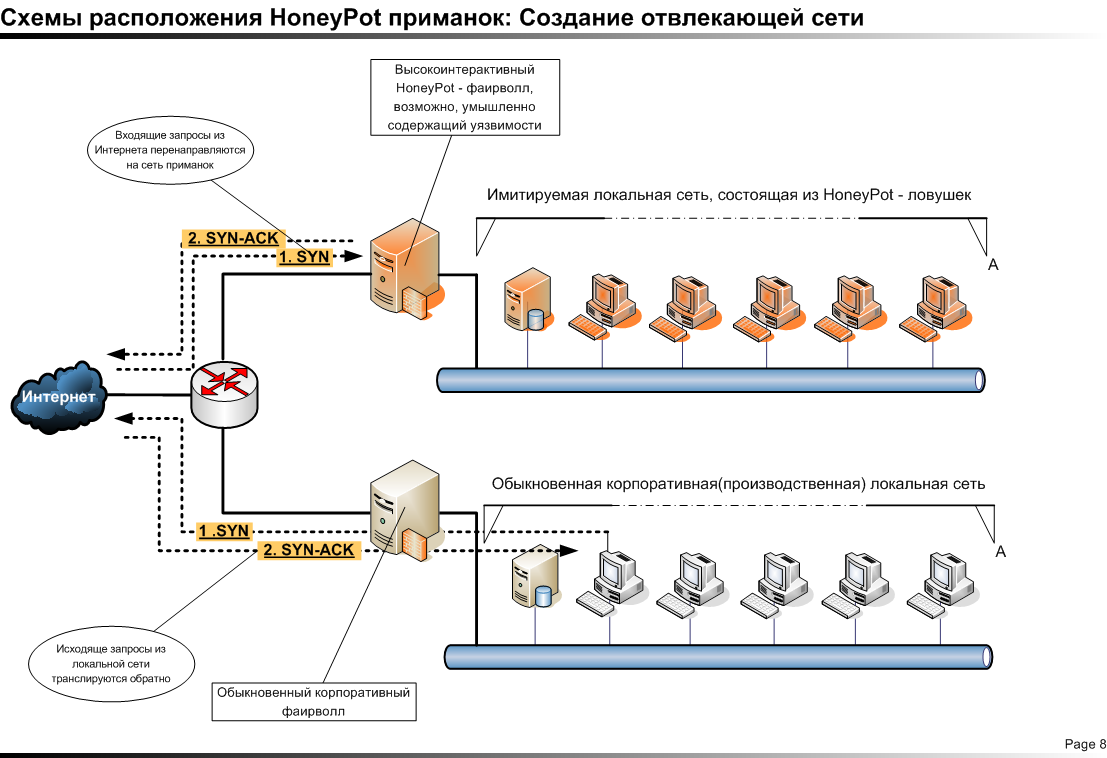
Топология такой сети выглядит так (рис. 3.7):

Рисунок 3.7 Схема отвлекающей сети

Ключевым моментом работы такой системы является наличие маршрутизатора, обладающего функцией внутренней трансляции портов (destination port mapping). Такой механизм позволит соединения, устанавливаемые из Интернета перебрасывать на виртуальную HoneyPot – сеть, а соединения, устанавливаемые из локальной сети нормальным образом транслировать в исходящие соединения с помощью механизма NAT.

При сканировании такой сети из Интернета, производственная сеть с ее firewall-ом будет скрыта от хакера, но взамен он увидит подставной firewall, который он наверняка попробует атаковать. Такой фаирволл можно умышленно сделать уязвимым для того чтобы у хакера возникло желание его взломать. После того как он его взломает, он окажется в локальной сети, которая также состоит из сетей приманок.

Проведенное в главе исследование работы HoneyPot-систем в сети Учреждения**,** показало, как работают различные типы ловушек, различные программные продукты, разные способы внедрения и размещения ловушек, точки сетей, где они применяться. Кроме того, были проведены атаки на сети организации, где эти ловушки были размещены и проведен анализ действий HoneyPot при этих атаках.

# Заключение

В ходе написания работы была рассмотрена система HoneyPot , как и любой программный продукт, предназначенный для обеспечения информационной безопасности, система HoneyPot не может использоваться сама по себе. Внедрение в инфраструктуру сети подразумевает ее совместное использование с прочими средствами защиты: брандмауэрами, антивирусным ПО, системами IDS, системами обновления ПО, и прочими программами, предназначенными для повышения безопасности сетевой инфраструктуры. В дополнении к вышеперечисленным средствам, HoneyPot может оказаться новой по технологии и принципу работы системой, что может означать существенное повышение вероятности обнаружение попытки взлома или успешного проникновения.

Обосновано, что исследовательские системы HoneyPot позволяют собрать множество важной и полезной информации о тактике действий и инструментах злоумышленников. Не раз случалось так, что система HoneyPot позволяла «рассказать» о новых уязвимостях в системах безопасности информационных систем, принимая на себя удар взломщика, а позже запротоколировав весь ход атаки. Не раз случалось и так, что злоумышленник, «взломав» HoneyPot, атаковал другие системы, используя ранее неизвестные эксплойты. На HoneyPot попадали исходные коды этих эксплойтов, которые позднее могли быть обследованы как администратором безопасности, так и направлены в компании, где разрабатывалось ПО, против которого предпринималась попытка взлома. Таким образом, ловушки позволяют обнаружить так называемые приватные 0-day эксплойты, представляющие огромную ценность как для хакера, так и для разработчиков ПО, против которого эксплойт предназначен.

В работе была предложена схема организации защиты периметра локальной сети Учреждения от внешних вторжений путем трансляции всех входящих запросов в сеть ловушек. Такая технология позволит заранее предупредить о проходящей атаке, а также отвлечь внимание злоумышленника от реальной производственной сети. При грамотном подходе к разворачиванию описанной схемы, злоумышленнику будет очень непросто понять, что он находится в ловушке, особенно если он не предпринимает специальных мер для попыток определения фиктивности системы. Также с помощью технологий виртуализации было продемонстрировано, что предложенная схема может быть развернута всего лишь на одном физическом компьютере, при учете того, что одновременно параллельно будет работать около 5 виртуальных машин, образующих сеть-ловушку, «защищенную» брандмауэром-ловушкой.

Показано, что системы HoneyPot имеют серьезный потенциал в плане повышения совокупной защищенности информационной системы. При грамотном внедрении в локальной сети Государственного бюджетного учреждения здравоохранения Республики Адыгея «Адыгейская республиканская станция переливания крови» будет способствовать защите от внешних атак путем перенаправления атакующих в сеть приманок

Применение такой системы может резко повысить безопасность сети от внешних вторжений, переадресовывая все входящие соединения на сеть ловушек. Кроме того, с ее помощью можно достаточно детально наблюдать за всеми действиями злоумышленника в этой сети. Реализованная конфигурация отделяет реальную сеть от виртуальной, поэтому проникновение взломщика из виртуальной сети в реальную практически невозможно.

* **Список источников и использованной литературы**

1. **Источники**
2. «Доктрина информационной безопасности РФ», утв. Указом Президентом РФ 05.12 2016 г., № - 646.
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4. Федеральный закон от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне" с изменениями и дополнениями от 12 марта 2014 г.
5. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" с изменениями и дополнениями от 23 июля 2013 г. N 205-ФЗ.
6. **Литература**
7. Эрик Коул. Руководство по защите от хакеров. Издательский дом «Вильямс», 2002 – 640 с.
8. М. Руссинович, Д. Соломон. Внутреннее устройство Microsoft Windows:Windows Server 2003, Windows XP и Windows 2000. Мастер-класс.СПб.:, Питер, 2006. - 992 стр.
9. Локальные сети: архитектура, алгоритмы, проектирование. Новиков Ю. В. и др., изд-во ЭКОМ, 2000 г.
10. Олифер В.Г. Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 1999 – 672с.
11. В.Мельников. ”Защита информации в компьютерных системах”. Москва. ”Финансы и статистика”. ”Электроинформ”. 1997.
12. А.Юдин. ”Концепции и руководство по планированию Microsoft Windows NT Server”.
13. Б.Нанс. “Компьютерные сети”. Москва. Бином. 1996.
14. Г.Дейтел. “Введение в операционные системы”. Т.2. Москва. Мир. 1987.
15. Кульгин М. «Технология корпоративных сетей. Энциклопедия». СПб, Питер, 2001
16. Новиков Ю. «Локальные сети: архитектура, алгоритмы, проектирование». Москва, ЭКОМ, 2000
17. Информационная безопасность [текст]. – М.: Новый Юрист, 1998.-350 с.
18. Торокин А. А. Инженерно-техническая защита информации [текст]. — М.: Гелиос АРВ, 2005.
19. Гостехкомиссия России. «Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения», - Москва, 1992.
20. П.Зегжда, «Теория и практика. Обеспечение информационной безопасности». - Москва, 1996.
21. Л.Хофман, «Современные методы защиты информации», - Москва, 1995.
22. Ярочкин В.И. Безопасность информационных систем [текст]. – М.: “Ось-89”, 1996. С. 239.
23. В.Галатенко, Информационная безопасность, «Открытые системы», № 1, 1996.
24. Алексенцев А. И. Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. - 2000. — № 3.— С. 79-84.
25. АлексенцевА. И. О классификации конфиденциальной информации по видам тайны // Безопасность информационных технологий. — 1999.—№3.—С. 65-71.
26. Ашимхин А. В., Рембовский А. М. Выявление технических кана-  
    лов утечки информации: методы, структура и характеристики  
    средств // Специальная техника, специальный выпуск. — 2002.—С.42-48.
27. Федоткин С., Бураев Ю. Сборник материалов по основам организации охранной деятельности. — М., 1996.
28. Руководство по организации защиты информации коммерческой тайны. Ч. 1, 2,3. — М.: Минатомпром СССР, 1991.
29. Андрианов В. И., Соколов А. В. Устройства для защиты объектов информатизации: Справочное пособие [текст]. C.120 — М.: АСТ; СПб.: Полигон. -2000.
30. Арлащенков Ю. П., Ковалев М. С., Котов Н. Н; Тюрин Е. П. Применение технических средств в борьбе с терроризмом [текст]. — М.: НИЦ «Охрана» ГУВО МВД России, 2000
31. Барсукова. С., Дворянкин С. В., Шеремет И. А. Безопасность связи в каналах телекоммуникаций. Серия «Технология электронных  
    коммуникаций» [текст]. — М.: НИФ «Электронные знания», СП «Эко-Трендз», 1992. Т. 20.
32. Гарсии А.М*.* Проектирование и оценка систем физической защиты.  
    Пер. с англ. [текст]. — М.: АСТ, 2002.
33. Гавриш В. Практическое пособие по защите коммерческой тайны. — Сим¬ферополь: Таврия, 1994
34. Герасименко В.А., Гришаев С.П., Павлов Д.В. и др. Основы защиты коммерческой информации и интеллектуальной собственности. М.: Научно-информационная внедренческая фирма «ЮНИС», 1991.
35. **Электронные ресурсы**
36. [http://ghh.sourceforge.net](http://ghh.sourceforge.net/)
37. [http://honeypots.sourceforge.net](http://www.securitylab.ru/bitrix/exturl.php?goto=http%3A%2F%2Fhoneypots.sourceforge.net%2F).

# ПРИЛОЖЕНИЯ