Государственное бюджетное профессиональное образовательное учреждение
Псковской области
«Псковский агротехнический колледж»

Допущен к защите
Заведующий экономическим отделением
ГБПОУ ПО
«Псковский агротехнический колледж»

_____О.Б. Борисенко

« ___» _____20___г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(дипломная работа)

Тема:

_____

_____

Выполнил (а) студент(ка) группы № _____ _____ _____
Подпись Ф. И. О.

Руководитель работы _____ _____
Подпись Ф. И. О.

Нормоконтролер _____ _____
Подпись Ф. И. О.

Рецензент _____ _____
Подпись Ф. И. О.

Выпускная квалификационная работа защищена

«____» _____ 2018 г. Оценка
_____

2018

Государственное бюджетное профессиональное образовательное учреждение
Псковской области
«Псковский агротехнический колледж»

ЗАДАНИЕ

на выполнение выпускной квалификационной работы

Форма ВКР Дипломная работа

Ф.И.О. студента _____

Специальность _____ _____
Код специальности Название специальности

_____

1. Тема ВКР_____

_____

Приказ об утверждении № _____ от «____» _____ 20____ г.

2. Срок сдачи студентом законченной работы «___» _____ 20____ г.

3. Исходные данные по ВКР_____
_____
_____
_____
_____

4. Содержание ВКР (перечень подлежащих разработке вопросов) _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Руководитель_____
Ф.И.О., должность, ученая степень, звание, категория

_____

Дата выдачи задания «___» _____ 20____ г.

Задание принял к исполнению _____

Содержание

Введение

Тема данной дипломной работы «

решаемые

безопасности

по

режима

на

ГБУСО

психоневрологического

».

информационной

– одна

важнейших

любого

работающего

информацией,

которой

повредить

деятельности.

в

работе

то,

каждый

понимает

защиты

но

практике

малая

из

действительно

себе

последствия

методы

предотвращения.

сознании

людей

о

угрозе

в

из

фильмов

телесериалов

«хакерах».

практике

работа

обеспечению

безопасности

учитывать

факторов,

с

конкретным

объектом.

каждым

скорость

новых

открытий

растет,

в

информационных

Появляются

технологии

информации,

хранения,

благодаря

растут

вычислительные

которые

направить

преодоление

самых

систем

Развитие

волн,

чувствительности

фиксирующего

волны,

порождает

более

методы

информации,

не

непосредственного

к

жертвы.

Информационная

состоит

множества

и

мер,

в

позволяют

необходимого

безопасности.

даже

система

достаточно

но

отдельных

узлах

сбои,

как

мощность

средств

пренебрежение

безопасности

то

ее

может

напрасной.

дипломной работы

– изучить

службы

на

по

режима

на

ГБУСО

психоневрологического

».

Объект

задачи

службой

«Первомайского

интерната»

Предметом

исследования

служба

на

Для

цели

выполнены

задачи:

-

имеющуюся

по

теме;

-

структуру

принцип

службы

на примере предприятия «ГБУСО «Первомайский психоневрологический о интернат»

- Исследовать

службы

на

ГБУСО

психоневрологического

».

-Предложить

совершенствования

обеспечению

безопасности

«Первомайского

интерната

1.Основные понятия службы безопасности предприятия

1.1 Понятия службы безопасности

Служба

(СБ)

самостоятельной

единицей,

непосредственно

предприятия.

структура

системой

имеющая

вертикаль,

для

обеспечения

где

определенность,

границы,

отношений

всех

– от

сотрудника

менеджеров

звена.

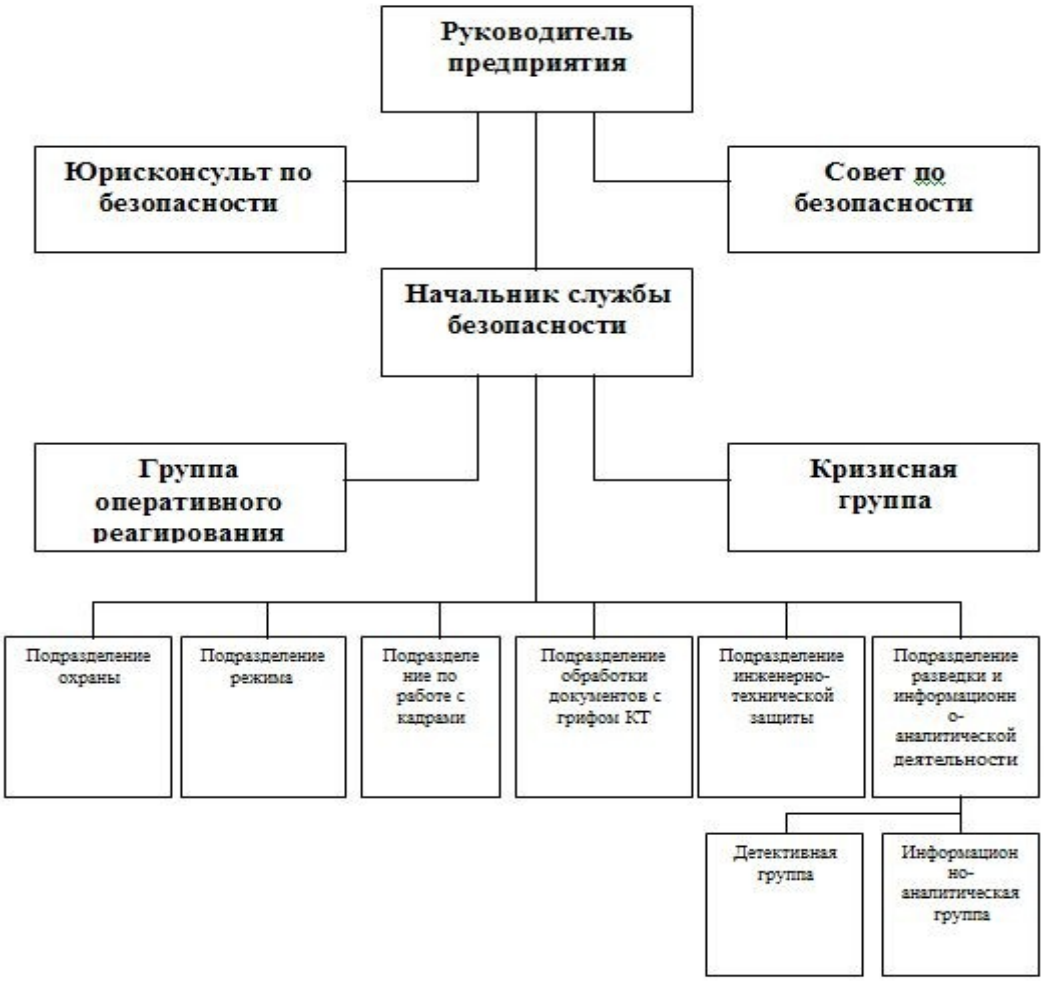


Рис.1.1 Схема структуры службы безопасности организации .

показывает

только

предприятиях,

проблемы

находятся

постоянным

руководителя

достигаются

высокие

Возглавляет

безопасности

службы

должности

руководителя

по

При

руководитель

должен

максимально

кругом

позволяющим

влиять

другие

и

области

предприятия,

этого

интересы

Основными

службы

предприятия

1. обеспечение

производственно-торговой

и

информации

сведений,

коммерческой

2. организация

по

организационной

инженерно-технической

аппаратной,

и

защите

тайны;

3.

специального

исключающего

получение

являющихся

тайной;

4.

необоснованного

и

к

и

составляющим

тайну;

5.

и

возможных

утечки

информации

процессе

производственной

и

экстремальных

пожарных

др.)

6. обеспечение

безопасности

проведении

видов

включая

встречи,

совещания,

связанные

деловым

как

национальном,

и

международном

7. обеспечение

зданий,

оборудования,

и

средств

производственной

8. обеспечение

безопасности

и

сотрудников

специалистов;

9.

маркетинговых

и

действий

и

Служба

предприятия

следующие

функции:

1.

и

пропускной

внутриобъектовый

в

и

порядок

службы

контролирует

требований

сотрудниками,

партнерами

посетителями;

2.

работами

правовому

организационному

отношений

защите

тайны;

3.

в

основополагающих

с

закрепления

них

обеспечения

и

коммерческой

в

Устава,

договора,

внутреннего

распорядка,

о

а

трудовых

соглашений,

должностных

и

руководства,

рабочих

служащих;

4.

и

совместно

другими

мероприятия

обеспечению

с

содержащими

являющиеся

тайной,

всех

работ

и

выполнение

«инструкций

защите

тайны»;

5.

все

коммерческой,

финансовой

другой

для

и

возможных

утечки

информации,

учет

анализ

режима

накапливает

анализирует

о

устремлениях

и

организаций,

деятельности

и

клиентов,

смежников;

6.

и

служебные

по

разглашения

утрат

и

нарушений

предприятия;

ведет,

и

«Перечень

составляющих

тайну»

другие

акты,

порядок

безопасности

защиты

7. обеспечивает

выполнение

нормативных

по

коммерческой

8. осуществляет

службами

подразделениями

подведомственных

организаций,

и

в

оговоренных

договорах

по

коммерческой

9. организует

регулярно

учебу

предприятия

службы

по

направлениям

коммерческой

добиваясь,

к

коммерческих

был

подход;

10.

учет

металлических

специальных

и

помещений,

которых

постоянное

временное

конфиденциальных

11. ведет

выделенных

конфиденциальной

помещений,

средств

них,

потенциальными

утечки

12.поддерживает

c

органами

службами

соседних

в

изучения

обстановки

районе

1.2 Сущность и задачи защиты информации на предприятии

Правовой

системы

защиты

на

основывается

нормах

права

предполагает

закрепление

фирмы

государства

поводу

использования

защиты

фирмы

персонала

поводу

персонала

установленные

защитного

ответственности

за

порядка

информации.

элемент

1. наличие

организационных

фирмы,

внутреннего

распорядка,

договорах,

должностных

положений

обязательств

защите

информации;

2.

и

до

всех

положения

правовой

за

конфиденциальной

несанкционированное

или

документов;

3.

лицам,

на

положения

добровольности

ими

себя

связанных

выполнением

по

информации.

числе

подсистем

информации

правовом

можно

1.установление

объекте

конфиденциальности;

2.

доступа

информации;

3.

обеспечение

защиты

4.четкое

конфиденциальной

как

объекта

Опираясь

государственные

акты

уровне

предприятия

организации),

собственные

правовые

ориентированные

обеспечение

безопасности.

таким

относятся:

1.

Информационной

2.Положение

коммерческой

3. Положение

защите

данных;

4.

сведений,

конфиденциальную

5. Инструкция

порядке

сотрудников

сведениям,

конфиденциальную

6.Положение

специальном

и

Обязательство

о

конфиденциальной

Памятка

о

коммерческой

Указанные

акты

на

случаев

оглашения

секретов

правовой

и

случае

нарушения

приниматься

меры

Обеспечение

безопасности

одним

необходимых

ведения

в

агрессивной

экономики.

мере

организации

ее

система,

задачей

является

максимальной

ведения

в

меняющихся

конкуренции

рынке.

Рассматривая

информацию

товар,

сказать,

информационная

в

может

к

экономии

в

время

ущерб,

ей,

к

затратам.

раскрытие

изготовления

продукта

к

аналогичного

но

другого

и

следствие

информационной

владелец

а

быть

автор,

часть

и

С

стороны,

является

управления,

ее

может

к

последствиям

объекте

Информационная

как

защита

задача

направленная

обеспечение

реализуемая

системы

Проблема

информации

многоплановой

комплексной

охватывает

важных

Проблемы

безопасности

усугубляются

проникновения

все

общества

средств

и

данных

прежде

вычислительных

На

день

три

принципа,

должна

информационная

- целостность

– защита

сбоев,

к

информации,

также

от

создания

уничтожения

- конфиденциальность

- доступность

для

авторизованных

Широкое

компьютерных

в

системах

информации

управления

к

проблемы

информации,

в

системах,

несанкционированного

Защита

в

системах

рядом

особенностей,

с

что

не

жёстко

с

может

и

копироваться

передаваться

каналам

Известно

большое

угроз

которые

быть

как

стороны

нарушителей,

и

стороны

нарушителей.

области

информации

компьютерной

в

наиболее

являются

группы

:

1. нарушение

информации;

2.

целостности

3. нарушение

информационно-вычислительных

Защита

превращается

важнейшую

государственной

когда

идет

государственной,

военной,

медицинской,

и

доверительной,

информации.

массивы

информации

в

архивах,

в

системах

передаются

телекоммуникационным

Основные

этой

- конфиденциальность

целостность,

поддерживаться

юридически,

также

технических

программных

Конфиденциальность

(от

confidentia -

предполагает

определенных

на

лиц,

доступ

данной

Степень

выражается

установленной

(особая

совершенно

секретно,

служебного

не

печати

т.п.),

субъективно

владельцем

в

от

сведений,

не

огласке,

ограниченному

лиц,

секретом.

установленная

конфиденциальности

должна

при

обработке

информационных

и

передаче

телекоммуникационным

Другим

свойством

является

целостность

Информация

если

в

момент

правильно

отражает

предметную

Целостность

в

системах

своевременным

в

достоверной

информации,

истинности

защитой

искажений

разрушения

Несанкционированный

к

лиц,

допущенных

ней,

или

ошибки

пользователей

программ,

изменения

вследствие

оборудования

к

этих

свойств

и

ее

и

опасной.

использование

привести

материальному

моральному

поэтому

системы

информации,

актуальной

Под

информации

защищенность

от

ее

(нарушения

искажения

целостности),

или

степени

информации,

также

ее

Безопасность

в

системе

телекоммуникационной

обеспечивается

этой

сохранять

информации

ее

выводе,

обработке

хранении,

также

ее

хищению

искажению.

информации

путем

допуска

ней,

ее

перехвата,

и

ложной

С

целью

физические,

аппаратные,

и

средства

Последние

центральное

в

обеспечения

информации

информационных

и

сетях.

обеспечения

:

1.защита

в

связи

базах

криптографическими

2. подтверждение

объектов

и

(аутентификация

устанавливающих

3. обнаружение

целостности

данных;

4.

защиты

средств

помещений,

которых

обработка

информации,

утечки

побочным

и

возможно

в

электронных

съема

5. обеспечение

программных

и

вычислительной

от

в

программных

и

6. защита

несанкционированных

по

связи

лиц,

допущенных

средствам

но

цели

секретной

и

работы

пунктов;

7.

мероприятия,

на

сохранности

да

Защитой информации на предприятии занимается отдел по защите информации.

Отдел по защите информации, являясь самостоятельным структурным подразделением предприятия, создается и ликвидируется приказом руководителя предприятиия . Отдел непосредственно подчиняется руководителю организации .

1.3 Анализ возможных внешних угроз безопасности информации на предприятие

Внешние угрозы это негативные факторы, воздействующие на то или иное предприятия извне, т.е. без вовлечения внутренних ресурсов. Внешние угрозы традиционно являются одними из наиболее важных к рассмотрению при формировании стратегии обеспечения безопасности предприятия.

Под

информации

условия

обработки

передачи

при

обеспечивается

защита

угроз,

изменения

хищения[1 с 45].

обеспечение

безопасности,

всего,

носить

характер.

она

на

анализе

всевозможных

В

очередь

инцидентов

рассматривает

идентификацию

распространенных

угроз,

и

способствующие

проявлению,

следствие

определение

угроз

безопасности.

угрозой

понимать

потенциальное

или

процесс

тем

явление,

может

к

ущерба

интересам.

ходе

необходимо

удостовериться,

все

источники

будут

И

с

угроз

возможные

свойственные

защиты,

и

источникам

также

факторам

угрозы

информации.

от

принципа,

и

источников

и

их

целесообразно

на

взаимодействия

цепочки:

угроз →

(уязвимость) →

(действия) →

(атака)

этим

будем

Источник

– это

антропогенные,

и

угрозы

.

Угроза

- это

опасность

или

существующая)

какого

деяния

или

направленного

объекта

(информационных

настоящего

собственнику,

или

проявляющего

опасности

и

информации.[12 с 123].

(уязвимость) -

присуще

информации

приводящие

нарушению

информации

конкретном

и

недостатками

функционирования

информации,

архитектуры

систем,

обмена

интерфейсами,

программным

и

платформой,

эксплуатации.[18].

(атака) -

возможное

реализации

(возможных

при

источника

через

факторы

Как

из

атака-

всегда

реализация

и

к

при

анализ

располагает

анализа

ущерба

выбора

отражения

информации

безопасности

не

уж

много.

как

из

это

причина

то

в

определении

жесткая

технических

с

категорией,

является

Ущерб

считать

как

угрозы

информации.

возможного

могут

различны

1.

и

ущерб

репутации.

2.

физический

материальный

связанный

разглашением

данных

лиц

3

(финансовый)

от

защищаемой

информации

4.

(финансовый)

от

восстановления

защищаемых

ресурсов

5.

ущерб

от

выполнение

на

обязательств

третьей

6. Моральный

материальный

от

деятельности

7.Материальный

моральный

от

международных

Ущерб

быть

каким-либо

И

ЭТОМ

имеется

лицо

а

явиться

независящим

субъекта

(например,

случаев

иных

таких

проявления

свойств

В

случае

вина

которая

причиненный

как

преступления,

по

умыслу

то

деяние

с

или

умыслом)

по

(деяние,

по

небрежности,

результате

причинения

и

ущерб

квалифицироваться

состав

оговоренный

правом.

втором

ущерб

вероятностный

и

быть

как

с

риском,

оговаривается

административным

арбитражным

как

рассмотрения.

теории

под

понимается

для

имущественные

начавшиеся

итоге

Ущерб

в

имущества,

в

дохода,

был

получен

отсутствии

(упущенная

При

в

субъекта,

ущерб

личность,

"ущерб"

только

том

когда

доказать,

он

то

деяния

необходимо

в

правовых

как

преступления.

при

угроз

информации

этом

целесообразно

требования

уголовного

определяющего

преступления.

некоторые

составов

определяемых

Кодексом

Федерации.

– совершенные

корыстной

противоправные

изъятие

(или)

чужого

в

виновного

других

причинившее

собственнику

владельцу

.[24с 111].

Копирование

информации –

и

запечатление

на

или

носителе.[16 с 48].

– внешнее

на

в

которого

прекращает

физическое

либо

в

непригодность

использования

целевому

Уничтоженное

не

быть

путем

или

и

выводится

хозяйственного

.[23].

Уничтожение

информации –

ее

памяти

Повреждение –

свойств

при

существенно

его

утрачивается

часть

полезных

и

становится

или

непригодным

целевого

Модификация

информации –

любых

кроме

с

программы

ЭВМ

баз

.

Блокирование

информации –

затруднение

пользователей

информации,

связанное

ее

.

Несанкционированное

блокирование

копирование

– любые

разрешенные

собственником

компетентным

указанные

с

.

Обман

подлинности,

ложной

– умышленное

или

истины

целью

в

лицо,

ведении

находится

и

образом

от

добровольной

имущества,

также

с

целью

ложных

.[17c 85]

Однако

о

умысле

в

информации

результате

бедствий

приходится,

и

факт,

вряд

стихия

воспользоваться

информацией

извлечения

выгоды.

и

том

в

случае

информации

ущерб.

правомочно

категории

вреда

При

речь

не

уголовной

за

или

чужого

а

случаях

под

право

части

причиненного

(риск

гибели

– то

риск

нанесения

в

с

или

имущества

причинам,

зависящим

субъектов).

общему

в

случае

в

с

или

имущества

собственник,

гражданское

предусматривает

другие

компенсации

ущерба.

анализе

качестве

нанесшего

какое-либо

или

явление,

ущербом

понимать

для

имущественные

вызванные

явлениями

которые

быть

за

средств

стороны

рисков

события)

за

собственных

собственника

Например,

представляет

отношения

защите

интересов

и

лиц

наступлении

событий

случаев)

счет

фондов,

из

ими

взносов.

страхования

быть

противоречащие

Российской

имущественные

связанные

возмещением

причиненного

вреда

или

физического

а

вреда,

юридическому

[27с 78].

Обобщая

можно

что

безопасности

являются:

1.

(копирование)

2. уничтожение

3. модификация

информации;

4.

доступности

информации;

5.

подлинности

6.навязывание

информации.

1.4 Источники угроз безопасности информации

В

качестве

угроз

выступать

субъекты

так

проявления

Причем

угроз

находиться

внутри

системы –

источник,

и

нее

источник.

на

и

источники

потому

для

и

же

методы

для

и

источников

быть

Но

свое

остановим

внешних

угроз,

на

что

меньше

изучены.

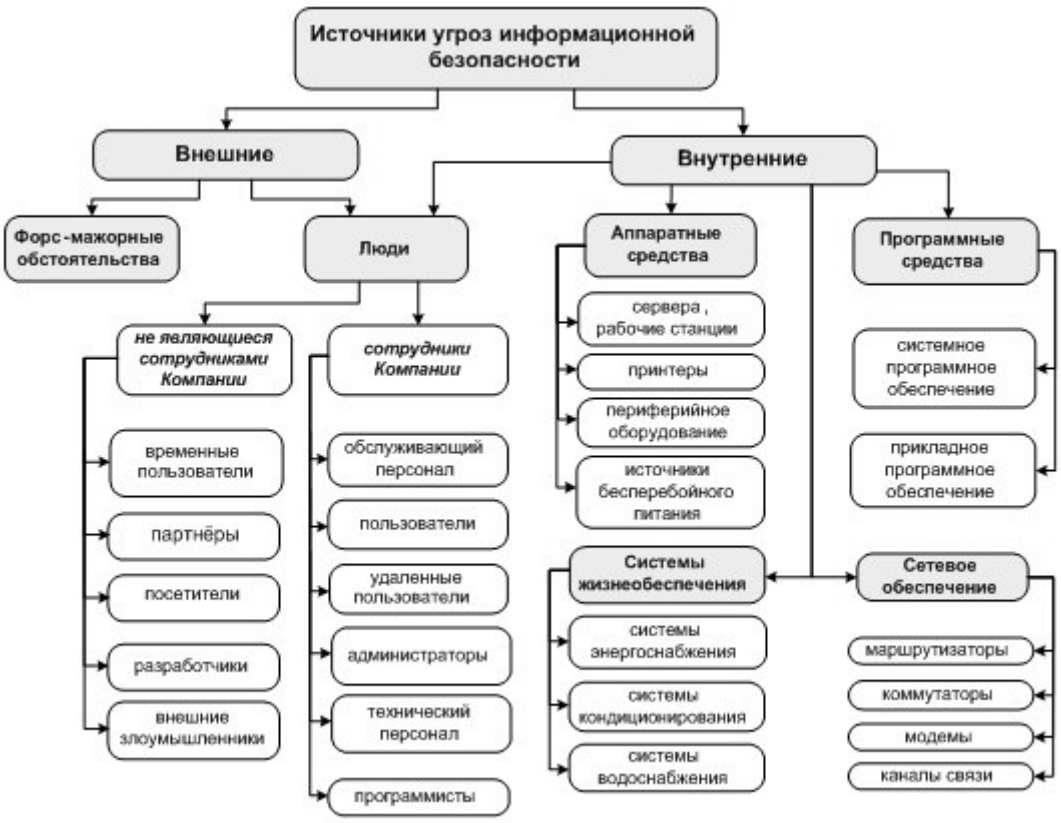


Рисунок .1.2 Источники угроз информации безопасности .

источники

безопасности

можно

на

основные

I.

действиями

(антропогенные

угроз).

Обусловленные

средствами

источники

III.

стихийными

Безопасностью

выступает

субъекты,

которых

быть

как

или

преступления.

в

случаях

говорить

причине

Эта

наиболее

и

наибольший

с

зрения

защиты,

как

человека

можно

спрогнозировать,

принять

меры.

качестве

источника

можно

субъекта,

доступ

или

к

со

средствами

объекта.

(источники),

которых

привести

нарушению

информации

быть

внешние,

и

Внешние

могут

случайными

преднамеренными

иметь

уровень

К

относятся:

-

структуры;

-

преступники

хакеры;

-

партнеры;

-

персонал

телематических

- представители

организаций

аварийных

- представители

структур.

субъекты

как

представляют

высококвалифицированных

в

разработки

эксплуатации

обеспечения

технических

знакомы

спецификой

задач,

и

функциями

принципами

программно-аппаратных

защиты

имеют

использования

оборудования

технических

сети.

ним

1. основной

(пользователи,

разработчики);

2.

службы

информации;

3.

персонал

охрана);

4.

персонал

эксплуатация).

учитывать

что

группу

антропогенных

составляют

с

психикой

специально

и

агенты,

могут

из

основного,

и

персонала,

также

службы

информации.

группа

в

перечисленных

источников

но

парирования

для

группы

иметь

отличия.

антропогенных

информации

важную

в

их

и

при

источников

Вторая

содержит

угроз,

технократической

человека

развитием

(Техногенные

угроз).

последствия,

такой

вышли

под

человека

существуют

по

Эти

угроз

прогнозируемые,

зависят

свойств

и

требуют

внимания.

класс

угроз

информации

актуален

современных

так

в

условиях

ожидают

роста

техногенных

вызванных

и

устареванием

парка

оборудования,

также

материальных

на

обновление.

средства,

источниками

угроз

информации

же

быть

1. средства

2. сети

коммуникации

канализации);

3.

4. несанкционированный

5.хакерская

сети

6.

на

7. IP-спуфинг

IP-адресов)

8.

(перехват

анализ)

9. злоупотребление

10.вирусы

приложения

"троянский

11. переадресация

12. отказ

обслуживании

13. раскрытие

топологии

14.

на

приложений

внутренними:

-

технические

обработки

- некачественные

средства

информации;

- средства сигнализации,

- другие

средства,

в учереждении .[7с 53].

Третья

источников

стихийные

угроз

обстоятельства,

непреодолимую

то

такие

которые

объективный

абсолютный

распространяющийся

всех.

непреодолимой

в

и

практике

стихийные

или

обстоятельства,

невозможно

или

или

предусмотреть,

невозможно

при

уровне

знания

возможностей.

источники

совершенно

поддаются

и

меры

от

должны

всегда.

источники

угроз

безопасности

правило

внешними

отношению

защищаемому

и

ними

прежде

природные

1. пожары;
2.

3. наводнения;
4.

5.различные

обстоятельства;

6.

явления;

-и дргие форс-можерные обстоятельства.

Анализируя все выше сказанное можно сделать следующие выводы :

Служба

(СБ)

самостоятельной

единицей,

непосредственно

предприятия.

структура

системой

имеющая

вертикаль,

для

обеспечения

где

определенность,

границы,

отношений

всех

– от

сотрудника

менеджеров

звена.

Основными

службы

предприятия

1. обеспечение

производственно-торговой

и

информации

сведений,

коммерческой

2. организация

по

организационной

инженерно-технической

аппаратной,

и

защите

тайны;

3.

специального

исключающего

получение

являющихся

тайной;

4.

необоснованного

и

к

и

составляющим

тайну;

5.

и

возможных

утечки

информации

процессе

производственной

и

экстремальных

пожарных

др.) и др.

Под

безопасности

являются:

1.

(копирование)

2. уничтожение

3. модификация

информации;

4.

доступности

информации;

5.

подлинности

6.навязывание

информации.

Правовой

системы

защиты

на

основывается

нормах

права

предполагает

закрепление

фирмы

государства

поводу

использования

защиты

фирмы

персонала

поводу

персонала

установленные

защитного

ответственности

за

порядка

информации.

Внешние угрозы это негативные факторы, воздействующие на то или иное предприятия извне, т.е. без вовлечения внутренних ресурсов. Внешние угрозы традиционно являются одними из наиболее важных к рассмотрению при формировании стратегии обеспечения безопасности предприятия.

В

качестве

угроз

выступать

субъекты

так

проявления

Причем

угроз

находиться

внутри

системы –

источник,

и

нее

источник.

на

и

источники

потому

для

и

же

методы

для

и

источников

быть

Но

свое

остановим

внешних

угроз,

на

что

меньше

изучены.

2 Задачи решаемые службой безопасности по обеспечению режима безопасности на примере ГБУСО «Первомайский психоневрологический интерната »

2.1 Характеристика объекта исследования

ГБУСО «Первомайский психоневрологический интернат » предназначен для проживания граждан, страдающих хроническими психическими заболеваниями и инвалидов первой и второй групп.

Изначально с 1960 года это был дом-интернат общего типа для престарелых и инвалидов, затем исходя из реальных жизненных запросов, учреждение неоднократно перепрофилировалось и переименовывалось.

Здание учреждения 3-х этажное кирпичное, типовое, один корпус, общей площадью 5786,6 кв. метров.

ГБУСО «Первомайский психоневрологический интерната» находится по адресу :Псковская область, Палкинский район, деревня Лещихино.

Интернат является юридическим лицом, имеет самостоятельный баланс,

лицевые счета по учету средств областного бюджета и средств, полученных от предпринимательской и иной приносящей доход деятельности, открытые в территориальном органе Федерального казначейства.

В соответствии с целями и задачами учреждения, установленными уставом, оно вправе осуществлять приносящую доход деятельность - предоставление социальных услуг гражданам на условиях частичной или полной оплаты, в порядке, предусмотренном действующим законодательством[7с 53].

2.2 Техническое обеспечение объекта исследования

ГБУСО

психоневрологический

состоит

30 комнат:

кабинета

а

кабинета

деректора ГБУСО

психоневрологический имеется

вспомогательных

.

В

«Первомайский

интерната » 13

и 2

Их

единая

система,

базе

сети

«звезда»,

использованием

восьми

коммутатора

фирмы-производителя

с

способностью 10/100

(является

коммутатором

предназначенным

повышения

работы

группы

обеспечивая

этом

уровень

Мощный

одновременно

этим,

в

Acorp

пользователям

труда

к

порту

оборудование,

на

10 Мбит/с

100 Мбит/с,

время

и

потребности

большой

способности

В

сетевого

в

используются

интегрированные

либо

карты

DFE-520TX

восьмижильного

(витая

Имеющиеся

учереждение

сервера

под

операционными

один

управлением

Linux,

другой

управлением

Windows (приложение А)

2.3 Прогаммное обеспечение ГБУСО «Первомайском психоневрологическом интернате »

В

учереждение

всех

станциях

операционная

Windows 7

стандартный

p

Microsoft

2010.

На

установлены

программы

8.0, 1С:УправлениеТорговлей 8.0,

и

8.0. К

1С

доступ

всех

компьютеров,

пользователь

зайти

под

именем

паролем

соответствующими

Сдесь

находятся

документооборота,

и

документы

«Первомайского

интерната » .

же

обновления,

для

программного

За

никто

работает,

образом,

представляет

«архив»,

самых

данных

этой

С

администратора

сервер

войти

технический

и

администратор.

иректор

учереждения

за

«Director».

имеет

ко

базам

и

папкам

данного

.

Он

и

всевозможные

отчеты,

стратегию

данного

на

этих

как

ближайшее

так

на

период.

компьютере

деректора

ДИУ

(к

базам

имеют

все

компьютеры

Заместитель

ведет

ГБУСО

психоневрологического

» . Для

он

специальной

данных,

в

Access»,

учета

клиентов.

2.4 Средства защиты информации объекта исследования

ГБУСО

психоневрологическом

» сервер

сервером

файл-сервером,

так

прокси-сервером .

качестве

защиты

учереждения

Dr.Web

Suite.

же

сервере

TrustAccess 1.2

TrustAccess —

межсетевой

высокого

защиты

централизованным

предназначенный

защиты

и

станций

сети

несанкционированного

а

разграничения

доступа

информационным

предприятия.

более

основные

данных

TrustAccess

компании

безопасности»

собой

экран,

защищать

(рабочие

или

от

доступа.

применения

является

локальной

предприятий

обеспечение

доступа

папкам

документами.

может

для

конфиденциальных

документов,

также

составляющих

тайну.

может

как

сетях

доменной

так

в

сетях,

этом

защиты

быть

физические,

и

машины.

построен

основе

«клиент-сервер».

аутентификации,

фильтрации

разграничение

доступа

администратором

сервере

Фильтрация

на

компьютерах.

действия

в

работы

программой

к

процедуры

на

части

TrustAccess

из

компонентов:

управления -

централизованное

агентами

на

компьютерах,

также

и

данных.

функции –

абонентов

при

протокола

регистрация

безопасности

хранение

Рекомендуется

на

сервер

на

из

в

агент

экрана

- агент) –

для

пользователя,

доверенного

передачи

и

функции

доступа

защищаемым

автоматизированное

место

администратора —

централизованное

абонентами

механизмами

Устанавливается

рабочее

администратора

Для

процедуры

в

пользователи

использовать

только

но

дополнительные

средства.

ним

персональные

eToken

фирмы

Knowledge

или

(производства

Dallas

Для

защиты

используются

правил :

доступа.

для

доступа

сетевым

защищаемого

Для

правил

данные

параметрах

с

(учетные

наименования

портов

и

д.);

правила.

для

доступа

общим

защищаемого

и

соединений

протоколу

Pipes;

правила.

для

доступа

защищаемым

по

протоколам,

удаленным

Также

позволяет

различные

протоколы

IPv6,

IPX,

IPX)

настраивать

от

сбоев.

защита

различных

атак:

in

Middle»,

защищаемого

Replay-атак,

IP-адреса

сетевых

прослушивания

подмены

пакетов,

в обслуживании.(приложение Б).

особенностью

является

его

использования

одном

с

программами

обеспечения

в

числе

с

экранами

производителей.

задачи

персональных

TrustAccess

получать

к

серверам,

данных

общим

только

пользователям,

работают

персональными

Для

остальных

в

сети

к

ресурсам

данным

недоступен.

информационных

персональных

Изоляция

разделение

на

участки,

снизить

стоимость

Разграничения

пользователей

серверам.

позволяет

сетевой

к

серверам

основе

пользователей.

в

OT

B

отделе

сотрудник,

получает

к

или

серверу

данных.(приложение С).

Также

организовать

к

на

общих

Это

делать

основе

допуска

должностей.

доступ

общей

на

всем

может

только

Решение

Enterprise

имеет

архитектуру.

клиентов

на

рабочие

и

Антивирусный

обеспечивает

администрирование

и

сети

включая

обновление

баз

программных

компонентов,

состояния

извещения

вирусных

сбор

Установка

сервера

развёртывание

сети

базе

ES

простотой

занимает

времени.

развёртывания

сети

применяться

технологии

Directory,

в

Для

антивирусного

с

агентами

использоваться

протокол

так

IPX/SPX/NetBIOS,

позволяет

антивирусную

не

исторически

инфраструктуру

Антивирусная

основанная

решении

Enterprise

обладает

прозрачностью

Все

антивирусной

могут

файлы

подробность

можно

.

Любое

над

производимыми

антивирусной

отображаются

статистике.

система

администратора

проблемах,

в

сети,

которой

отображаться

в

администратора,

и

по

почте.

выбор

компаний,

о безопасности своего бизнеса. Многообразие и количество современных компьютерных угроз вывели приоритет мероприятий по защите данных, проводимых в организациях, на передних план. Антивирус является одним из главных технических инструментов, позволяющих автоматизировано решить эту проблему и продолжать бесперебойно бизнес-процесс.

К приемуществам Dr.Web Enterprise Suite можно отнести:

1. Опыт крупных проектов

Среди клиентов «Доктор Веб» - крупные компании с мировым именем, банки, государственные организации, сети которых насчитывают десятки тысяч компьютеров. Антивирусным решениям "Доктор Веб" доверяют высшие органы государственной и исполнительной власти, компании топливно-энергетического сектора, предприятия с мульти-аффилиатной структурой. Dr.Web имеет 14-летний опыт разработок решений для бизнеса, проверенных нашими пользователями и временем.

2. Исключительная масштабируемость

Возможность иерархического построения системы антивирусной защиты на базе нескольких серверов Dr.Web Enterprise Suite, соединённых между собой и обеспечивающих своими ресурсами единую антивирусную сеть, делает это решение незаменимым для компаний, имеющих многофилиальную структуру. Программа легко масштабируется в зависимости от размеров и сложности сети и может быть адаптирована как для простых сетей из нескольких компьютеров, так и для сложных распределенных интранет-сетей, насчитывающих десятки тысяч узлов. [27].

Масштабирование обеспечивается возможностью использовать группирование из нескольких взаимодействующих серверов Dr.Web Enterprise Suite и отдельного SQL-сервера для хранения данных и комплексной структурой взаимодействия между ними.

3. Единый центр управления антивирусной защитой

Dr.Web Enterprise Suite предоставляет возможность установки рабочего места администратора (консоли) практически на любом компьютере под управлением любой операционной системы.

2.5 Политики безопасности В ГБУСО «Первомайском психоневрологическом интернате »

После детального изучения системы безопасности объекта исследования был установлен большой пробел в системе защиты – это факт отсутствия официальной политики безопасности. Конечно существовали некие правила, но они не носили систематического характера и не носили

всеобьемлющего характера.

Для защиты информации в данном учреждение совместно с директором была разработана политика безопасности соответствующая сегодняшним требованиям.(приложение D).

Цель: гарантировать использование по назначению компьютеров и телекоммуникационных ресурсов учереждения ее сотрудниками, независимыми подрядчиками и другими пользователями. Все пользователи компьютеров обязаны использовать компьютерные ресурсы квалифицированно, эффективно, придерживаясь норм этики и соблюдая законы.

Следующая политика, ее правила и условия касаются всех пользователей компьютерных и телекоммуникационных ресурсов и служб компании, где бы эти пользователи ни находились. Нарушения этой политики влечет за собой дисциплинарные воздействия, вплоть до увольнения и/или возбуждения уголовного дела.

Данная политика может периодически изменяться и пересматриваться по мере необходимости.

Руководство данного учереждения имеет право, но не обязано проверять любой или все аспекты компьютерной системы, в том числе электронную почту, с целью гарантировать соблюдение данной политики. Компьютеры и бюджеты предоставляются сотрудникам учереждения с целью помочь им более эффективно выполнять свою работу.

Компьютерная и телекоммуникационная системы принадлежат данному учереждению и могут использоваться только в рабочих целях. Сотрудники учереждения не должны рассчитывать на конфиденциальность информации, которую они создают, посылают или получают с помощью принадлежащих Компании компьютеров и телекоммуникационных ресурсов.

Пользователям компьютеров следует руководствоваться перечисленными ниже мерами предосторожности в отношении всех компьютерных и телекоммуникационных ресурсов и служб. Компьютерные

и телекоммуникационные ресурсы и службы включают в себя (но не ограничиваются) следующее: хост-компьютеры, серверы файлов, рабочие станции, автономные компьютеры, мобильные компьютеры, программное обеспечение, а также внутренние и внешние сети связи (интернет, коммерческие интерактивные службы и системы электронной почты), к которым прямо или косвенно обращаются компьютерные устройства Компании.

Пользователи должны соблюдать условия всех программных лицензий, авторское право и законы, касающиеся интеллектуальной собственности.

Неверные, навязчивые, непристойные, клеветнические, оскорбительные, угрожающие или противозаконные материалы запрещается пересылать по электронной почте или с помощью других средств электронной связи, а также отображать и хранить их на компьютерах Компании. Пользователи, заметившие или получившие подобные материалы, должны сразу сообщить об этом инциденте своему руководителю.

Все, что создано на компьютере, в том числе сообщения электронной почты и другие электронные документы, может быть проанализировано руководством учереждения .

Пользователям не разрешается устанавливать на компьютерах и в сети Учереждения программное обеспечение без разрешения системного администратора.

Пользователям запрещается удалять и перенастраивать антивирусные программы без разрешения системного администратора.

Пользователь обязан сообщать обо всех сбоях в работе системы и программном обеспечении службы безопасности ГБУСО «Первомайского психоневрологического интерната. »

Пользователи не должны пересылать электронную почту другим лицам и организациям без разрешения отправителя.

Электронная почта или представляющего ее адвоката должна содержать в колонтитуле каждой страницы сообщение: "Защищено

адвокатским правом/без разрешения не пересылать".

Пользователям запрещается изменять и копировать файлы, принадлежащие другим пользователям, без разрешения владельцев файлов.

Запрещается использование без предварительного письменного разрешения компьютерных и телекоммуникационных ресурсов и служб Компании для передачи или хранения коммерческих либо личных объявлений, ходатайств, рекламных материалов, а также разрушительных программ (вирусов и/или самовоспроизводящегося кода), политических материалов и любой другой информации, на работу с которой у пользователя нет полномочий или предназначенной для личного использования.

Пользователь несет ответственность за сохранность своих паролей для входа в систему. Запрещается распечатывать, хранить в сети или передавать другим лицам индивидуальные пароли. Пользователи несут ответственность за все транзакции, которые кто-либо совершит с помощью их пароля.

Если пользователь узнал о компрометации своего пароля или пароля другого сотрудника компании он должен немедленно сообщить об этом службы безопасности .

Возможность входа в другие компьютерные системы через сеть не дает пользователям права на подключение к этим системам и на использование их без специального разрешения операторов этих систем.

ЗАКЛЮЧЕНИЕ

Служба безопасности (СБ) имеется на каждом крупном и среднем предприятии (фирме) и выполняет многообразные функции по обеспечению экономической и информационной безопасности бизнеса.

Служба безопасности - это правоохранительная некоммерческая организация, оказывающая охранно-сыскные услуги своему (своим) учредителю (учредителям) и другим организациям на основе действующего законодательства, собственного Устава и заключенного с ними договора.

Цель деятельности СБ - своевременное пресечение (нейтрализация) противоправных посягательств на экономические интересы и персонал предприятия.

Служба безопасности выполняет многообразные функции и обеспечивает экономическую и информационную безопасность бизнеса.

Исходя из всего вышеизложенного, можно сделать следующие выводы - без службы безопасности не сможет стабильно работать ни одно крупное и среднее предприятие (фирма), поскольку СБ - это гарант бесперебойной и безопасной работы предприятия.

В ближайшее время, когда прогресс в области развития средств вычислительной техники, программного обеспечения и сетевых технологий даст толчок к развитию средств обеспечения безопасности, тогда потребуется во многом пересмотреть существующую научную парадигму информационной безопасности.

Основными положениями нового взгляда на безопасность должны являться:

исследование и анализ причин нарушения безопасности компьютерных систем;

разработка эффективных моделей безопасности, адекватных современной степени развития программных и аппаратных средств;

создание методов и средств корректного внедрения моделей безопасности с возможностью гибкого управления безопасностью в зависимости от выдвигаемых требований, допустимого риска и расхода ресурсов;

необходимость разработки средств анализа безопасности компьютерных системс помощью осуществления тестовых воздействий (атак).

Широкая информатизация обществ,внедрение компьютерной технологии в сферу управления объектамигосударственногозначения, стремительныйрост темпов научно-технического прогресса наряду с положительными достижениями в информационных технологиях, создают реальные предпосылки для утечки конфиденциальной информации.

В настоящее время проблемы связанные с защитой информации

беспокоят как специалистов в области компьютерной безопасности, так и многочисленных рядовых пользователей персональных компьютеров. Это связано с глубокими изменениями, вносимыми компьютерной технологией в нашу жизнь. Изменился сам подход к понятию “информация”. Этот термин сейчас больше используется для обозначения специального товара, который можно купить, продать, обменять на что-то другое и т.д. При этом стоимость подобного товара зачастую превосходит в десятки, а то и в сотни раз стоимость самой вычислительной техники, в рамках которой он функционирует .

В работе была проанализирована деятельность службы безопастности ее техническое и программное оснащение. Был подвергнут анализу комплекс мер по защите информации, в ходе которого были выявлены небольшиенедостаткии был предложен комплекс мер по их устранению.

Была разработана политика корпоративной безопасности, в которой были отображены основные действия сотрудников и их обязанности в плане защиты информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. http://www.compdoc.ru/secur/soft/comparative-review-modern-antivir/
2. Айтипедия http://www.itpedia.ru/index. php/
3. Википедия (свободная энциклопедия) http://ru. wikipedia.org/wiki/
4. http://roox.net.ru/infosec/04/
5. http://www.thg.ru/software/malware_spyware_faq/index.html
6. http://www.oxpaha.ru/publisher_234_28501
7. Биячуев Т.А. / под ред. Л.Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2014.
8. Гмурман А.И. Информационная безопасность. М.: «БИТ-М», 2014 г.
9. Домарев В.В. Безопасность информационных технологий. Системный

подход. – К: ООО ТИД «Диасофт», 2014

10. www.citforum.ru
11. www.DrWeb.com
12. www.microsoft.com
13. www.securitylab.ru
14. Баслы П.Н. «Информационная безопасность» – Ростов на Дону: Феникс,2006.- 253 с.
15. Партыка Т.Л. «Информационная безопасность». – М., Форум, 2017
16. Материалы и журналы компьютера www.computerra.ru
17. Агеев А. С. «Организация работ по комплексной защите информации». - К., 2013.
18. Ярочкин В. И. «Технические каналы утечки информации».- М., 2015
19. http://engine.adland.ru
20. Батурин Ю.М., Жодзинский А.М. «Компьютерная преступность и компьютерная безопасность» - М.: Юрид. лит.,2014.
21. Домарев В.В. «Безопасность информационных технологий. Системный подход». - К.: ООО ТИД «Диасофт», 2014. - 992 с.
22. Хофман Л., «Современные методы защиты информации», - Москва, 2015.
23. Евгений Касперский «Компьютерные вирусы» - М.: 2017
24. http://antispam.home.nov.ru/index.htm.
25. Панасенко С.П., «Защита информации в компьютерных сетях» // Журнал «Мир ПК» 2012 № 2.
26. Форд Джерри Ли «Персональная защита от хакеров». – М., Куденец – Образ, 2013
27. Грибунин В.Г. Политика безопасности: разработка и реазизация// «Информационная безопасность», 2015, №1.
28. Андрианов В. И «Шпионские штучки и устройства для защиты объектов и информации». - СПб., 2011.
29. http://antispam.home.nov.ru/index.htm.

30. Медведевский И.Д., П.В Семьянов, Д.Г Леонтьев «Атака на Интернет» - 2-ое издание – М.:2015

31. Д.Ведеев «Защита данных в компьютерных сетях» - М.:2015

32. Локхард Э. «Антихакенг в сети» СПБ: Питер 2015.-297с.

33. Библиотека сетевой безопасности security.tsu.ru

34. Глобальные сети и коммуникации № издания с1-по 6 – М.:2015

35. Лысов А.В., Остапенко А.Н.. Энциклопедия промышленного шпионажа.-СПб., 2013.

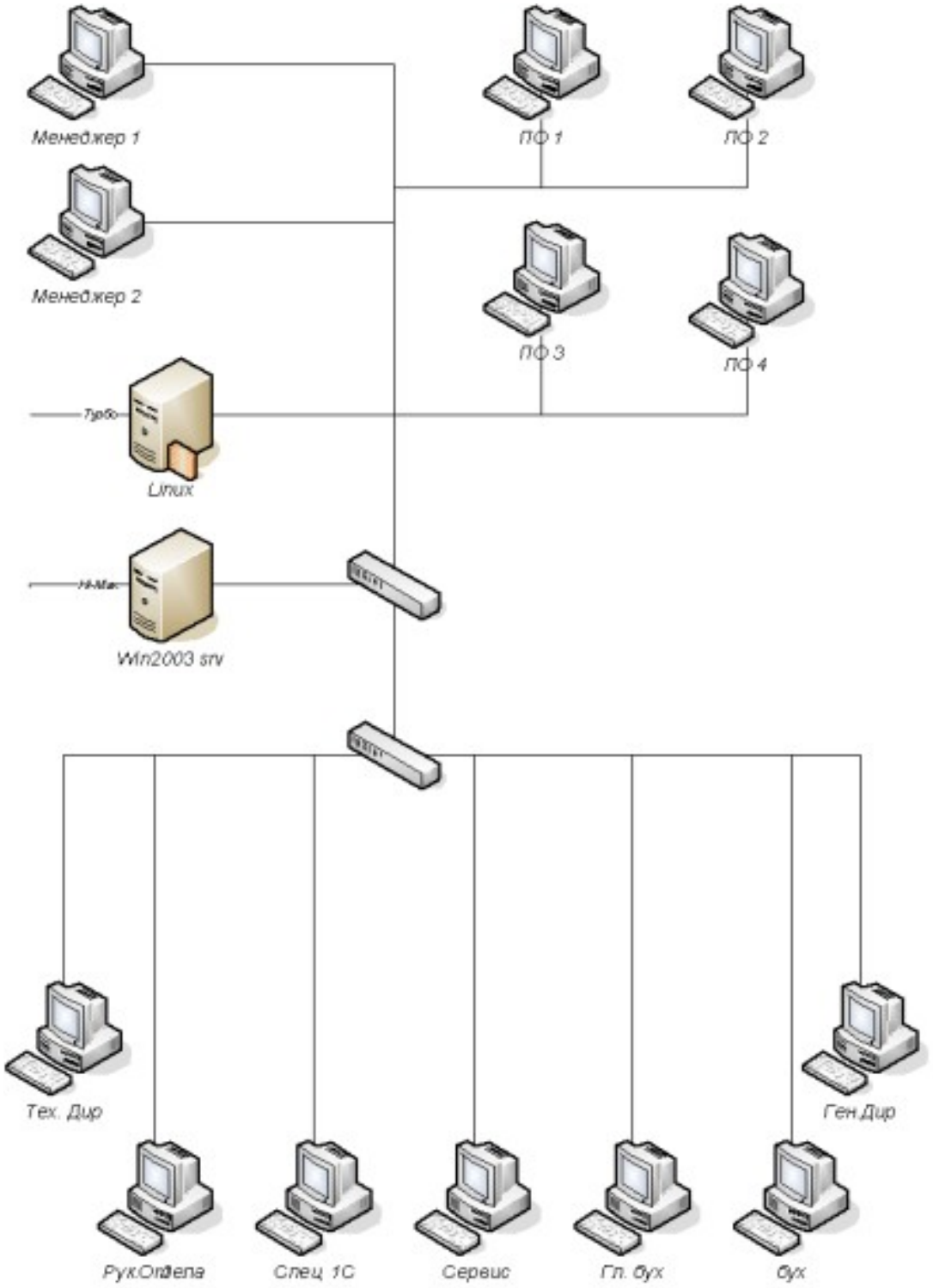
36. Торокин А.А. «Основы инженерно-технической защиты информации». – М.: 2077. – 345 с.

37. Халяпин Д. Б., Ярочкин В. И. «Основы защиты промышленной и коммерческой». - К.,2011.

38. Ярочкин В. И. «Технические каналы утечки информации».- М., 2005

39. Максимов Ю. Н. «Защита информации в системах и средствах информатизации и связи». - СПб., 2017

Приложение А


Менеджер 1
ПФ 1
ПФ 2
Менеджер 2
ПФ 3
ПФ 4
Турбо
Linux
Win2003 srv
Тех. Дир
Ген.Дир
Рук.Отдела
Спец. 1С
Сервис
Гл. бух
бух

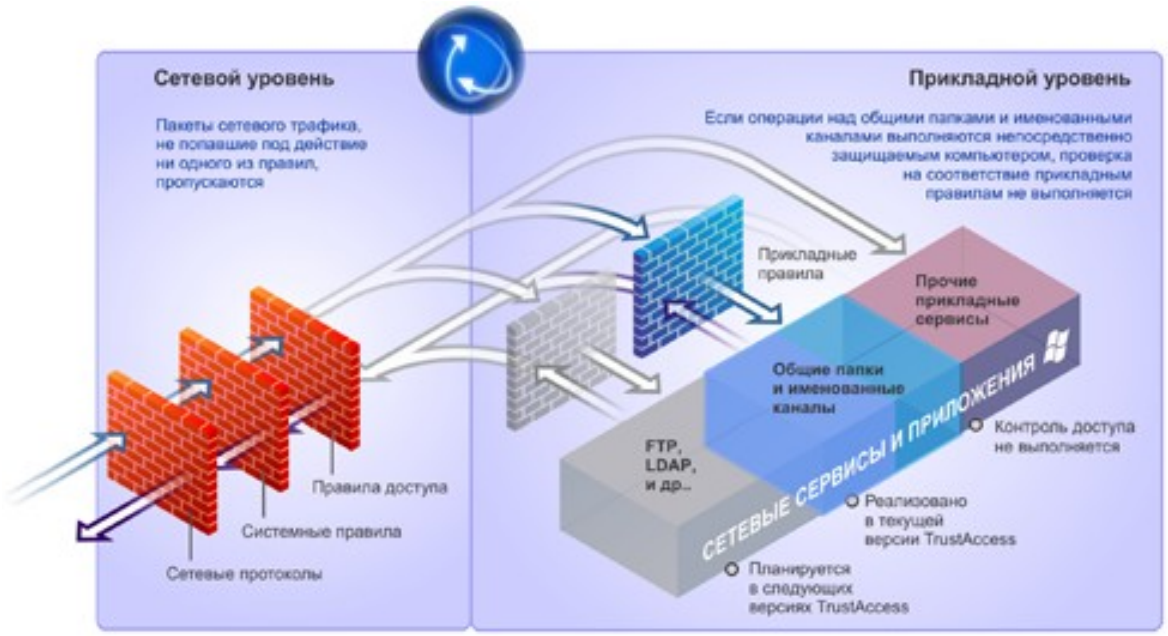
схема

сети

«Первомайского

интерната » .

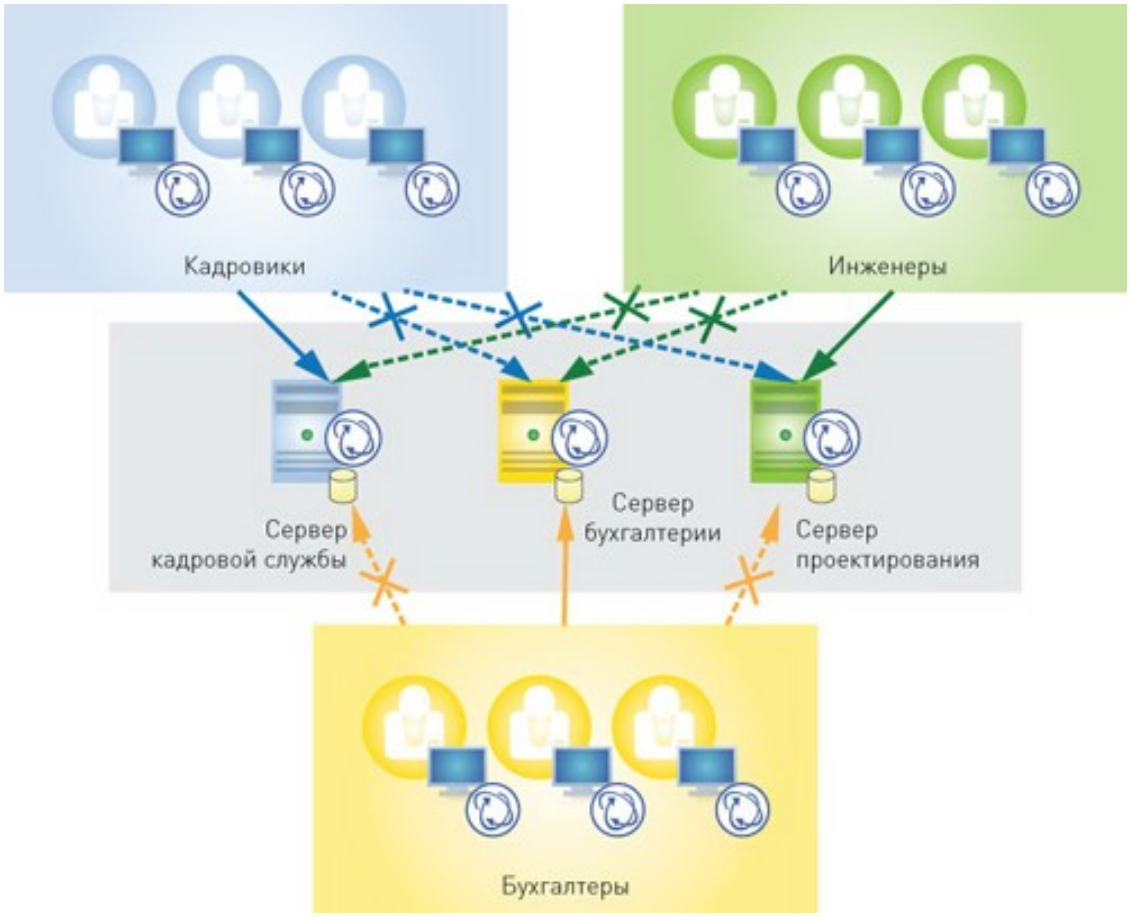
Приложение Б



применения

правил

Приложение С



Пример

доступа

серверам

группам

Приложение D

Схема политики безопасности в ГБУСО «Первомайском психоневрологическом интернате »