АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«УРЮПИНСКИЙ КОЛЛЕДЖ БИЗНЕСА»

Кафедра экономики и информационных дисциплин

ОТЧЕТ
по практической подготовке

Студента Бескоровайного Ивана Александровича
(Фамилия, имя, отчество)

Специальность 10,02,05 Обеспечение информационной безопасности автоматизированных систем (шифр, наименование)

Группа ЗОибП, 40иб9
Форма обучения очная

Наименование базы практической подготовки: Государственное бюджетное учреждение здравоохранения Урюпинская центральная районная больница имени В,Ф, Жогова

Адрес: 403112 Волгоградская обл., г. Урюпинск, ул. Весенняя, д.2

Сроки прохождения практической подготовки с «08» декабря 2022 г. по «21» декабря 2022 г.

Руководитель практической подготовке от принимающей организации

_____Говоров С. В._____
(подпись) (Фамилия И.О.)

Отчет по практической подготовке защищен с оценкой

_____

«21» _____ 2022 г.

Руководитель практической подготовки от колледжа преподаватель

_____ Кузнецов А. В.

г. Урюпинск 2022/2023 учебный год

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«УРЮПИНСКИЙ КОЛЛЕДЖ БИЗНЕСА»

ДНЕВНИК
прохождения практической подготовки
ПМ.03 Защита информации техническими средствами

Компонент образовательной программы: производственная практика по профилю специальности

Обучающийся Бескоровайный Иван Александрович_____

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Группа ЗОибП, 4Оиб9_____

Руководитель от АНПОО «Урюпинский колледж бизнеса»

Кузнецов Александр Викторович

Место прохождения практической подготовки:

ГБУЗ Урюпинская ЦРБ имени В. Ф. Жогова

Руководитель практической подготовки от принимающей организации

Говоров Сергей Викторович

Отметка о прохождении практической подготовки

Прибыл на практику	Выбыл с практики
«08» декабря 2022 г.	«21» декабря 2022 г.
Главный врач	Главный врач
_____ / Сизов Г. Д./	_____ / Сизов Г. Д./
(подпись) М.П.	(подпись) М.П.

1. Календарно-тематический план прохождения практической подготовки

№ п/п	Содержание планируемой работы	Сроки выполнения
1	2	3
1.	Участие в монтаже, обслуживании и эксплуатации технических \ средств защиты информации	08.12.2022 - 10.12.2022
2.	Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения	12.12.2022- 14.12.2022
3.	Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам	15.12.2022- 17.12.2022
4.	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами	19.12.2022- 20.12.2022
5.	Оформление дневника отчета	21.12.2022

1 .Обучающийся Бескоровайный И. А._____ _____

2. Руководитель практической подготовки от АНПОО «Урюпинский колледж бизнеса» преподаватель Кузнецов А. В.__ _____

2. Выполнение заданий по программе практической подготовки

Дата	Выполнение заданий согласно календарно-тематического плана
1	2
08.12.2022	Знакомство с базой практики, описание предметной области, анализ объектов информатизации
09.12.2022	Участие в установке компонентов технических средств защиты информации
10.12.2022	Участие в эксплуатации ИС и системы защиты информации в ее в соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией
1202.2022	Участие в монтаже компонентов инженерной защиты, технической охраны объектов, систем видеонаблюдения
13.12.2022	Выявление и устранение недостатков инженерно-технических средств обеспечения информационной безопасности
14.12.2022	Участие в эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения в соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией
15.12.2022	Участие в монтаже компонентов средств защиты информации от несанкционированного съема и утечки по техническим каналам
16.12.2022	Выявление и устранение недостатков технических средств защиты информации от несанкционированного съема и утечки по техническим каналам
17.12.2022	Участие в эксплуатации средств защиты информации от несанкционированного съема и утечки по техническим каналам в соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией
19.12.2022	Изучение порядка применения нормативных правовых актов в сфере обеспечения защиты информации техническими средствами
20.12.2022	Оформление технической и технологической документации
21.12.2022	Оформление дневника отчета

1.Обучающийся Бескоровайный И. А..

2.Руководитель практической подготовки от принимающей организации Говоров С. В, &'

3. Замечание руководителей практической подготовки от учебного заведения

Дата проверки	Содержание замечания	Подпись и должность проверяющего преподавателя
1	2	\ 3

Оценка по практической подготовке _____

Руководитель практической подготовки от АНПОО «Урюпинский колледж бизнеса»

Кузнецов Александр Викторович

(Ф.И.О) (подпись)

«-<'$> декабря 2022г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Важным аспектом профессиональной подготовки специалистов в любой отрасли является освоение практических навыков и подготовка конкурентоспособных специалистов.

Цель производственной практики - закрепление теоретических знаний по изученным дисциплинам, ознакомление студентов с характером и особенностями их будущей деятельности на основе развития профессиональных умений и получения опыта профессиональной деятельности как в рамках отдельно взятой организации.

Задачи производственной практики:

- участвовать в монтаже, обслуживании и эксплуатации технических средств защиты информации;

- участвовать в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;

- участвовать в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам;

- применять нормативно правовые акты, нормативных методических документов по обеспечению защиты информации техническими средствами.

Объектом практики - государственное бюджетное учреждение здравоохранения «Урюпинская центральная районная больница имени В.Ф. Жогова».

Предметом практики является: защита информации техническими средствами.

1. УЧАСТИЕ В МОНТАЖЕ, ОБСЛУЖИВАНИИ И ЭКСПЛУАТАЦИИ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Объектом для защиты информации техническими средствами конфиденциальной информации являлся ГБУЗ «Урюпинская центральная больница» (ЦРБ).

В ЦРБ используется функциональная организационная структура. Функциональная структура управления это структура, сформированная в соответствии с основными направлениями деятельности организации, где подразделения объединяются в блоки. Организационная структура больницы разделяется на пять блоков (Приложение 1).

Средства защиты информации, это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Для защиты больницы по периметру с трех сторон от нее установлен двух метровый бетонный забор и с одной стороны полтора метровый железный забор.

На территории ЦРБ установлено охранное освещение, которое освещает земельный участок.

Так же на территории больницы присутствует видеонаблюдение. По периметру ЦРБ расположено четыре камеры (Приложение 2).

На въезде в больницу установлен шлагбаум, который открывается по нажатию охранником специальной кнопки. Так же здесь установлена кнопка экстренного вызова оперативной группы Росгвардии. Въезд осуществляется строго по предъявлении специального разрешения. Для служебных машин въезд на территорию свободный.

Урюпинская центральная больница занимает отдельно стоящее четырехэтажное здание. Стены здания кирпичные. Несущие стены в толщину пятьдесят сантиметров, а внутренние тридцать сантиметров.

В ЦРБ имеется один главный и три запасных выходов. На главном входе

установлена двухстворчатая пластиковая дверь, а запасные выходы оборудованы металлическими дверями. В кабинетах и палатах установлены пластиковые двери.

В медицинском учреждении установлена охранная система «С2000-Пирон-Ш». Также в больнице установлена пожарная сигнализация «ИП 212-45».

Пожарная сигнализация выполняет целый ряд функций, осуществление которых обеспечивается комплексом сложных устройств. Для их налаженной работы необходимо соблюдать определенные правила монтажа, настройки и эксплуатации, а так же периодической проверки работоспособности. Если все устройства системы работают хорошо, то сигнализация способна выполнить следующие функции:

- обнаружение возгорания в помещении на самой ранней стадии;
- передачу сигнала о возгорании на пульт пожарной охраны;
- запуск сигнала, оповещающего о пожаре;
- отключение системы общей вентиляции и включение системы дымоотвода;
- запуск системы автоматического тушения пожара.

На производственной практике было рассмотрено отделение травматологии. Оно расположено на третьем этаже, в правом крыле. В него можно попасть через лестничную клетку.

Здесь расположено семнадцать кабинетов. Все двери в отделении - пластиковые, оборудованные внутренними врезными замками, по одному замку на каждую дверь. В отделении установлено двадцать шесть окон, на окнах отсутствуют железные решетки, в каждом окне установлена форточка. В отделении отсутствуют камеры видеонаблюдения (Приложение 3).

2. УЧАСТИЕ В МОНТАЖЕ, ОБСЛУЖИВАНИИ И ЭКСПЛУАТАЦИИ СРЕДСТВ ОХРАНЫ И БЕЗОПАСНОСТИ, ИНЖЕНЕРНОЙ ЗАЩИТЫ И ТЕХНИЧЕСКОЙ ОХРАНЫ ОБЪЕКТОВ, СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

Инженерная защита (ИЗ) - это совокупность технических средств и мероприятий, нацеленных на предотвращение утечек, разглашения информации, и несанкционированного доступа в сетевые ресурсы организации.

Существует классификация инженерной защиты информации:

- по виду;
- объектам воздействия;
- используемым технологиям.

Выделяют следующие виды средств инженерной защиты:

1. Физические. Используются с целью решения задач по охране предприятия, наблюдению за территорией и помещениями, осуществлению контролируемого доступа в здание. К ним относят охранно-пожарные системы, аварийное и локальное освещение, а также охранное телевидение. Физические средства защиты информации можно разделить на предупредительные, обнаруживающие и ликвидирующие угрозы, активно используемые сегодня руководителями многих предприятий.

2. Аппаратные. К ним относятся электронные и механические устройства, предназначенные для инженерно-технической защиты информации и для противодействия шпионажу. Их главная задача - выявление каналов утечки информации, их локализация (обнаружение) и нейтрализация. Примерами таких средств могут служить комплексы для поиска сетевых радиопередатчиков, телефонных закладок и радиомикрофонов, устанавливаемых с целью секретного прослушивания.

3. Программные. Включают в себя системы по защите информации, обеспечивающие защиту секретных данных: проектов, чертежей,

В процессе производственной практики, в отделении травматологии, в кабинете заведующей отделением была обнаружена неисправность замка, а именно при повороте ключа в замочной скважине выдвижные запоры не выдвигались. Было принято решение - снять нерабочий замок и заменить на новый, полностью рабочий. После того как, замок был заменен, были проверены все остальные замки. Неисправностей обнаружено не было

Так же в целях усиления защиты был установлен новый дверной замок в сестринском кабинете (Приложение 3).

Во время производственной практики было принято участие в плановом обслуживании пожарной сигнализации.

Осуществлялась проверка всей системы в целом. В процессе проверки было выявлено, что один из датчиков не реагирует на искусственное задымление и не посылает сигнал на пульт управления. После чего было неисправный датчик был заменен на исправный.

Таким образом, в ходе производственной практики было проведено знакомство с отделением травматологии, в котором были изучены технические средства защиты информации Урюпинской ЦРБ.

Также были получены практические навыки в обслуживание пожарно-охранной системы сигнализации, а именно обнаружение неисправных датчиков задымления и замена их на новые. Помимо, этого было проведено обслуживание, замена и установка новых дверных замков. *

 стратегических и тактических задач

фирмы, финансовых и бухгалтерских данных, сведений о работающих сотрудниках.

К средствам технической охраны в больнице относятся:

- видеонаблюдение;
- пожарная сигнализация;
- охранная сигнализация;
- тревожная кнопка.

На территории больницы ведется видеонаблюдение. Оно состоит, из видеорегистратора «ORIENT XVR-1908/1080HN [8x BNC, 4xRCA, PTZ, Ethernet, RS-485, USB x2]», монитора «18.5" Монитор AOC E970SWN», видеокамер марки «HiWatch DS-I200(D)».

Видеорегистратор самостоятельное устройство для записи, хранения и дальнейшего воспроизведения и передачи архивов видеонаблюдения. Видеорегистраторы в системах видеонаблюдения в настоящее время имеют наибольшее распространение среди записывающих устройств. Видеорегистратор установленный в ЦРБ имеет 8 портов BNC, 4 RCA, Ethernet вход, а так же 2 USB порта.

Видеокамеры размещенные на территории больницы имеют разрешение 2Мп 1920x1080 FullHD. Они обладают углом обзора 132.2 градуса. Имеют ночной режим съемки. Видеокамера работает в черно-белом режиме (Приложение 2).

Пожарная сигнализация состоит из:

- пожарных извещателей (дымовые, пламени);
- прибор приемно-контрольный (ППК);
- релейный блок;
- источник бесперебойного электропитания;
- вспомогательные устройства канала передачи сообщений (повторители);

Пожарный приёмно-контрольный прибор — главное устройство, предназначенное для приёма сигналов от пожарных извещателей, звуковой и световой сигнализации, выдачи информации на пульты централизованного наблюдения, формирования стартового импульса запуска пожарного прибора управления, а также благодаря нему в пожарной части происходит процесс получения сигнала и его обработки.

Охранная сигнализация-это система, предназначенная для обнаружения вторжений, таких как несанкционированное проникновение в здание. Она выведена на пульт централизованного наблюдения в Росгвардии.

В ЦРБ установлена охранная сигнализация «С2000-Пирон-Ш». Она позволяет организовать простую, и надёжную защиту медицинского учреждения. Система моментально оповестит Росгвардию по радиосвязи, в случае вторжения злоумышленников в здание.

К данной сигнализации можно подключить проводные и беспроводные датчики. Для поддержания работоспособности проводных датчиков при отключении электричества установлен блок резервного питания.

К сигнализации подключены следующие датчики:

1. Датчик разбития стекла - срабатывает на звук разбития стекла. Он анализирует частотный диапазон и может различать звуки разбития стекла разных типов (обычное, армированное, стеклопакет).

2. Магнито-контактный датчик или датчик открытия. Установлен на дверях и окнах. При открытии окна или двери происходит удаление магнита, установленного на подвижной части от геркона, размещенного в неподвижной части, что вызывает его срабатывание.

Кроме того, дополнительно у охранника установлена тревожная кнопка. Благодаря которой осуществляется вызов оперативной группы Росгвардии можно с помощью тревожной кнопки, выполненной в виде брелока. Брелоки имеют глав, врач и зам. глав. врач. Связь с блоком управления тревожной кнопки, расположенной так же у охранника, осуществляется при помощи радиосвязи.

В ходе производственной практики было принято участие в обслуживании систем видеонаблюдения. Одна из камер на территории ЦРБ перестала функционировать.

В процессе поиска неисправности был обнаружен оборванный кабель RCA с питанием. После обнаружения неисправности было принято решение заменить RCA кабель.

В ходе производственной практики было проведено участие в монтаже и обслуживании видеокамеры на въезде. Для начала была выявлена причина поломки, а затем предприняты действия для устранения поломки. А именно был поврежден кабель RCA с питанием. После замены кабеля, камера заработала.

Таким образом, в процессе практики были изучены технические средства, присутствующие на территории ЦРБ, а также были получены практические навыки в эксплуатации технических и инженерных средств охраны.

Также были изучены технические характеристики видеокамер, установленных в ЦРБ. Во время обслуживания видеокамер был заменен RCA кабель с питанием.

3. УЧАСТИЕ В МОНТАЖЕ, ОБСЛУЖИВАНИИ И ЭКСПЛУАТАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО СЪЁМА И УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

ч

Для того чтобы иметь возможность обнаружить несанкционированный съем или утечку данных, необходимо регулярно проводить аудит доступа.

Аудит доступа к данным должен входить в функционал средств информационной безопасности. Помимо этого, программы, которые компания решила использовать, должны включать следующие опции:

- аутентификация и идентификация при входе в систему;
- контроль допуска к информации для пользователей разных уровней;
- обнаружение и регистрация попыток НСД;
- контроль работоспособности используемых систем защиты информации;
- обеспечение безопасности во время профилактических или ремонтных работ.

Маршрутизатор является обязательным средством, но не единственным. Серьезную дополнительную защиту от утечек данных по каналам ПЭМИН, несанкционированного взаимодействия приложений, способных передавать информацию друг другу и обеспечивать ее утечку по менее контролируемым каналам, от проникновения в информационную систему организации вредоносных программ дает межсетевой экран. В больнице установлен межсетевой экран от компании «Kaspersky».

Для выполнения идентификации и аутентификации пользователей необходимы технические средства, с помощью которых производится двухступенчатое определение личности и подлинности полномочий пользователя. Необходимо учитывать, что в ходе идентификации необязательно устанавливается личность. Возможно принятие любого

другого идентификатора, установленного службой безопасности. После этого следует аутентификация - пользователь вводит пароль.

В ходе производственной практики выполнялись работы по настройке межсетевого экрана.

Необходимо в разделе интерфейс установить «Защиту паролем», чтобы запретить доступ к антивирусу, изменению настроек, завершению его работы или удалению (рис. 1).

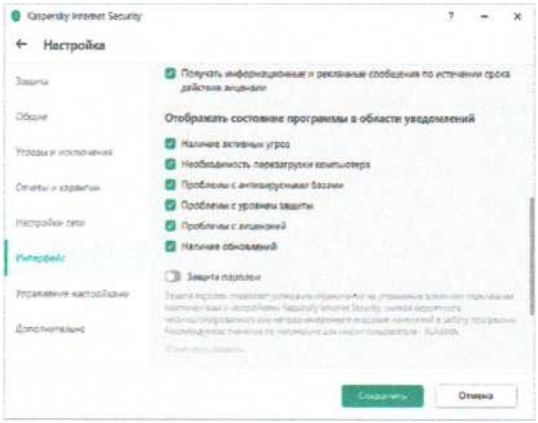


Рис. 1. Установка защиты паролем

Следует перейти в меню защита и зайти в файловый антивирус (рис. 2).

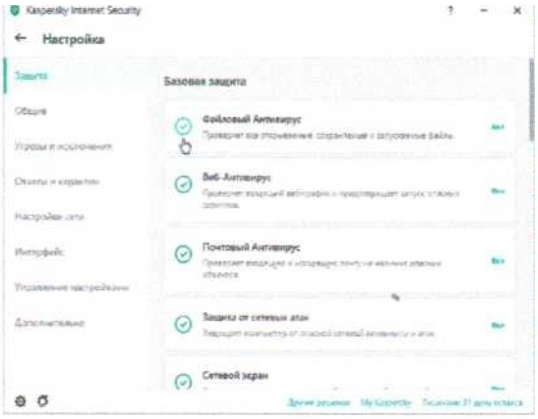


Рис. 2. Файловый антивирус

Необходимо установить уровень безопасности на «Высокий», после установки следует зайти в расширенные настройки (рис. 3).

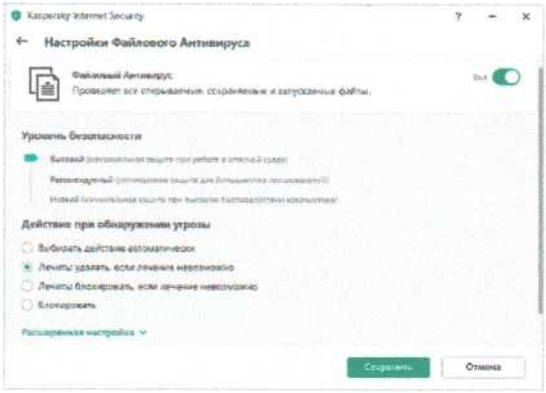


Рис. 3. Настройки файлового антивируса

*

Следует установить галочки «Проверка составных файлов», «Проверять архивы» и «Проверять дистрибутивы», отметив в каждом пункте «Все». Чуть ниже в «Режиме проверки» отметить «При доступе и изменении» и сохранить параметры (рис .4).

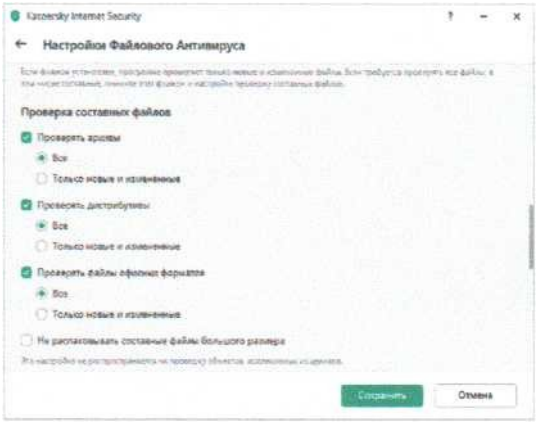


Рис. 4. Проверка составных файлов

Необходимо перейти в раздел «Настройка» и выбрать «Веб-Антивирус» (рис. 5).

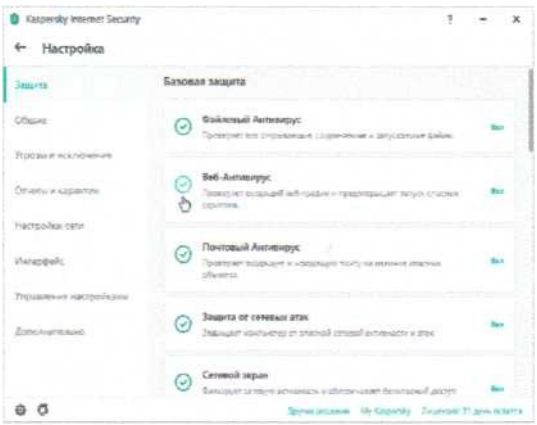


Рис. 5. Настройка Веб-Антивируса

Требуется установить уровень безопасности на «Высокий», а действия при обнаружении «Запрещать загрузку» (рис. 6).

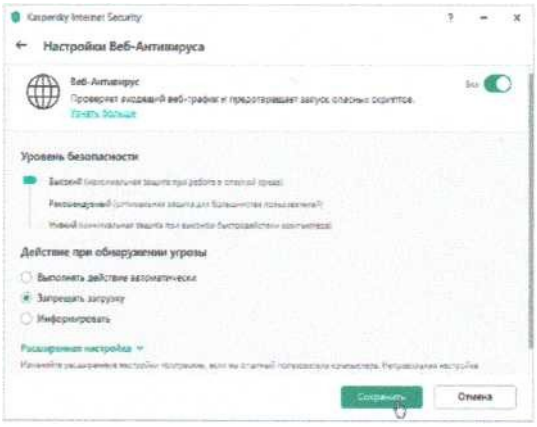


Рис. 6. Установка уровня безопасности

Необходимо зайти в «Сетевой Экран» (рис. 7).

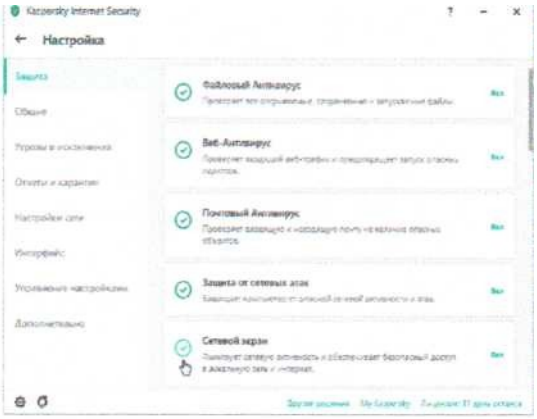


Рис. 7. Сетевой экран

После чего включить «Запрещать передачу пароля в интернете в незащищенном виде и показывать уведомления» (рис. 8).

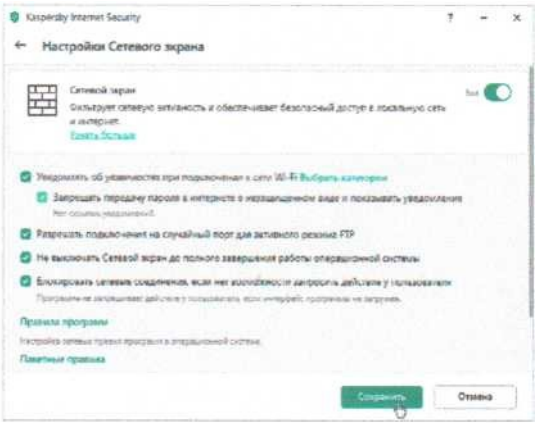


Рис. 8. Настройка Сетевого экрана

Затем вернуться в настройки и перейти в раздел «Защита от сбора данных» (рис. 9).

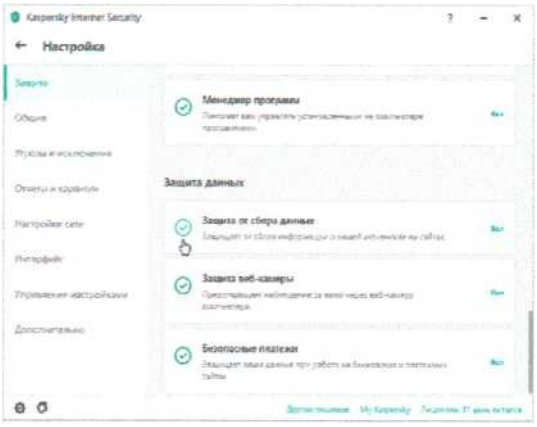


Рис. 9. Включение защиты от сбора данных

После чего требуется запретить сбор данных и сохранить (рис. 10).

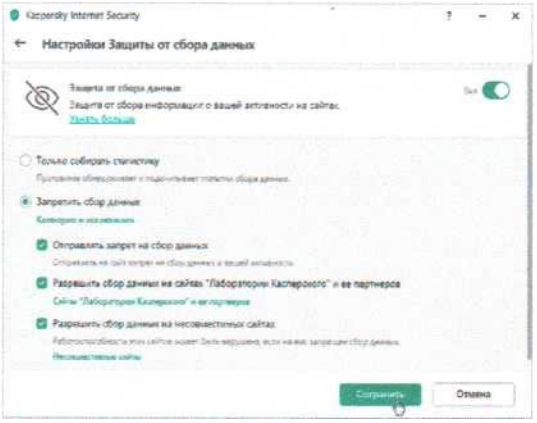


Рис. 10. Настройка Защиты от сбора данных

Необходимо перейти в раздел «Настройки Защиты веб-камеры» и запретить всем программам доступ к веб-камере (рис. 11).

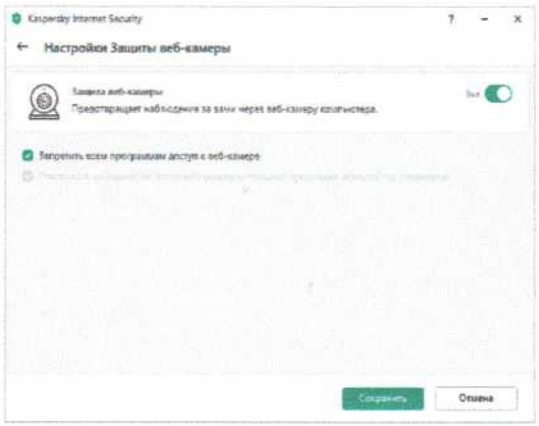


Рис. 11. Настройка Защиты веб-камеры

После следует вернуться в настройки и перейти в раздел «Настройки сети», затем включить параметры «Внедрять в трафик скрипт взаимодействия с веб-страницами», «Поддерживать работу DNS поверх HTTPS (DoH)», и «Контролировать все сетевые порты» (рис. 12).

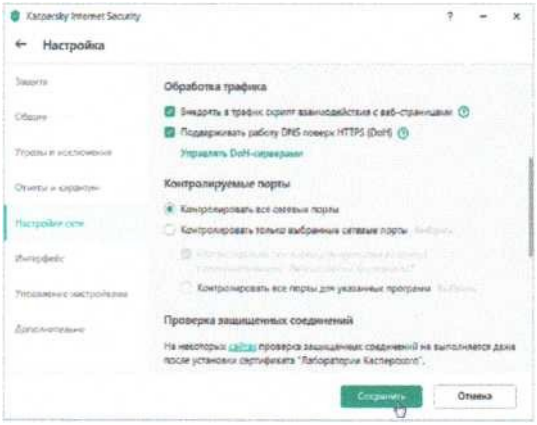


Рис. 12. Обработка трафика

Таким образом, в ходе производственной практики была проведена работа с аудитом безопасности, а именно ознакомление с его назначением, возможностями и функциональными особенностями.

Так же производилась настройка межсетевого экрана «Kaspersky Internet Security», а конкретно настройка защиты от сбора данных, а также производились настройки сети.

4. ПРИМЕНЕНИЕ НОРМАТИВНО ПРАВОВЫХ АКТОВ, НОРМАТИВНЫХ МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

Законы в области обеспечения защиты информации представляют собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности. *

Основные законы РФ на которые опираются и базируются концепция (доктрина) информационной безопасности.

В соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее - Закон об информации), в широком понимании информация подразделяется на общедоступную информацию и информацию ограниченного доступа. В зависимости от порядка ее предоставления или распространения она подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Нормативное регулирование работы с информацией ограниченного доступа, устанавливаются только федеральными законами (ст. 5, п. 2 Закона об информации). Законодательно установлено, что информация ограниченного доступа может составлять государственную тайну или относиться к конфиденциальной информации.

149-ФЗ «Об информации, информационных технологиях и о защите информации» это главный закон об информации в России. Он определяет ключевые термины. Непосредственно на этот закон и эти определения нужно

ссылаться при составлении документов по информационной безопасности.

В 149-ФЗ указано, какая информация считается конфиденциальной, а какая общедоступной, когда и как можно ограничивать доступ к информации, как происходит обмен данными. Также конкретно здесь прописаны основные требования к защите информации, а так же ответственность за их нарушения.

В Законе об информации дается определение конфиденциальности информации, под которым понимается обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Ключевые моменты закона об информационной безопасности:

- нельзя собирать и распространять информацию о жизни человека без его согласия;

- все информационные технологии равнозначны — нельзя обязать компанию использовать какие-то конкретные технологии для создания информационной системы;

- есть информация, к которой нельзя ограничивать доступ, например сведения о состоянии окружающей среды;

- некоторую информацию распространять запрещено, например ту, которая пропагандирует насилие или нетерпимость;

*

- тот, кто хранит информацию, обязан ее защищать, например, предотвращать доступ к ней третьих лиц.

Приказ ФСТЭК России от 18 февраля 2013 г. N 21 включает в себя состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

- регистрация событий безопасности;

- антивирусная защита;

- обнаружение (предотвращение) вторжений;

- контроль (анализ) защищенности персональных данных;

- обеспечение целостности информационной системы и персональных данных;

- обеспечение доступности персональных данных;

- защита среды виртуализации;

- защита технических средств;

- защита информационной системы, ее средств, систем связи и передачи данных;

- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

- управление конфигурацией информационной системы и системы защиты персональных данных.

Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» установлены виды конфиденциальной информации. К ней относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г.

N 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

Секрет производства, то есть сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности.

Таким образом, в ходе производственной практики было произведено знакомство с нормативно правовыми актами, нормативными методическими документами по обеспечению защиты информации техническими средствами. Также были получены практические навыки в применении этой документации.

ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

В рамках прохождения производственной практики, были приобретены практические навыки и умения, путём непосредственного участия в деятельности Урюпинской ЦРБ. Эти навыки необходимы для дальнейшей работы по специальности.

Во время прохождения практики, были выполнены все поставленные задачи. Достигнута цель производственной практики, а именно, освоение необходимых компетенций, систематизацией, обобщением и углубление

теоретических знаний.

Базой для данной производственной практики является государственное бюджетное учреждение здравоохранения «Урюпинская центральная районная больница».

В больнице применена функциональная организационная структура.

В ходе производственной практики было проведено знакомство, с отделением в котором были изучены технические средства защиты информации Урюпинской ЦРБ.

Также были получены практические навыки в обслуживание пожарно-охранной системы сигнализации, а именно обнаружение неисправных датчиков задымления и замена их на новые. Помимо, этого было проведено обслуживание, замена и установка новых дверных замков.

Помимо этого, во время производственной практики было принято участие в плановом обслуживании пожарной сигнализации. Осуществлялась проверка всей системы в целом. В процессе проверки было выявлено, что один из датчиков не реагирует на искусственное задымление и не посылает сигнал на пульт управления. После чего было неисправный датчик был заменен на исправный.

В процессе практики были изучены технические средства, присутствующие на территории ЦРБ, а также были получены практические навыки в эксплуатации технических и инженерных средств охраны.

Также были изучены технические характеристики видеокамер, установленных в ЦРБ. Во время обслуживания видеокамер был заменен RCA кабель с питанием.

В ходе производственной практики была проведена работа с аудитом безопасности, а именно ознакомление с его назначением, возможностями и функциональными особенностями.

Так же производилась настройка межсетевого экрана «Kaspersky Internet Security», а конкретно настройка защиты от сбора данных, а также * производились настройки сети.

В ходе производственной практики было произведено знакомство с

нормативно правовыми актами, нормативными методическими документами по обеспечению защиты информации техническими средствами. Также были получены практические навыки в применении этой документации.

В результате прохождения производственной практики в ГБУЗ «Урюпинская центральная районная больница имени В.Ф. Жогова» с 8 по 21 декабря 2022 г. были закреплены теоретические знания, получены новые необходимые практические и профессиональные навыки и умения.

В качестве предложений рекомендуется установить дополнительные камеры в связи с тем, что некоторые участки территории нечетко просматриваются. Также установить фонари по всему периметру ЦРБ для улучшения просмотра территории в ночное время. А также, для усиления физической защиты по периметру установить на забор колючую проволоку.

17.12.2022 Г.И.А. Бескоровайный

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. —URL: https://urait.ru/bcode/512861.

2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239.

3. Чернова, Е. В. Информационная безопасность человека: учебное

пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. —URL: https://urait.ru/bcode/51844L.

4. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5- 534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. —URL: https://urait.ru/bcode/519614.

5. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518005.

6. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : x
Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. —URL: https://urait.ru/bcode/519079.

7. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518006.

8. Внуков, А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023.— 161 с.— (Высшее образование).— ISBN 978-5-534-07248-8. — Текст :

электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268.

9. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023.— 312 с.— (Высшее образование).— ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300.

10. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин.— Москва : Издательство Юрайт, 2023.— 312 с.— (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст :
электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519364.

11. Проектирование информационных систем: учебник и практикум для вузов / под общей редакцией Д. В. Чистова. — Москва : Издательство Юрайт, 2022. — 258 с. — (Высшее образование). — ISBN 978-5-534-00492-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489307.

12. Шульц, В. Л. Безопасность информационных сетей: учебник для вузов / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко ; под редакцией В. Л. Шульца. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 585 с. — (Высшее образование). — ISBN 978-5-534-12368-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518878

13. Милешко, Л. П. Технические средства и методы защиты информации учебное пособие для вузов / Л. П. Милешко. — Москва: Издательство Юрайт, 2023. — 99 с. — (Высшее образование). — ISBN 978-5-534-13764-4. — Текст : электронный // Образовательная платформа Юрайт

[сайт]. — URL: https://urait.ru/bcode/519758.

14. Чикилева, Л. С. Системы и сети передачи информации: учебник и практикум для среднего профессионального образования / Л. С. Чикилева, Е. Л. Авдеева, Л. С. Есина. — Москва : Издательство Юрайт, 2023. — 185 с. — (Профессиональное образование). — ISBN 978-5-534-14043-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519882.

15. Сафиуллин, Р. К. Технические средства защиты информации: учебное пособие для вузов / Р. К. Сафиуллин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 146 с. — (Высшее образование). — ISBN 978-5-534-06491-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. —URL: https://urait.ru/bcode/514996.

16. Соколова, В. В. Основы информационной безопасности: учебное пособие для среднего профессионального образования / В. В. Соколова. — Москва: Издательство Юрайт, 2023. — 175 с. — (Профессиональное образование). — ISBN 978-5-534-10680-0. — Текст : электронный *И* \ Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518008.

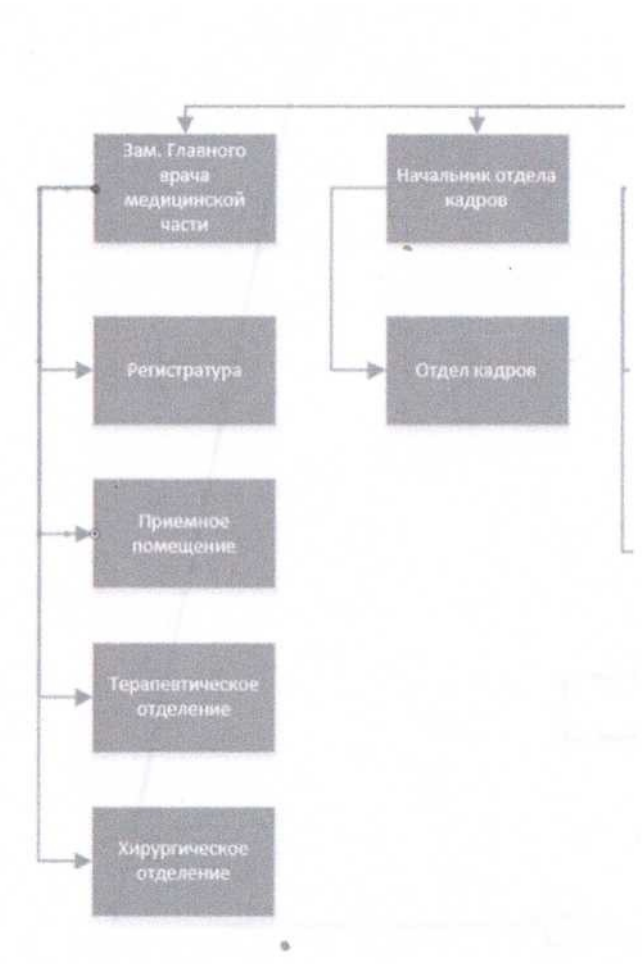
17. Защита и обработка конфиденциальных документовъ и практикум для вузов / Т. М. Беляева [и др.]; под редакцией В. Д. Элькина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 402 с. — (Высшее образование). — ISBN 978-5-534-10684-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ni/bcode/512072.

18. Илякова, И. Е. Инженерно-техническая защита информации: учебное пособие для вузов / И. Е. Илякова, С. Э. Майкова. — 2-е изд. — Москва : Издательство Юрайт, 2023. — 185 с. — (Высшее образование). — ISBN 978-5-534-14708-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. —URL: https://urait.ru/bcode/520280.

19. Средства защиты от несанкционированного съема: учебник и практикум для бакалавриата и магистратуры / Ю. Д. Романова [и др.];

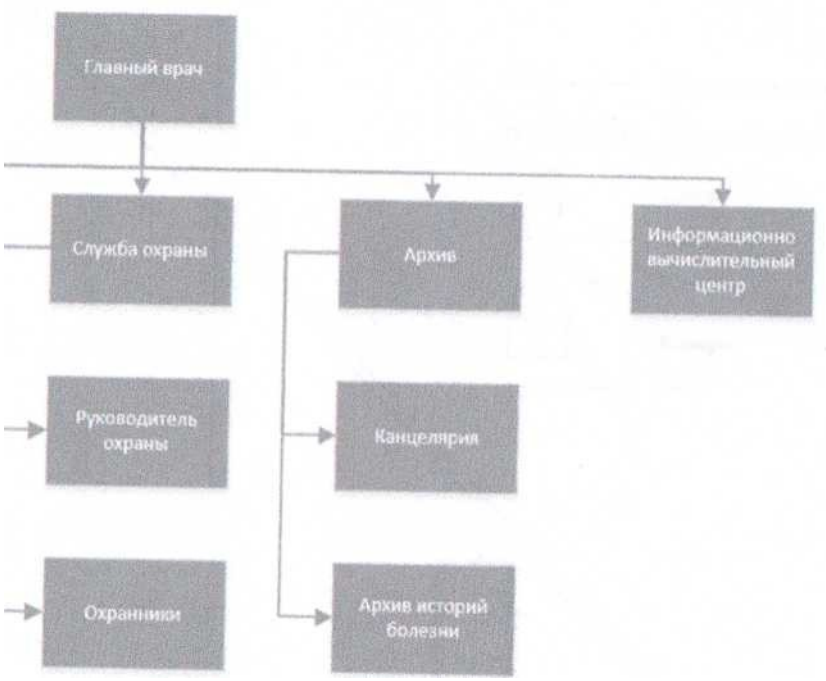
ответственный редактор Ю. Д. Романова. — Москва : Издательство Юрайт, 2022. — 495 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-9916-3770-1. — Текст : электронный *И* Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/508139.

20. Корниенко, К. И. Информационная защита в государственных учреждениях: учебное пособие для среднего профессионального образования/ К. И. Корниенко.— Москва: Издательство Юрайт, 2023.— 224 с. — (Профессиональное образование). — ISBN 978-5-534-14901-2. — Текст : электронный *И* Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519986


Зам. Главного врача медицинской части
Начальник отдела кадров
Регистратура
Отдел кадров
Приемное помещение
Терапевтическое отделение
Хирургическое отделение

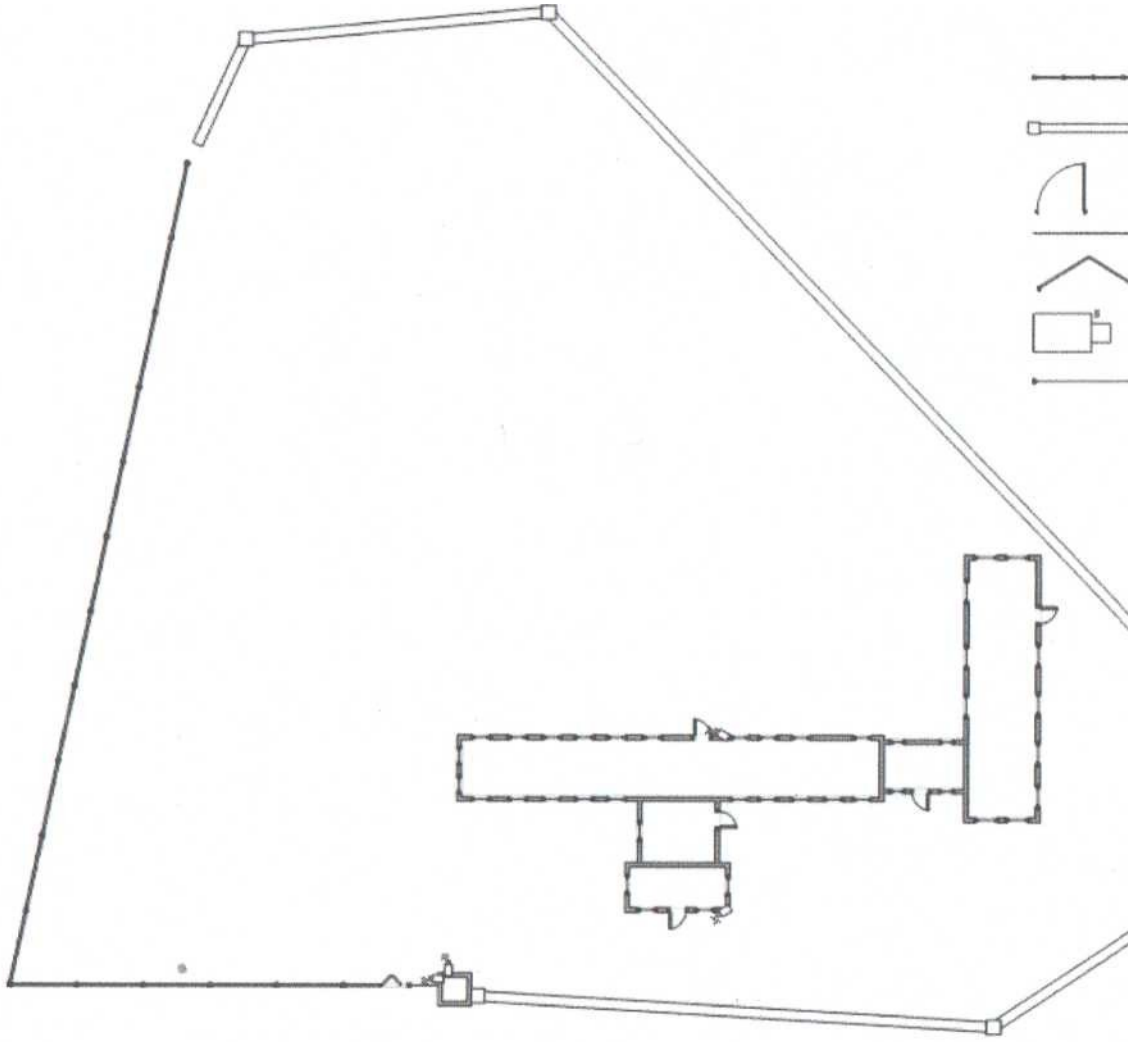
ПРИЛОЖЕНИЕ 1

Организационная структура Урюпинской ЦРБ



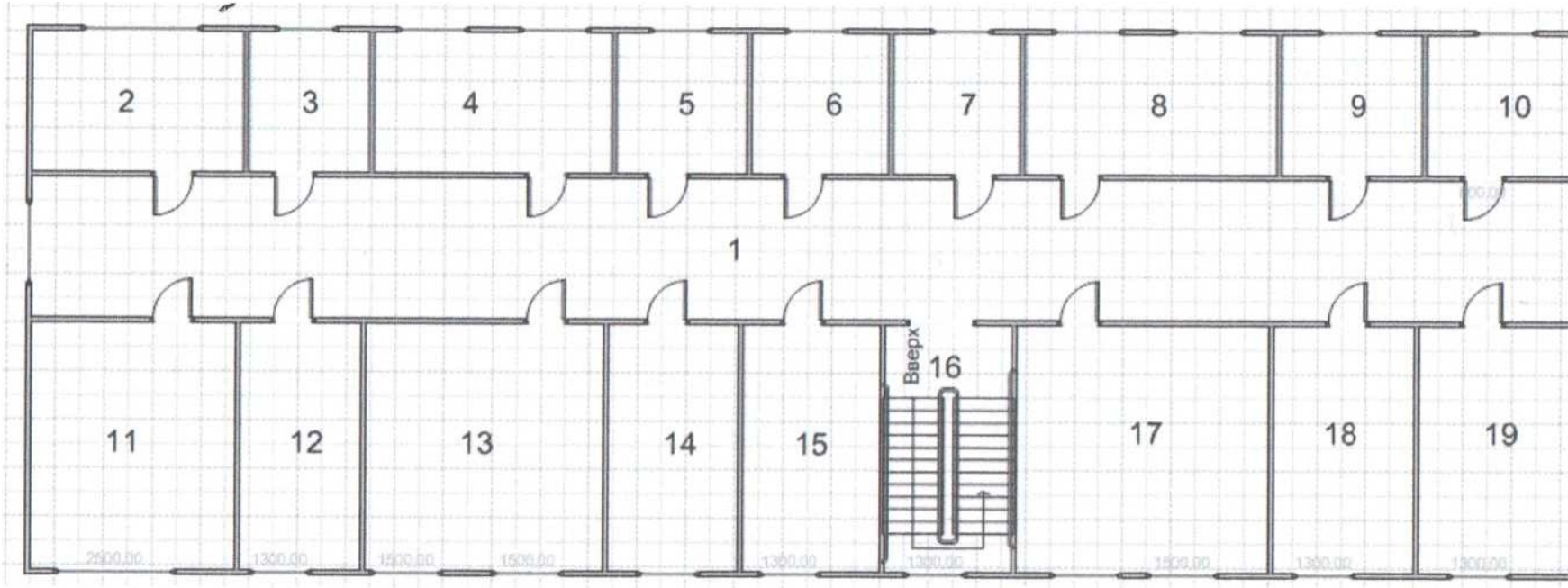
ПРИЛОЖЕНИЕ 2

Расположение камер на территории ЦРБ



ПРИЛОЖЕНИЕ 3

Схема отделения травматологии



1. коридор
2. палата №1
3. кабинет ст. медсестры
4. палата №2
5. душевая
6. санузел
7. санузел
8. палата №3
9. палата №4
10. процедурный кабинет
11. палата №5
12. кабинет зав. отделения
13. палата №6
14. перевязочная
15. сестринская
16. лестничная клетка
17. раздаточная
18. столовая
19. палата №7

-ч L