Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

«Проект разработка политики информационной безопасности персональных данных частной клиники»

Студент: Марчук К.С.

ФИТ 3 курс 1 группа

Преподаватель: Копыток Д.В.

Минск 2020

Оглавление

[Введение 3](#_Toc3551204)

[1 Структура бизнес-компании 4](#_Toc3551205)

[2 Объекты защиты 6](#_Toc3551206)

[3 Оценка рисков и угроз 7](#_Toc3551207)

[4 Меры защиты 9](#_Toc3551208)

[4.1 Меры информационного уровня 9](#_Toc3551209)

[4.2 Меры технического уровня 9](#_Toc3551210)

[4.3 Меры режимного уровня 10](#_Toc3551211)

[4.4 Общие принципы современных методов защиты информации 10](#_Toc3551212)

[Вывод 12](#_Toc3551213)

[Список литературы 13](#_Toc3551214)

# Введение

Современный этап общемирового развития характеризуется возрастающей ролью информационной сферы. Превращаясь в системообразующий фактор жизни общества, она все более активно влияет на состояние политической, экономической, оборонной, личной, имущественной и других составляющих безопасности.

Сотрудничество и соперничество государств и организаций из традиционной материальной сферы все более отчетливо смещаются в информационную область*.*

Беларусь стоит перед необходимостью осознания и принятия вызова, связанного с вступлением человечества в эпоху формирования мирового информационного сообщества. Современные информационные технологии существенно меняют не только структуру отношений, но и образ жизни людей, их мышление, механизмы функционирования семьи, общественных институтов, органов власти. Они становятся действенным фактором развития личности и общества. В то же время широкое распространение некоторых информационных технологий сопровождается появлением ряда новых угроз конституционным правам и свободам граждан, формированию здоровья, полноценной духовной жизни. Эти технологии уже используются для целей экономики, торговли, рекламы, политической борьбы, оказывая порой разрушительное воздействие на психику людей, в особенности подростков.

Информационное воздействие становится главным рычагом управления людьми, все больше заменяя физическое воздействие, тысячелетиями считавшееся непременным средством управления.

Вот почему одним из основных элементов национальной, общественной и личной безопасности становится информационная безопасность. В современном мире информационная безопасность – жизненно необходимое условие обеспечения интересов человека, общества и государства.

Одной из основных структур частных клиник и подобных интернет-сервисов является организация работы с пользователями. В связи с этим возникает необходимость осуществлять комплекс операция по защите персональных данных (в будущем ПД).

Под информационной безопасностью ПД понимается защищенность персональных данных и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПД) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПД, а также к прогнозированию и предотвращению таких воздействий.

# 1 Структура бизнес-компании

Онлайн сервис частной клиники предполагает удобную удаленную работу с записью на обследование в клинику, онлайн мониторингом анализов и рекомендаций лечащего врача, наличие форума для обсуждения проблем, некоторую полезную информацию.

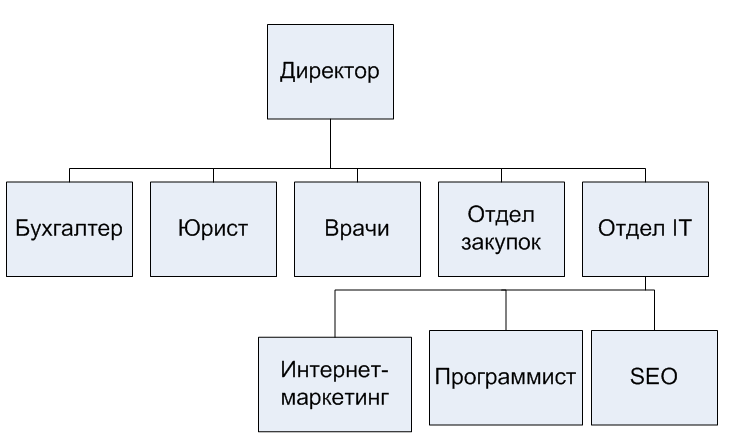


Рисунок 1.1 – Структура работников сервиса

Для управления и администрирования частной клиники нужна некоторая иерархическая структура работников, где каждый будет выполнять свою роль и обязанности. Она может быть представлена следующими кадрами:

1. Директор.

Именно он разрабатывает стратегию развития проекта. Директор набирает штат, определяет обязанности каждого сотрудника и контролирует выполнение работы. От этого зависит эффективность работы частной клиники. Руководитель также занимается вопросами, связанными с финансовой стороной проекта, определяет ассортимент продукции, разрабатывает новые бизнес-программы. Директор должен владеть информацией об IT-технологиях, о SEO, о WEB-дизайне, а также понимать важность работы контент-менеджеров и логистов.

2. Бухгалтер.

Контролирует бухгалтерский учет совершения предоставляемых услуг, ведет необходимую документацию, предоставляет финансовый отчет в налоговую службу. Проверка товарных и кассовых отчетов. Проведение инвентаризаций. Составление статистической отчетности, учет БСО. Сопровождение операционной деятельности торговых объектов.

3. Юрист.

Если часто возникают конфликтные ситуации с клиентами, услуги юриста помогут при заключении различных договоров. Правовая экспертиза хозяйственных договоров по текущей деятельности компании. Претензионная, исковая работа, представление интересов организации в судебных инстанциях, а также в других государственных и общественных организациях при рассмотрении правовых вопросов, ведение судебных дел. Контроль исполнения судебных решений. Юридическое сопровождение бизнес-процессов компании, предоставление консультаций, правовых заключений. Корпоративное право (оформление протоколов, решений и т.д.)

4. Программист.

Является разработчиком интернет-сервиса. Программист разрабатывает базу данных пользователей, а также информационную систему(ИС) управления базой данных. Не только участвует в развитии и поддержке сервисов частной клиники. Именно он реализует информационную систему персональных данных, поэтому он обязан ответственно отнестись к разработке, тестированию, нужным доработкам и поддержанию работоспособности ИС.

5. Отдел IT.

Занимается настройкой серверов, удаленных компьютеров. Являются администраторами баз персональных данных. В основном, защита конфиденциальности ложится на их плечи. Специалисты этой службы могут заниматься настройками бухгалтерской ИС.

6. Отдел продвижения.

SEO-специалисты занимаются увеличением релевантного трафика и, как следствие, увеличением продаж. SEO-направление представлено сотрудниками, которые знают товар и целевую аудиторию, а также умеют писать интересные, качественные тексты. Специалист SEO-продвижения может вести корпоративный блог. Аудит, анализ сайта и его видимости для поисковых машин. Анализ конкурентов. Разработка и проведение мероприятий по внутренней и [внешней оптимизации ресурса](https://seo.artox-media.ru/wiki/vneshnyaya-optimizaciya-saita.html). Реализация мероприятий по продвижению сайта. Улучшение ресурса с целью [привлечения клиентов](https://seo.artox-media.ru/wiki/kak-privlech-potencialnyh-klientov.html) и увеличения конверсии из посетителей в покупателей. Отслеживание изменений в алгоритмах поисковых машин и адаптация сайта к ним. Предоставление необходимых данных, позволяющих составить мнение о результатах продвижения в поисковых системах. К таким данным можно отнести позиции ресурса в поисковых системах по ключевым для него запросам, источники трафика, анализ поведения посетителей на сайте, изменение количества продаж с сайта.

7. Отдел интернет-маркетинга.

Маркетологи анализируют внешнюю среду сайта, планируют стратегию развития частной клиники, трафика, объемы посещений и бюджет. Контролируют эффективность работы сайта – обеспечивают удобство работы с интерфейсом, следят за качеством контента. Опытный маркетолог управляет перемещениями посетителей по ресурсу и использует особые приемы, способствующие привлечению клиентов. Подготовка и реализация годового и квартального плана маркетинговых активностей. Подготовка и исполнение годового бюджета маркетинга в разрезе торговых марок. Планирование и анализ продаж по каналам(аптечные сети, детская розница, косметическая розница). Организация event- и промомероприятий, семинаров, выставок, проведение презентаций. Составление отчетности по брендам. Разработка матриц по выкладке товара в торговых точках и контроль. Организация работы с подрядчиками: договор, контроль исполнения (+фотоотчеты), документооборот, контроль оплат. Организация проведения акций в сетях, а также контроль за исполнением. Работа с подрядчиками по продвижению сайтов и групп в соцсетях.

8. Отдел закупок.

Если **частная клиника имеет большой клиентский оборот**, актуальным становится планирование закупок некоторых материалов для функционирования. Это необходимо для того, чтобы обеспечить конкурентное преимущество. В обязанности закупщиков также входят переговоры с поставщиками, направленные на снижение цен и другие выгодные для частных клиник условия.

9. Штат врачей и медработников.

Именно они являются основными работниками частной клиники, выполняющие главную лечебную работу. В их обязанности входит прием пациентов в клинике в выходные и праздничные дни. Ведение медицинской документации.

# 2 Объекты защиты

Основными объектами защиты в частной клинике являются базы данных клиентов и вся интеллектуальная собственность сервиса.

Объекты информатизации – средства и системы информатизации, технические средства приема, хранения, передачи и обработки информации.

Предметом защиты информации в частной клинике являются носители информации, на которых зафиксированы, отображены защищаемые сведения

* + Личные дела клиентов в бумажном и электронном (база данных клиентов) виде;
  + личные дела работников в бумажном и электронном (база данных работников) виде;
  + обращения к услугам клиники физических лиц, журналы, ведомости, положения, инструкции, соглашения и обязательства о неразглашении, распоряжения, договоры, отчеты;
  + локальная сеть;
  + информация, относящаяся к защите ПД, включая ключевую, парольную аутентифицирующую информацию;
  + результаты научно-исследовательской деятельности работников компании.

# 3 Оценка рисков и угроз

Оценка рисков начала использоваться на атомных электростанциях Европы и Америки в начале 1960-х годов, а в последствии развивалась и применялась аэрокосмической инженерии, химической промышленности, охране окружающей среды, здравоохранении, спорте, развитии национальной экономики и многих других областях. В информационной безопасности методики оценки рисков появились с целью прогнозирования возможного ущерба, связанного с реализацией угроз, и соответственно оценки необходимого размера инвестиций на построение систем защиты информации.

Четкой методики количественного расчета величин рисков как не было, так и нет. Это связано в первую очередь с отсутствием достаточного объема статистических данных о вероятности реализации той или иной угрозы. В результате наибольшее распространение получила качественная оценка информационных рисков. Но как использовать результаты такой оценки? Как рассчитывать возможный ущерб и размер необходимых инвестиций для предотвращения реализации рисков?

До сих пор ведутся споры на тему оценки информационных рисков или экономического обоснования инвестиций в информационную безопасность. В настоящее время идет активное накопление данных, на основании которых можно было бы с приемлемой точностью определить вероятность реализации той или иной угрозы. К сожалению, имеющиеся справочники опираются на зарубежный опыт и потому с трудом применимы к российским реалиям.

Оценка рисков информационной безопасности имеет некоторые характеристики, такие как:

* + нелинейность;
  + сложность применения;
  + характеристики, обусловленные некоторыми ограничениями на использование традиционных моделей для проведения оценки рисков информационной безопасности.

Эти традиционные методы оценки несут массу субъективных проблем и неясностей, поэтому они более сложны в применении.

Информация может существовать в различных формах. Она может быть написана на бумаге, храниться в электронном виде, пересылаться по почте или с использованием электронных средств, транслироваться на экране или обсуждаться в разговоре.

Какие бы формы информация ни принимала, она всегда должна быть защищена соответствующим образом. Оценка рисков информационной безопасности, с точки зрения управления рисками, это анализ систематически подвергающихся угрозам и существующим уязвимостям информационных систем и технологий научными методами и средствами. Оценка потенциального ущерба в случае угрожающих событий проведена и выдвинуты контрмеры против угроз для предотвращения и урегулирования рисков информационной безопасности, а также контроль рисков на приемлемом уровне таким образом, чтобы максимально обеспечить безопасность информации.

Оценка рисков информационной безопасности состоит из трех основных этапов: идентификация угроз, идентификация уязвимостей, идентификация активов.

На основании оценивания рисков выбираются средства, обеспечивающие режим ИБ. Ресурсы, значимые для нормальной работы организации и имеющие определенную степень уязвимости, считаются подверженными риску, если по отношению к ним существует какая-либо угроза. При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для этих ресурсов.

В целях предотвращения несанкционированного доступа организации используют различные контрмеры для защиты своих активов. Но даже благодаря применению контрмер и управлению информационной безопасностью активы зачастую не в полной мере защищены от угроз из-за недостатка контроля. Таким образом, оценка рисков является одним из важнейших шагов в управлении рисками информационной безопасности. На практике оценка рисков информационной безопасности является довольно сложным и полным неопределенностей процессом. Неопределенности, существующие в процессе оценки, являются основным фактором, влияющим на эффективность оценки риска информационной безопасности. Поэтому они должны быть приняты во внимание при оценке рисков. Однако большинство существующих подходов имеют некоторые недостатки по обработке неопределённости в процессе оценки.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

Под актуальными угрозами безопасности понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать их уничтожение, изменение, блокирование, копирование, предоставление, распространение и т.п.

Актуальными при обработке ПД в частной клинике, являются следующие угрозы:

* + Несанкционированного доступа к ПД лицами, обладающими полномочиями в ИС, в том числе в ходе ее создания, эксплуатации или технического обслуживания;
  + воздействия вредоносного кода, внешнего по отношению к информационной системе;
  + несанкционированного доступа к оставленным носителям персональных данных;
  + утраты носителей ПД;
  + несанкционированного доступа к ПД лицами, не обладающими полномочиями в ИС, с использованием уязвимостей:
  + в организации защиты ПД;
  + в программном обеспечении ИС;
  + в обеспечении защиты каналов передачи данных;
  + вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации;
  + хищение, физический вывод из строя технических средств;
  + внедрение деструктивных программ – вирусов, сетевых червей и пр.;
  + проникновение зловредных программ через интернет, электронную почту, гибкие диски, флэш-носители;
  + умышленное изменение используемого ПО для несанкционированного сбора защищаемой информации.

Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка политики безопасности требует учета специфики конкретных организаций.

# 4 Меры защиты

Исходя из анализа основных угроз и рисков, следует принять соответствующие меры защиты. Их можно разграничить на 3 логических уровня:

* + информационный уровень;
  + технический уровень;
  + режимный уровень.

# 4.1 Меры информационного уровня

Меры информационного уровня в основной своей части достигаются при использовании определенного ПО, предназначенного для мониторинга, фиксирования событий, настройки, криптографии и защиты интернет-сервиса. Они могут в себя включать следующие пункты:

* + Использование антивирусной защиты с базами последней версии;
  + установка защиты от DDoS атак;
  + проведение эффективной парольной защиты;
  + мониторинг входящего и исходящего трафика интернет-сервиса;
  + проверка исходного кода на наличие внедренного вредоносного кода в исходный;
  + разграничены права доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
  + обеспечение доверенной загрузки на техническое оборудование посредством настройки соответствующего ПО;
  + защита информационной системы, ее средств и систем связи и передачи данных;
  + аутентификация пользователей и работников сервиса строго по их аутентификационным данным;
  + использовать шифрование данных;
  + обнаружение фактов несанкционированного доступа к персональным данным и принятие соответствующих мер;
  + использование лицензионного программного обеспечения;
  + восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
  + применение в необходимых случаях средств межсетевого экранирования, обнаружения вторжений, анализа защищенности;
  + использование средств криптографической защиты информации.

# 4.2 Меры технического уровня

Меры данного уровня реализуются с помощью физических аппаратных средств и мероприятий по поддержанию их работоспособности. Они могут включать следующие пункты:

* + Технические проверки аппаратных средств;
  + техническое обслуживание оборудования;
  + проведение контроля трафика сети на отдельных ее участках (сегментах);
  + проведение контроля состояния программного и информационного обеспечения компьютеров (состава и целостности программного обеспечения, корректности настроек и т.д.) и маршрутизаторов (маршрутных таблиц, фильтров, паролей);
  + обеспечение резервного копирования;
  + запрет несанкционированного доступа к оборудованию, различным средствам хранения данных и рабочие помещения.
  + проведение контроля за несанкционированными физическими подключениями системам.

# 4.3 Меры режимного уровня

Меры режимного уровня подразумевают поддержание внутреннего распорядка и могут быть представлены следующими пунктами:

* + Организация режима обеспечения безопасности помещений;
  + обеспечение сохранности носителей персональных данных;
  + повышение ответственности сотрудников за выполнение требований установленных режимов;
  + разграничение доступа и контроль за доступом в выделенные помещения;
  + назначение лица, ответственного за обеспечение безопасности ПД;
  + инструктаж и обучение персонала курсах в учебном центре.

# 4.4 Общие принципы современных методов защиты информации

Технологии защиты данных основываются на применении современных методов, которые предотвращают утечку информации и ее потерю. Сегодня используется шесть основных способов защиты:

* + Препятствие;
  + маскировка;
  + регламентация;
  + управление;
  + принуждение;
  + побуждение.

Все перечисленные методы нацелены на построение эффективной технологии защиты информации, при которой исключены потери по причине халатности и успешно отражаются разные виды угроз.

Препятствием – способ физической защиты информационных систем, благодаря которому злоумышленники не имеют возможность попасть на охраняемую территорию.

Маскировка – способы защиты информации, предусматривающие преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа.

Управление – способы защиты информации, при которых осуществляется управление над всеми компонентами информационной системы.

Регламентация – важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Принуждение – методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Если используются способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям, то речь идет о побуждении.

Таким образом, будут добавлены должностные обязанности сотрудников предприятия, а именно:

1. Директор.

Разработка политики безопасности. Директор определяет обязанности каждого сотрудника и контролирует выполнение регламента политики безопасности. От этого зависит эффективность созданной политики. Руководитель также занимается вопросами, связанными с финансовой стороной проекта, определяет меры и методы. Директор должен владеть информацией о применяемых технологиях, о юридической стороне вопроса, о новом регламенте компании, а также понимать важность данных мер.

2. Юрист.

Проверка политики безопасности предприятия на соответствие нормативным документам по защите ПД (например, ISO 27001). Правовая экспертиза выполнения норм и правил по текущей деятельности компании, изложенных в политике информационной безопасности.

3. Программист.

Является разработчиком интернет-сервиса. Программист разрабатывает базу данных пользователей, а также информационную систему(ИС) управления базой данных, которые должны быть обеспечены уровнями защиты в соответствии с политикой безопасности. Обеспечивает системы и каналы передачи данных шифрованием, создаёт методы защиты данных во время их обработки в системах и устраняет уязвимости в системе. Не только участвует в развитии и поддержке сервисов частной клиники. Именно он реализует информационную систему персональных данных, поэтому он обязан ответственно отнестись к разработке, тестированию, нужным доработкам и поддержанию работоспособности ИС.

4. Отдел IT.

Занимается настройкой серверов, удаленных компьютеров. Являются администраторами баз персональных данных. В основном, защита конфиденциальности ложится на их плечи. Специалисты этой службы могут заниматься настройками бухгалтерской ИС. Работа отдела по защите информации сводятся к трём основным задачам:

Конфиденциальность – обеспечение информацией только тех людей, которые уполномочены для получения такого доступа. Хранение и просмотр ценной информации только теми людьми, кто по своим служебным обязанностям и полномочиям предназначен для этого.

Целостность - поддержание целостности ценной и секретной информации означает, что она защищена от неправомочной модификации. Существуют множество типов информации, которые имеют ценность только тогда, когда мы можем гарантировать, что они правильные. Главная цель информационной политики информационной безопасности должна гарантировать, что информация не была повреждена, разрушена или изменена любым способом.

Пригодность – обеспечение того, чтобы информация и информационные системы были доступны и готовы к эксплуатации всегда, как только они потребовались. В этом случае, основная цель информационной политики безопасности должна быть гарантия, что информация всегда доступна и поддерживается в пригодном состоянии.

6. Отдел интернет-маркетинга.

Маркетологи обязаны соблюдать требования политики безопасности о неразглашении ПД.

7. Штат врачей и медработников.

Основной ресурс компании, на который ориентирована политика информационной безопасности. Их дополнительные обязанности:

Исключить:

* + Несанкционированный доступ к ПД лицами, обладающими полномочиями в ИС, в том числе в ходе ее создания, эксплуатации или технического обслуживания;
  + Скачивание непроверенного или нелицензионного ПО и проникновение зловредных программ через интернет, электронную почту, гибкие диски, флэш-носители;
  + Несанкционированный доступ к оставленным носителям персональных данных;
  + Утрату носителей ПД;
  + Хищение, физический вывод из строя технических средств;
  + Несанкционированный доступ к ПД лицами, не обладающими полномочиями в ИС, с использованием уязвимостей:

Штат врачей и медработников обязуется соблюдать требования по эксплуатации средств криптографической защиты информации;

# Вывод

Под политикой безопасности организации понимают совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности является тем средством, с помощью которого реализуется деятельность в компьютерной информационной системе организации. Вообще политика безопасности определяется используемой компьютерной средой и отражает специфические потребности организации.

На политике безопасности не стоит экономить, так как затраты на восстановление бизнеса в результате негативных действий могут стоить гораздо больше ее защиты. Политика безопасности должна быть разработана так, чтобы её взлом стоил дороже, чем сама информация.

Таким образом, в ходе работы был произведен анализ потенциальных уязвимостей в системе и разработаны способы их защиты. Каждому предприятию присущи сходные уязвимости и, как следствие, способы их предотвращения. Грамотное проектирование политики безопасности позволяет не только защитить данные, но и обеспечить их сохранность в будущем.

# Список литературы

1. Бракович, А. И. конспект лекций по предмету основы защиты информации – 2017
2. Политика информационной безопасности – Введение [Электронный ресурс] – Режим доступа: <http://www.xliby.ru/tehnicheskie_nauki/informacionnaja_bezopasnost_cheloveka_i_obshestva_uchebnoe_posobie/p1.php>
3. Структура интернет-сервиса [Электронный ресурс] – Режим доступа: <http://brief-obozrenie.ru/security-biznes/bezopasnost-biznesa/cvoy-biznes/organizacionnaya-struktura-internet-magazina/>
4. Меры защиты информации [Электронный ресурс] – Режим доступа: <https://www.cryptopro.ru/service/zashchita-is-pd>
5. Основные принципы современных мер защиты информации [Электронный ресурс] – Режим доступа: <http://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi>
6. Козлова Е. А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации // Молодой ученый. — 2013. — №5. — С. 154-161. — [Электронный ресурс] – Режим доступа: <https://moluch.ru/archive/52/6967/>