Учреждение образования “БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ”

Практическая работа №3 «**Разработка политики информационной безопасности бизнес-компании**»

Выполнил:

студент 2 курса, 7 группы

Бобрович Глеб Сергеевич

Проверил:

Барковский Евгений Валерьевич

Оглавление

[**Введение** 3](#_Toc103892056)

[**Структура больницы** 5](#_Toc103892057)

[**Оценка рисков** 6](#_Toc103892058)

[**Разработка мер защиты** 6](#_Toc103892059)

[**Вывод** 9](#_Toc103892060)

# **Введение**

В век информационных технологий мы имеем выбор хранения информации, таким образом мы можем хранить её:

* На бумажных носителях;
* На различных цифровых носителях.

Каждый день мы используем устройства, из которых мы считываем довольно большие объёмы информации, либо заносим туда свою информацию, которая может быть сугубо личной, либо открытой для всех, так же это относится и к компании. Так что главной задачей для всех является защита своей информации, что является довольно сложной задачей в связи с развитием технологий и появлением глобальной сети. Модели угроз и нарушителей должны быть основным инструментом менеджмента нашей организации при развертывании, поддержании и совершенствовании системы обеспечения информационной безопасности организации.

Информационные ресурсы в современном обществе являются наиболее значимыми, но при этом, очень уязвимыми т.к. механизм их распространения становится все более гибким и количество возможностей их передачи растет. В связи с этим информационная безопасность — одно из важнейших условий функционирования любой структуры, будь то государственное учреждение или частное предприятие.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение вопроса об разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации.

Пока не существует формальных методов нейтрализации угроз безопасности информации. По этой причине разработка мер по защите информации должна производиться на основе знаний и опыта соответствующих специалистов (каждый член бригады, выполняющей лабораторную работу, является специалистом - экспертом по защите конфиденциальной информации). Однако в интересах минимизации ошибок процесс разработки должен соответствовать следующим рекомендациям.

Разработку мер защиты информации целесообразно начинать с угроз, имеющих максимальное значение; далее - с меньшей угрозой, и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы. Такой подход гарантирует, что даже при малых ресурсах хватит ресурсов для предотвращения наиболее значимых угроз. Для каждой угрозы разрабатываются меры (способы и средства) по защите информации.

Существуют различные подходы к оценке рисков. Выбор под хода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Разработанная и утвержденная документация должна включать в себя следующие разделы:

- перечисление объектов, в отношении которых устанавливается режим информационной безопасности, их ранжирование по значимости и требуемой степени защиты;

- описания технологий, применяемых для обеспечения сохранности информации;

- перечень действующих и потенциальных угроз информационной безопасности, описание степени их серьезности и реализуемости;

- описание внешних и внутренних субъектов, которые могут стать источниками потенциальной угрозы;

- описание понятия инцидента информационной безопасности, процедур уведомления о его возникновении;

- описание применяемых организационных мер, действий сотрудников компании по обеспечению информационной безопасности;

- описание выбранной политики защиты от вирусных атак, программ-вредителей, возможных действий хакеров;

- описание системы резервного копирования важных данных, ее периодичности, моделей хранения – на дисках, на посторонних серверах;

- описание того, в каком порядке будут проводиться аварийные и восстановительные работы при повреждении аппаратной части в случае пожара, проблем с электросвязью или по иным причинам, повлекшим за собой гибель компьютеров, носителей информации или самих баз данных;

- план мероприятий по постоянному поддержанию готовности системы к работе, ее обновлению при изменении правил сертификации или степени значимости угроз.

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения:

- антропогенные,

- техногенные,

- естественные (природные).

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре Главпочтамта могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются:

- сотрудники организации;

- программное обеспечение;

- аппаратные средства.

К информационным угрозам относятся:

- несанкционированный доступ к информационным ресурсам;

- незаконное копирование данных в информационных системах;

- противозаконный сбор и использование информации;

- использование информационного оружия.

К программным угрозам относятся:

- использование ошибок и «дыр» в ПО;

- компьютерные вирусы и вредоносные программы;

К физическим угрозам относятся:

- уничтожение или разрушение средств обработки информации и связи;

# **Структура больницы**

Не существует строго утвержденной структуры политики информационной безопасности больниц, но многие организации следуют рекомендациям стандартов. Размер политики может варьироваться от 11 до 200 и более страниц, это зависит от того, как именно принято решение отражать существенные моменты. Часто многие регламенты и методики реализации процессов выносятся в документы второго и третьего уровней. Такие документы предназначены, в отличие от информационной политики больниц, для конкретных подразделений, а не для отдельных сотрудников. В документе отражаются средства и методы защиты информационной безопасности, призванные обеспечить конфиденциальность персональных данных, врачебной тайны. Отражаются и меры, направленные на защиту технических средств, составляющих периметр информационной безопасности больницы.

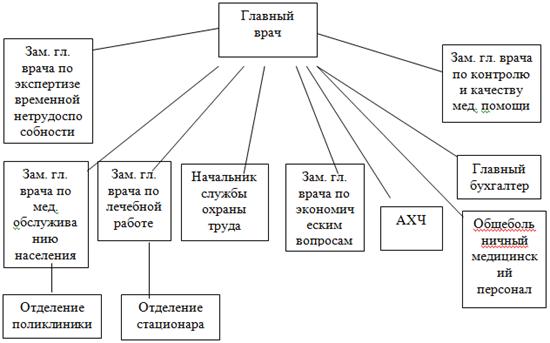


Рисунок 1 – Структура больницы

Таким образом, процесс разработки политики информационной безопасности больницы делится на следующие этапы:

* постановка задачи на высшем уровне управления;
* распределение поручений и сфер ответственности;
* сбор необходимой информации с причастных подразделений;
* разработка проекта;
* внесение средств, требуемых для разработки и внедрения проекта, в бюджет организации и подразделений;
* согласование проекта всеми подразделениями;
* утверждение документа;
* внедрение документа;
* аудит качества его действия;
* доработка документа.

Весь процесс может занять несколько месяцев.

Объектом защиты в контексте данной Политики являются информационные ресурсы больницы, обрабатываемые в информационных системах и ее функциональных подсистемах, содержащие сведения, доступ к которым ограничен, и используемые в процессах сбора, обработки, накопления, хранения и распространения в границах информационных систем больницы. Основными объектами защиты больницы являются:

- информационные ресурсы больницы ограниченного распространения, в том числе содержащие конфиденциальные сведения;

- программные информационные ресурсы больницы, а именно: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

- физические информационные ресурсы больницы:

- компьютерное аппаратное обеспечение всех видов;

- носители информации всех видов (электронные, бумажные и прочие);

- все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным аппаратным и программным обеспечением;

- технические сервисы больницы (отопление, освещение, энергоснабжение, кондиционирование воздуха и т.п.)

# **Оценка рисков**

Для оценки рисков при составлении и последующем пересмотре организационно-распорядительных документов необходимо систематически рассматривать следующие аспекты:

- ущерб, который может нанести деятельности больницы серьезное нарушение информационной безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации;

- реальную вероятность такого нарушения защиты в свете превалирующих угроз и средств контроля.

# **Разработка мер защиты**

Целями обработки Оператором персональных данных являются:

- обеспечение соблюдения законодательства Республики Беларусь;

- осуществление своей деятельности в соответствии с учредительными документами Оператора;

- обработка сообщений и запросов, поступивших от субъекта персональных данных;

- осуществление коммуникаций с субъектами персональных данных;

- ведение кадровой работы и организации учета работников Оператора, в том числе привлечении и отбор кандидатов для работы у Оператора;

- ведение индивидуального (персонифицированного) учета застрахованных лиц;

- ведение воинского учета;

- ведение бухгалтерского и налогового учета;

- начисление и перечисление заработной платы, назначение и выплата пособий;

- заполнение и передача в государственные органы и иные уполномоченные организации требуемых форм отчетности;

- обработка персональных данных в целях назначения пенсий;

- осуществление гражданско-правовых отношений;

- предоставление субъектам персональных данных информации о деятельности Оператора, о разработке операторами новых сайтов и серверов;

- отправка субъектам персональных данных уведомлений, коммерческих предложений, сообщений рекламно-информационного характера;

- проведение Оператором акций, опросов, интервью, тестирования на сайтах и серверах Оператора;

- оценка и анализ работы серверов Оператора, контроль и улучшение качества сервисов Оператора;

- информирование о работе сайтов Оператора;

- регистрация и обслуживание аккаунтов на сайтах и в серверах Оператора;

- осуществление пропускного режима;

- выполнение иных обязанностей (полномочий), предусмотренных законодательством.

Персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством.

# **Вывод**

Вся ответственность по разработке информационной безопасности лежит на вас. Конечно самому разрабатывать вам ее не придется, но никогда не стоит о ней забывать. Стоит изучить некоторые документы, обратиться за помощью к специалистам или поинтересоваться у других владельцев больниц о проблемах, с которыми они столкнулись.

Важно помнить, что прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот.

Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Опыт показывает, что для достижения удачных решений по защите информации компаний необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведёт к нарушению защищённости.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надёжности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надёжности технических средств.