МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическая работа №3**

по дисциплине «Основы защиты информации»

на тему: Разработка политики информационной безопасности больницы

Выполнил студентка 2 курса 5 группы специальность ПОИТ Буранко В.Д.

(Ф.И.О.)

Преподаватель ассистент Берников Владислав Олегович

(Ф.И.О.)

Цель:Разработать проект политики информационной безопасности больницы.

# **Введение**

Что такое информационная безопасность?

Информационная безопасность — это различные меры по защите информации от посторонних лиц. В доцифровую эпоху для защиты информации люди запирали важные документы в сейфы, нанимали охранников и шифровали свои сообщения на бумаге.

Сейчас чаще защищают не бумажную, а цифровую информацию, но меры, по сути, остались теми же: специалисты по информационной безопасности создают защищенные пространства (виртуальные «сейфы»), устанавливают защитное ПО вроде антивирусов («нанимают охранников») и используют криптографические методы для шифрования цифровой информации.

Однако цифровую информацию тоже нужно защищать не только виртуально, но и физически. Антивирус не поможет, если посторонний похитит сам сервер с важными данными. Поэтому их ставят в охраняемые помещения.

За что отвечает информационная безопасность

Она отвечает за три вещи: конфиденциальность, целостность и доступность информации. В концепции информационной безопасности их называют принципами информационной безопасности.

Конфиденциальность означает, что доступ к информации есть только у того, кто имеет на это право. Например, ваш пароль от электронной почты знаете только вы, и только вы можете читать свои письма. Если кто-то узнает пароль или другим способом получит доступ в почтовый ящик, конфиденциальность будет нарушена.

Целостность означает, что информация сохраняется в полном объеме и не изменяется без ведома владельца. Например, на вашей электронной почте хранятся письма. Если злоумышленник удалит некоторые или изменит текст отдельных писем, то это нарушит целостность.

Доступность означает, что тот, кто имеет право на доступ к информации, может ее получить. Например, вы в любой момент можете войти в свою электронную почту. Если хакеры атакуют серверы, почта будет недоступна, это нарушит доступность.

Какая бывает информация и как ее защищают

Информация бывает общедоступная и конфиденциальная. К общедоступной имеет доступ любой человек, к конфиденциальной — только отдельные лица.

Может показаться, что защищать общедоступную информацию не надо. Но на общедоступную информацию не распространяется только принцип конфиденциальности — она должна оставаться целостностной и доступной. Поэтому информационная безопасность занимается и общедоступной информацией.

Например, возьмем интернет-магазин. Карточки товаров, статьи в блоге, контакты продавца — все это общедоступная информация, ее может просматривать любой. Но интернет-магазин все равно нужно защищать, чтобы никто не нарушил его работу, например, не изменил важную информацию в карточках товаров или не «уронил» его сайт.

Главная задача информационной безопасности в IT и не только — защита конфиденциальной информации. Если доступ к ней получит посторонний, это приведет к неприятным последствиям: краже денег, потере прибыли компании, нарушению конституционных прав человека и другим неприятностям.

Основные виды конфиденциальной информации

Персональные данные. Информация о конкретном человеке: ФИО, паспортные данные, номер телефона, физиологические особенности, семейное положение и другие данные. В России действует 152-ФЗ — закон, который обязывает охранять эту информацию. Мы подробно рассказывали об этом в статье «Как выполнить 152-ФЗ о защите персональных данных и что с вами будет, если его не соблюдать».

Тот, кто работает с персональными данными, обязан защищать их и не передавать третьим лицам. Информация о клиентах и сотрудниках относится как раз к персональным данным.

Коммерческая тайна. Внутренняя информация о работе компании: технологиях, методах управления, клиентской базе. Если эти данные станут известны посторонним, компания может потерять прибыль.

Компания сама решает, что считать коммерческой тайной, а что выставлять на всеобщее обозрение. При этом не вся информация может быть коммерческой тайной — например, нельзя скрывать имена учредителей юрлица, условия труда или факты нарушения законов. Подробнее о коммерческой тайне рассказывает закон 98-ФЗ.

Профессиональная тайна. Сюда относятся врачебная, нотариальная, адвокатская и другие виды тайны, относящиеся к профессиональной деятельности. С ней связано сразу несколько законов.

Служебная тайна. Информация, которая известна отдельным службам, например, налоговой или ЗАГСу. Эти данные обычно хранят государственные органы, они отвечают за их защиту и предоставляют только по запросу.

Государственная тайна. Сюда относят военные сведения, данные разведки, информацию о состоянии экономики, науки и техники государства, его внешней политики. Эти данные самые конфиденциальные — к безопасности информационных систем, в которых хранится такая информация, предъявляют самые строгие требования.

Если ваша компания хранит персональные данные, коммерческую или профессиональную тайну, то эти данные нужно защищать особым образом. Для этого необходимо ограничить доступ к ней посторонним лицам — установить уровни доступа и пароли, поставить защитное ПО, настроить шифрование.

**Структура больницы**

Все подразделения больницы можно разделить на 2 большие группы:

- Лечебно-диагностическая;

- административно-хозяйственная.

Лечебно-диагностическая часть включает в себя:

- приемное отделение;

- специализированные лечебные отделения (терапевтические, хирургические, гинекологическое и т. д.);

- оперблок;

- диагностические лаборатории (клиническую¸ биохимическую, цитологическую, иммунологическую и пр.);

- диагностические отделения и кабинеты.

Административно-хозяйственная часть включает в себя:

- кабинеты главного врача и его заместителей,

- канцелярию;

- бухгалтерию;

- пищеблок;

- прачечную;

- аптеку;

- стерилизационное отделение;

- отделение переливания крови;

- котельную.

При поступлении в стационар, в большинстве случаев пациент проходит через приемное отделение. Правильно организованная и четко осуществляемая работа приемного отделения во многом определяет работу стационара в целом. Качество оказания помощи, правильность и скорость сортировки пациентов формируют у них первое (а зачастую, и основное) впечатление от стационара и его сотрудников.

Приемное отделение состоит из следующих помещений:

· Вестибюль (зал ожидания для родственников и сопровождающих);

· Диспетчерский пост (регистратура);

· Смотровые кабинеты, в т.ч. специализированные (гинекологический, хирургический, травматологический и др.);

· Санитарный пропускник;

· Изоляторы для инфекционных и для социально опасных больных;

· Процедурная и перевязочная;

· Реанимационный зал («шоковая» палата);

· Лаборатория и рентгеновский кабинет;

· Туалеты;

· Вспомогательные помещения (комнаты персонала, кладовки, камера хранения вещей госпитализированных пациентов и др.).



# **Оценка рисков**

1. Определить ценность информационных активов в денежном выражении.

2. Оценить в количественном выражении потенциальный ущерб от реализации каждой угрозы в отношении каждого информационного актива.

Следует получить ответы на вопросы «Какую часть от стоимости актива составит ущерб от реализации каждой угрозы?», «Какова стоимость ущерба в денежном выражении от единичного инцидента при реализации данной угрозы к данному активу?».

3. Определить вероятность реализации каждой из угроз ИБ.

Для этого можно использовать статистические данные, опросы сотрудников и заинтересованных лиц. В процессе определения вероятности рассчитать частоту возникновения инцидентов, связанных с реализацией рассматриваемой угрозы ИБ за контрольный период (например, за один год).

4. Определить общий потенциальный ущерб от каждой угрозы в отношении каждого актива за контрольный период (за один год).

Значение рассчитывается путем умножения разового ущерба от реализации угрозы на частоту реализации угрозы.

5. Провести анализ полученных данных по ущербу для каждой угрозы.

По каждой угрозе необходимо принять решение: принять риск, снизить риск либо перенести риск.

Принять риск — значит осознать его, смириться с его возможностью и продолжить действовать как прежде. Применимо для угроз с малым ущербом и малой вероятностью возникновения.

Снизить риск — значит ввести дополнительные меры и средства защиты, провести обучение персонала и т д. То есть провести намеренную работу по снижению риска. При этом необходимо произвести количественную оценку эффективности дополнительных мер и средств защиты. Все затраты, которые несет организация, начиная от закупки средств защиты до ввода в эксплуатацию (включая установку, настройку, обучение, сопровождение и проч.), не должны превышать размера ущерба от реализации угрозы.

Перенести риск — значит переложить последствия от реализации риска на третье лицо, например с помощью страхования.

В результате количественной оценки рисков должны быть определены:

ценность активов в денежном выражении;

полный список всех угроз ИБ с ущербом от разового инцидента по каждой угрозе;

-частота реализации каждой угрозы;

-потенциальный ущерб от каждой угрозы;

-рекомендуемые меры безопасности, контрмеры и действия по каждой угрозе. Основными объектами защиты в медицинском учреждении являются:

- персонал (так как эти лица допущены к работе с охраняемой законом информацией (медицинская тайна, персональные данные) либо имеют доступ в помещения, где эта информация обрабатывается).

- объекты информатизации - средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний, заседаний и переговоров с пациентами;

Медицинская тайна (сведения о пациентах, состоянии их здоровья, результатах исследований);

Персональные данные работников (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия, уровень квалификации, доход, наличие судимостей и некоторая другая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника).

- документированная информация, регламентирующая статус учреждения, права, обязанности и ответственность его работников (Устав, журнал регистрации, учредительный договор, положение о деятельности, положения о структурных подразделениях, должностные инструкции работников)

- материальные носители охраняемой законом информации (личные дела работников, личные дела пациентов, электронные базы данных работников и пациентов, бумажные носители и электронные варианты приказов, постановлений, планов, договоров, отчетов, составляющих коммерческую тайну)

- средства защиты информации (Интернет-шлюз, система сигнализации и др.)

- технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации (личные дела бывших пациентов)

# Предметом защиты информации в мед. учреждении являются носители информации, на которых зафиксированы, отображены защищаемые сведения:

# - Личные дела пациентов в бумажном и электронном (база данных пациентов) виде;

# - Личные дела работников в бумажном и электронном виде;

# - Приказы, постановления, положения, инструкции, соглашения и обязательства о неразглашении, распоряжения, договоры, планы, отчеты, ведомость ознакомления с Положением о конфиденциальной информации и другие документы, в бумажном и электронном виде.

# Документы, которые имеют конфиденциальный характер и требующие зашиты

# **Разработка мер защиты**

Клиники, медицинские центры, другие учреждения здравоохранения сталкиваются с большим количеством персональных данных как сотрудников, так и клиентов. Многие документы попадают в категорию врачебной тайны. Поэтому информационная безопасность в медицине переходит на новый уровень.

Медучреждения переходят на электронный документооборот, автоматизируется ведение электронного учета или медицинских карт пациентов. Нельзя сказать, что вопросом оптимизации регистратур или безопасности баз данных заинтересовались в системе здравоохранения только сейчас. Впервые хранить документацию, используя компьютер, предложил Николай Амосов (знаменитый советский хирург). С развитием информационных технологий ускорился и переход медучреждений на новый уровень обработки и хранения персональных данных.

Для организации эффективной защиты конфиденциальной информации необходимо разработать программу, которая должна позволить достигать следующие цели:

- обеспечить обращение сведений, содержащих различные виды тайн, в заданной сфере;

- предотвратить кражу и утечку, а так же любую порчу конфиденциальной информации;

- документировать процесс защиты тайны, чтобы в случае попыток незаконного завладения любой нежелательной информацией для учреждения можно было защитить свои права юридически и наказать нарушителя.

Планируемые мероприятия должны:

- способствовать достижению определенных задач, соответствовать общему замыслу;

- являться оптимальными.

Не должны:

- противоречить законам, требованиям руководителя организации;

- дублировать другие действия.

Правовая защита - специальные правовые правила, процедуры и мероприятия, создаваемые в целях обеспечения информационной безопасности предприятия.

Уголовно-правовые нормы по своему содержанию являются, с одной стороны, запрещающими, то есть они под страхом применения мер уголовного наказания запрещают гражданам нарушать свои обязанности и совершать преступления, а с другой стороны, они обязывают соответствующие органы государства (ФСБ, МВД, прокуратуру) привлечь лиц, виновных в совершении преступления, к уголовной ответственности.

Кроме того, нарушения режима секретности, правил сохранения тайны, не являющиеся преступлением, могут повлечь ответственность материального, дисциплинарного или административного характера в соответствии с действующими нормативными актами: отстранение от работы, связанной с секретами, или перевод на другую работу, менее оплачиваемую и тоже не связанную с засекреченной информацией.

Организационная защита - регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, использующей нанесение ущерба.

Организационную защиту обеспечивает:

- Организация режима охраны, работы с кадрами, документами;

- Использование технических средств безопасности;

- Использование информационно-аналитической работы по выявлению угроз.

Организационные меры по защите информации предусматривают, прежде всего, подбор и расстановку кадров, которые будут осуществлять мероприятия по защите информации, обучение сотрудников правилам защиты засекреченной информации, осуществление на практике принципов и методов защиты информации. информация защита безопасность надежность

Инженерно-техническая защита - использование различных технических средств для обеспечения защиты конфиденциальной информации. Инженерно-техническая защита использует такие средства как:

- Физические - устройства, инженерные сооружения, организационные меры, исключающие или затрудняющие проникновение к источникам конфиденциальной информации (системы ограждения, системы контроля доступа, запирающие устройства и хранилища);

- Аппаратные - устройства, защищающие от утечки, разглашения и от технических средств промышленного шпионажа

- Программные средства.

# **Вывод**

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 кампаний 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.