Учреждение образования

«Белорусский государственный технологический университет»

**Отчет к лабораторной работе №1**

ТЕМА «РАЗРАБОТКА И ВНЕДРЕНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ПОЛИКЛИНИКИ»

Выполнил:

Студент 3 курса 5 группы ФИТ

Древотень Евгений Владимирович

**Цель работы**: приобретение практических навыков разработки и внедрения эффективной политики информационной безопасности организации или учреждения на примере поликлиники.

**Задачи:**

1. Научиться выделять и классифицировать особенности информационной или информационно-вычислительной системы (ИВС) поликлиники как объекта защиты.
2. Овладеть навыками принятия обоснованных решений по организационному и правовому регулированию проблем, относящихся к состоянию безопасности ИВС, обеспечению необходимого уровня защиты информации в ИВС.
3. Овладеть основными приемами анализа угроз информационной безопасности ИВС.
4. Научиться выявлять все возможные угрозы и их источники информационной безопасности в поликлинике, анализировать и оценивать собранные данные.
5. Разработать концепцию, основные элементы политики безопасности для поликлиники.
6. Разработать мероприятия по внедрению предложенной Вами политики безопасности.
7. Результаты выполнения лабораторной работы оформить в виде описания разработанной политики безопасности, а также плана мероприятий по ее реализации.

**Введение**

Необходимо разрабатывать политику информационной безопасности потому, что сейчас идёт постиндустриальное общество, где информация – наивысшая ценность. При любом виде представления и хранения информации её возможно потерять, повредить, украсть или получить несанкционированный доступ к ней.

Миллионы лет развития человека в целом, антропосоциогенез в частности, привели общество к текущему состоянию, что человек вечно пытается несмотря на чужие жизни получить хотя бы мнимую минимальную власть и богатство, украв, повредив, утратив, продав или подсмотрев конфиденциальную информацию, то есть доступ к которой должен быть только у определённого круга лиц, а у прочих доступа к ней не должно быть.

Ежедневно миллиарды людей создают и потребляют колоссальные объёмы данных. При этом большая часть информации – конфиденциальная. Информация может быть конфиденциальной в рамках одного человека, семьи, компании, группы компаний, государства и т.п. Для обеспечения уверенности, что информация будет конфиденциальна и целостна, вводится политика безопасности.

Политика безопасности — совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации.

Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа высокоуровневой политики, поддерживаемого конкретными документами специализированных политик и процедур безопасности. Высокоуровневая политика безопасности должна периодически пересматриваться, гарантируя тем самым учет текущих потребностей организации. Документ политики составляют таким образом, чтобы политика была относительно независимой от конкретных технологий, в этом случае документ не потребуется изменять слишком часто.

Политика информационной безопасности (ПИБ) организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

Информационная (информационно-вычислительная) система – организационно упорядоченная совокупность документов, технических средств и информационных технологий, реализующая информационные (информационно-вычислительные) процессы.

Информационные процессы – процессы сбора, накопления, хранения, обработки (переработки), передачи и использования информации.

Информационные ресурсы – отдельные документы или массивы документов в информационных системах.

Объект – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

Субъект – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

Доступ – специальный тип взаимодействия между объектом и субъектом, в результате которого создается поток информации от одного к другому.

Атака – попытка несанкционированного преодоления защиты системы.

Несанкционированный доступ (НСД) – доступ к информации, устройствам ее хранения и обработки, а также к каналам передачи, реализуемый без ведома (санкции) владельца и нарушающий тем самым установленные правила доступа.

Защита информации – организационные, правовые, программно-технические и иные меры по предотвращению угроз информационной безопасности и устранению их последствий.

Безопасность информации – защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Безопасность любого ресурса информационной системы складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности, также могут быть включены другие, такие как аутентичность, подотчетность, надежность; или иначе: информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности информации или средств ее обработки:

* конфиденциальность (англ. confidentiality) компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия;
* целостность (англ. integrity) компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права; целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени;
* доступность (англ. availability) компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

В случае, когда нарушения информационной безопасности чреваты тяжелыми последствиями, базовый уровень требований к режиму информационной безопасности является недостаточным. Для того, чтобы сформулировать дополнительные требования, необходимо:

* определить ценность информационных ресурсов;
* к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы – в нашем случае поликлиники;
* оценить вероятности угроз;
* определить уровень уязвимости ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

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.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

Для эффективной организации системы информационной безопасности целесообразно разработать аварийные планы. Они необходимы на случай восстановления информационных систем при возникновении форс-мажорных обстоятельств: аварий, катастроф и т. д.

1. **Описание структуры поликлиники**

Цели разработки политики информационной безопасности поликлиники:

1. защита конфиденциальности информации о пациентах;
2. защита конфиденциальности информации о персонале;
3. защита инфраструктуры;
4. улучшение управления рисками.

Задачи разработки ПИБ поликлиники:

1. создание и поддержка политики безопасности;
2. обеспечение безопасного хранения данных;
3. управление доступом к информации;
4. обучение персонала;
5. регулярное обновление систем безопасности.

В классической поликлинике структура дифференцирована преимущественно по профессиональному направлению работников с медицинским образованием и в общем случае имеет следующий вид:

1. руководство поликлиники;
2. регистратура;
3. отделение профилактики;
4. лечебно-профилактические подразделения:

* терапевтические отделения;
* хирургические отделения;
* травматологическое отделение;
* офтальмологическое отделение;
* отоларингологическое отделение;
* неврологическое отделение;
* физиотерапевтическое отделение;
* кардиологический кабинет;
* ревматологический кабинет;
* эндокринологический кабинет;
* кабинет инфекциониста;
* отделение неотложной помощи;

1. вспомогательно-диагностические подразделения:

* рентгенологический кабинет;
* лаборатории;
* отделение функциональной диагностики;
* эндоскопический кабинет;
* кабинет для оформления медицинской документации;

1. хозяйственная часть;
2. система материально-технического обеспечения.

К объектам защиты медицинской информационной системы относят:

* сведения в базе данных;
* резервные и архивные копии сервера;
* целевые данные администратора и начальника.

К субъектам отнесём:

* работников учреждения;
* пациентов;
* серверы;
* терминалы.

Однако данная структура неочевидно отражает разделение особенностей ПИБ. Тогда рекомендуется обобщить структуру для явного определения особенностей ПИБ:

1. руководство поликлиники;
2. регистратура;
3. хозяйственная часть;
4. система материально-технического обеспечения;
5. персонал, принимающий, опрашивающий, исследующий пациентов.

Из этого уже относительно просто выделить структуру ИС организации (рисунок 1.1):

1. распределённая система хранения медицинских данных между поликлиниками и прочими учреждениями здравоохранения;
2. локальная база данных с медицинскими сведениями о пациентах, принимаемых в конкретной поликлинике;
3. терминалы для получения, внесения, изменения и удаления данных в базу данных учреждения, не имеющие своих локальных хранилищ данных, но потенциально обладающие дополнительным специализированным ПО для выполнения тех либо иных услуг, анализа получаемого биоматериала;
4. специализированное оборудование для предоставления услуг и анализа получаемого биоматериала;
5. локальные базы данных для ведения хозяйственной работы и материально-технического обеспечения;
6. терминалы для получения, внесения, изменения и удаления данных в базы данных учреждения, не имеющие своих локальных хранилищ данных, но обладающие дополнительным специализированным ПО для учёта материального обеспечения, информационного, ведения финансовых дел;
7. необязательный пункт, веб-приложение для получения информации об учреждении и заказе талонов на приём.



Рисунок 1.1 – Структура поликлиники

Цели поликлиники могут варьироваться от учреждения к учреждению, но их можно обобщить в следующие пункты:

* обеспечение доступа населения к качественным медицинским услугам;
* предотвращение развития заболеваний и поддержание здоровья пациентов;
* диагностика и лечение заболеваний;
* координация медицинской помощи;
* оказание психологической помощи;
* организация профилактических и лечебных мероприятий.

Задачи поликлиники нацелены на реализацию целей и включают:

* проведение медицинских осмотров и консультаций;
* проведение диагностических и лабораторных исследований;
* проведение профилактических мероприятий;
* лечение пациентов;
* ведение медицинской документации.

**2. Оценка рисков для информационных ресурсов**

Фактор, воздействующий на ИВС, – это явление, действие или процесс, результатом которых может быть утечка, искажение, уничтожение данных, блокировка доступа к ним, повреждение или уничтожение системы защиты.

Все многообразие дестабилизирующих факторов можно разделить на два класса: внутренние и внешние.

Внутренние дестабилизирующие факторы влияют:

1) на программные средства (ПС):

* некорректный исходный алгоритм;
* неправильно запрограммированный исходный алгоритм (первичные ошибки);

2) на аппаратные средства (АС):

* системные ошибки при постановке задачи проектирования;
* отклонения от технологии изготовления комплектующих изделий и АС в целом;
* нарушение режима эксплуатации, вызванное внутренним состоянием АС.

Внешние дестабилизирующие факторы влияют:

1) на программные средства:

* неквалифицированные пользователи;
* несанкционированный доступ к ПС с целью модификации кода;

2) на аппаратные средства:

* внешние климатические условия;
* электромагнитные и ионизирующие помехи;
* перебои в электроснабжении;
* недостаточная квалификация обслуживающего персонала.

Все многообразие потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.

Искусственные угрозы – это угрозы, вызванные деятельностью человека.

Преднамеренные угрозы – угрозы, выполняемые лицами со злым умыслом, например угрозы хакерских атак, получения вредоносного ПО и социальной инженерии.

Непреднамеренные угрозы – угрозы, вызываемые лицами непроизвольно, без злого умысла, или природными явлениями, например т.н. «человеческий фактор» и землетрясения.

С учетом изложенного основные факторы (угрозы) ресурсам можно идентифицировать следующим образом:

1. действия внутреннего или внешнего злоумышленника (несанкционированный, в том числе удаленный доступ с целью нарушения работоспособности ИВС, кражи, удаления или модификации информации, несанкционированного распространения материальных носителей за пределами организации);
2. наблюдение за источниками информации;
3. подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов;
4. перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений;
5. разглашение информации компетентными людьми;
6. утеря носителей информации;
7. несанкционированное распространение информации через поля и электрические сигналы, случайно возникшие в аппаратуре;
8. воздействие стихийных сил (наводнения, пожары и т. п.);
9. сбои и отказы в аппаратуре сбора, обработки и передачи информации;
10. отказы системы электроснабжения;
11. воздействие мощных электромагнитных и электрических помех (промышленных, в том числе излучение от магнитно-резонансной томографии, и природных).

При оценивании рисков учитываются:

* ценность ресурсов;
* оценка значимости угроз;
* эффективность существующих и планируемых средств защиты.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:

* количественными (например, стоимостными);
* качественными (могут быть построены на использовании таких понятий, как «умеренный» или «чрезвычайно опасный»);
* их комбинацией.

Тогда составим таблицу условной численной шкалы для оценки ущерба поликлинике от НСД (таблица 2.1).

Таблица 2.1 – Условная шкала для оценки ущерба поликлинике от НСД

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб поликлинике |
| 1 | Ущерб от атаки есть, но он незначителен, основные операции и положение поликлиники на рынке не затронуты |
| 2 | Финансовые операции и предоставление услуг не ведутся в течение некоторого времени, за это время поликлиника терпит убытки, но её положение на рынке и количество пациентов изменяются минимально |
| 3 | Значительные потери на рынке и в прибыли. От поликлиники уходит ощутимая часть пациентов |
| 4 | Потери очень значительны, поликлиника на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы |
| 5 | Поликлиника прекращает существование |

Вероятность того, что угроза реализуется, определяется на основе следующих факторов:

* привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* технические возможности угрозы, используемые при умышленном воздействии со стороны человека;
* вероятность того, что угроза реализуется;
* степень легкости, с которой уязвимость может быть использована.

Далее построим таблицу шкалы вероятности то, что угроза будет реализована (таблица 2.2).

Таблица 2.2 – Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

Далее можно создать таблицу рисков (табл. 1.3). На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем (порогом), например значением 0,5.

К основным угрозам ИБ поликлиники можно отнести копирование жёсткого диска, террористическая атака, утечка персональных данных, непреднамеренное искажение информации, несанкционированный доступ к информационным ресурсам, физический износ ИВС, природные катаклизмы, забастовка, отключение электроэнергии и заражение учреждения.

К естественным атакам ИВС поликлиники можно отнести заболевания и природные катаклизмы: пожары, землетрясения, штормы, магнитные бури.

К искусственным относятся кибератаки, вирусы, фишинг, нарушение безопасности сотрудниками (копирование данных и непреднамеренное искажение информации (НИИ), забастовки), НСД.

Из них преднамеренные – взлом, кибератаки, вирусы, фишинг, НСД, внутренние угрозы. Непреднамеренные – природные катаклизмы, непреднамеренное искажение информации, отключение электричества, физический износ оборудования.

К внутренним атакам можно отнести НСД, непреднамеренное искажение информации, слив информации сотрудниками, мошенничество со стороны сотрудников. К внешним – кибератаки, террористическая атака, вирусы, социальная инженерия, природные катаклизмы.

Далее проверяется каждая строка таблицы: превышен или не превышен порог для значения риска, связанного с анализируемой атакой? Если такое превышение имеет место, данная атака должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности (таблица 2.3).

Таблица 2.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (У\*В) |
| Копирование жесткого диска | 3 | 0,2 | 0,6 |
| Террористическая атака | 5 | 0 | 0 |
| Кибератака | 4 | 0,3 | 1,2 |
| Утечка персональных данных сотрудников или пациентов | 4 | 0,1 | 0,4 |
| Слив данных сотрудниками | 5 | 0,3 | 1,5 |
| Мошенничество сотрудниками | 2 | 0,4 | 0,8 |
| Социальная инженерия | 4 | 0,1 | 0,4 |
| НИИ | 4 | 0,3 | 1,2 |
| НСД | 2 | 0,5 | 1,0 |
| Фишинг | 1 | 0,3 | 0,3 |
| Физический износ ИВС | 2 | 0,2 | 0,4 |
| Землетрясения, наводнения, ураганы и прочие природные катаклизмы | 5 | 0,1 | 0,5 |
| Забастовка | 2 | 0,1 | 0,5 |
| Отключение электричества | 2 | 0,2 | 0,4 |
| Вирусы, бактерии и прочие виды заболевания (заражения) | 2 | 0,3 | 0,6 |
| Итого |  |  | 9,8 |

**3. Разработка мер защиты**

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

На основании политики безопасности строится программа безопасности, которая реализуется на процедурном и программно-техническом уровнях уровне.

К процедурному уровню относятся меры безопасности, реализуемые людьми.

Можно выделить следующие группы процедурных мер:

* управление персоналом;
* физическая защита;
* поддержание работоспособности;
* реагирование на нарушения режима безопасности;
* планирование восстановительных работ.

Управление персоналом заключается в выполнении следующих условий. Прежде всего для каждой должности должны быть определены квалификационные требования по ИБ. Также в должностные инструкции должны входить разделы, касающиеся ИБ. И каждого работника нужно научить мерам безопасности теоретически и на практике. Более того, необходимо полностью дифференцировать работу по должностям и предметным областям для минимизации возможности непреднамеренного искажения информации если работник другого отдела своевольно принял на себя работу другого работника другого отдела.

Меры физической защиты включают в себя защиту от утечки информации по техническим каналам, инженерные способы защиты и т.д. Например, обязательно требуется поставить дополнительные экраны в кабинетах рентгенологии из-за возможного повреждения данных по причине избыточного излучения и укрепить или спрятать оборудования и средства физической связи в кабинетах функциональной диагностики.

Поддержание работоспособности включает в себя создание инфраструктуры, включающий в себя как технические, так и процедурные регуляторы и способной обеспечить любой наперед заданный уровень работоспособности на всем протяжении жизненного цикла информационной системы.

Реагирование на нарушение режима безопасности может быть регламентировано в рамках отдельно взятой поликлиники.

Планирование восстановительных работ предполагает:

* слаженность действий персонала во время и после аварии;
* наличие заранее подготовленных резервных производственных площадок;
* официально утвержденную схему переноса на резервные площадки основных информационных ресурсов;
* схему возвращения к нормальному режиму работы.

Основой программно-технического уровня являются следующие механизмы безопасности:

* идентификация и аутентификация пользователей;
* управление доступом;
* протоколирование и аудит;
* криптография;
* экранирование.

Теперь рассмотрим теоретическую модель поликлиники для разработки модели безопасности. При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя части оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Поскольку в поликлиниках может розниться физическое обеспечение, то процедурные меры более подробно рассмотрены не будут из-за избыточности данной информации на фоне представленной выше.

С уровня программно-технического предлагаются следующие меры по обеспечению информационной безопасности:

* на терминальных устройствах не хранить какие-либо данные для минимизации потерь при копировании жёсткого диска устройства из кабинетов с приёмом пациентов;
* добавить охранников внутри и снаружи поликлиники для минимизации шанса успешной минимизации шанса террористического акта;
* укрепление защиты от внешних кибератак – минимизация данных в открытых базах данных, укрепление защиты локальной базы данных;
* инвестирование в систему укрепления защиты локальной и глобальной баз данных от несанкционированного доступа для минимизации ущерба от утечки персональных данных работников и/или пациентов и обнуления шанса несанкционированного доступа;
* увеличить HR отдел для общения с сотрудниками и исследованием их настроений – это позволит минимизировать шанс, что сотрудник начнёт сливать данные, мошенничать, бастовать, а также минимизирует ущерб от внешней социальной инженерии путём затмения её своей социальной инженерией;
* добавить в ПО избыточное количество проверок при вводе данных и требование от сотрудников повторять пациентам их информацию для минимизации шанса НИИ;
* обучение сотрудников правилам информационной безопасности;
* требовать от IT отдела регулярного исследование на наличие клонов веб-страницы поликлиники для уменьшения ущерба от фишинга;
* регулярно проводить осмотр целостности всех ИВС для принятия своевременных мер по восстановлению/замене ИВС и минимизации шанса получения ущерба от износа ИВС;
* внимательно следить за погодными условиями и разработать планы эвакуации и укрепить подвалы для потенциального использования оных как бункеров для минимизации ущерба от стихийных бедствий;
* реализация автономной системы питания для значительного снижения ущерба от отключения электричества;
* реализация системы автономного анализа среды внутри поликлиники и системы быстрого оповещения внутри поликлиники для минимизации ущерба от заражений внутри учреждения.

**Заключение**

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.