



Norwegian Centre for
Integrated Care and Telemedicine

Аспекты безопасности в электронном здравоохранении и телемедицине Arctic Telemedicine 2014 Нарьян-Мар, НАО

Ева Шипенес, советник по вопросам электронной
безопасности, НЦТ
eva.skipenes@telemed.no



План

- Электронная история болезни или бумажная
- Клятва Гиппократата
- Стандарты информационной безопасности
- Определение персональных данных
- Конфиденциальность, целостность, доступность и качество
- Меры информационной безопасности
- Некоторые риски и угрозы безопасности
- Доступ к ЭИБ других учреждений
- Управление рисками / оценка рисков



Электронные или бумажные истории болезни

“Компьютеры вызывают смешанные чувства, потому что легкость, с которой они могут сделать данные широко доступными, создает новые риски для личной жизни. По сравнению с бумажной медицинской документацией, электронной информацией легче манипулировать, и она связана... Это также наводит на мысль об огромной национальной базе идентифицированной комплексной информации о состоянии здоровья.”

(Lise Rybowski, *Protecting the Confidentiality of Health Information*)



Гиппократ и его клятва

Клятва Гиппократа - это залог, принятый врачами, поклявшись этически вести медицинскую практику. Широко распространено мнение, что она была написана Гиппократом, отцом западной медицины в 4-м веке до нашей эры, или одним из его учеников

“... Все, что мне станет известно в результате моей профессиональной деятельности или в повседневном общении с людьми, то, что не должно переходить границы, я буду обязан держать в тайне и никогда не раскрывать...”



Профессиональные тайны/ конфиденциальность – некоторые важные аспекты

- **Без уверенности в конфиденциальности больные могут неохотно давать врачам необходимую им информацию для того, чтобы обеспечить хороший уход**
- Конфиденциальность гарантирует неприкосновенность личной жизни и целостность
- Информация должна быть конфиденциальной, если ее распространение может потенциально травмировать человека эмоционально или материально
- Важная профессиональная обязанность медперсонала
- Вопрос в принятии на себя ответственности за персональную информацию
- Медперсонал должен защищать сензитивную информацию от любого, кто не участвует в лечении пациента
- Связь между этическими, юридическими и вопросами безопасности
- Врач должен всегда исходить из разрешения от пациента об использовании информации в нелечебных целях, например, страховки, определения нагрузок на работе, документации степени заболевания и пр.



Принципы безопасности

- *Соответствующие технические и организационные меры должны быть приняты как во время конструирования системы обработки, так и во время проведения обработки, особенно с целью поддержания безопасности и, таким образом, чтобы предотвратить любую несанкционированную обработку*
- *Эти меры должны обеспечить надлежащий уровень безопасности*



ISO стандарты систем работы с информационной безопасностью

ISO 27000-серии:

(<http://www.27000.org/> or <http://www.iso27001security.com/html/27000.html>)

- ISO/IEC 27000:2014 информационные технологии – техники безопасности – система управления информационной безопасностью – обзор и вокабуляр
- ISO/IEC 27001:2013 информационные технологии – техники безопасности – система управления информационной безопасностью – требования
- ISO/IEC 27002:2013 ... – коды работы с управлением информационной безопасности
- ISO/IEC 27003:2013 ... Наставления по внедрению – информационная безопасность
- ISO/IEC 27004:2009 ... – информационная безопасность – мероприятия
- ISO/IEC 27005:2011 ... – риски инф. безопасности
- ISO/IEC 27006:2011 ... – Требования к органам, проводящим аудит и сертификацию систем менеджмента информационной безопасности
- ISO/IEC 27007:2011 ... – Руководящие принципы для аудита систем менеджмента информационной безопасности
- ISO/IEC 27008:2011 ... – руководство для аудиторов контроля ISMS



ISO стандарты систем работы с информационной безопасностью

The ISO 27000-series:

- ISO/IEC 27009:2014 Information technology – Security techniques – Sector specific application of ISO/IEC 27001 – Requirements (draft)
- ISO/IEC 27010:2012 ... – Information security management for inter-sector and inter-organisational communications
- ISO/IEC 27011:2008 ... – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013:2012 ... – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014:2013 ... – Governance of information security
- ISO/IEC 27017 ... – Code of practice for information security controls based on ISO/IEC 27002 for cloud services (DRAFT)
- ISO/IEC 27017:2014 ... – Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors
- ISO/IEC 27021 ... – Competence requirements for information security management professionals (NWIP)



Определение персональных данных

- «Личные данные» означают любую информацию, касающуюся идентифицированного или идентифицируемого физического лица («Данные субъекта»)
- Идентифицируемое лицо – тот, кто может быть идентифицирован прямо или косвенно, в частности посредством ссылки на идентификационный номер или на один или несколько параметров, определенных для его физического, физиологического, психологического, экономического, культурного и социального удостоверения
- Принципы защиты должны применяться к любой информации в отношении идентифицированного или идентифицируемого человека

(из Директивы 95/46/ЕС Парламента ЕС)



Примеры “личных данных” без имени или идентификаторов

- Возраст, пол, профессия, город или деревня:
 - 55 лет мужчина, стоматолог в НАО
 - 30 лет женщина, с/х, Нарьян-Мар
 - 23 года мужчина, водитель автобуса в Нарьян-Маре
- Возраст, пол, диагноз, город:
 - 40 лет женщина с рассеянным склерозом в Нарьян-Маре

Чтобы определить, является ли человек идентифицируемым, следует учитывать все средства, которые чаще всего используют для идентификации указанного лица.



«Ответственное лицо»

- Должно быть физическое или юридическое лицо, государственный орган, учреждение или любой другой орган, который в одиночку или совместно с другими *определяет цели и средства обработки персональных данных*
- Это «ответственное лицо» должно нести ответственность за защиту прав и свобод персональных данных



Сфера ответственности

- Меры, принятые для защиты прав и свобод субъектных данных, должны обеспечить соответствующий уровень безопасности, принимая во внимание уровень техники и затрат на их реализацию по отношению к рискам, связанным с обработкой и характером данных, которые должны быть защищены (=> оценка риска является необходимой)



Принципы в отношении качества данных

Персональные данные должны быть

- обработаны беспристрастно и законно;
- собраны для указанных, явных и законных целей и не должны подвергаться дополнительной обработке образом, несовместимым с этими целями;
- адекватны и не чрезмерны по отношению к целям, для которых они собираются и / или дальнейшей обработке;
- точными и, в случае необходимости, обновляться; все разумные действия должны быть предприняты для того, чтобы гарантировать, что данные, которые являются неточными или неполными, с учетом целей, для которых они были собраны или для которых они в дальнейшем обрабатываются, были исправлены или уничтожены;
- храниться в форме, позволяющей идентифицировать субъекты данных, не дольше, чем это необходимо для целей, для которых данные были собраны или для которых они в дальнейшем будут обработаны



Аспекты информационной безопасности

- Конфиденциальность
 - Защита сензитивной информации от ”прочих”
 - Внешних
 - Семьи
 - Коллег
 - Других учреждений
 - Пр.
- Целостность/интегритет
 - Защита против неавторизированного изменения данных
- Доступность
 - Защита от разрушения или потери данных
 - Внедрение мер, обеспечивающих доступность данных, когда это необходимо
- Качество
 - Обеспечить, чтобы информация была правильной и обновленной и выдавалась пациенту на руки



Интегрированность

- Защита против неавторизованного просмотра и изменения данных
 - системные ошибки, которые изменяют или разрушают информацию, например при передаче данных из одной системы в другую
 - системные ошибки, которые вызывают регистрацию информации в ЭИС другого пациента
 - слабый интерфейс => провал у пользователя
 - кто-то помимо лечащего персонала может изменить информацию о пациенте



Доступность

- История болезни должна быть доступна только для лиц с авторизованным доступом
 - В основном, люди, принимающие участие в лечении пациента
- История болезни должна быть доступна в случае необходимости для авторизованных лиц



Качество

- Для достижения хорошего качества информации в ЭИБ, система должна давать возможность исправлять ошибки или неточности
- Поправки должны осуществляться таким образом, который показывает исходную информацию и то, что было исправлено
- Когда для консультаций пациентов используется видеоконференция, техническое качество изображения, звука, света и т.д., должны быть достаточными для предоставления надлежащих диагностики и лечения



Мероприятия информационной безопасности

- Оценки риска
- Организационные мероприятия
- Система безопасности и информационные решения для выполнения юридических требований и рекомендаций по оценке риска



Нельзя недооценивать установленные организационные процедуры

- Когда внедряется ЭИБ или электронный обмен информацией, часто не считаются с их влиянием на существующие организационные процедуры
- Могут возникнуть новые риски или увеличены существующие



Безопасность и электронные коммуникации в системе здравоохранения

- Системам ЭИБ часто не хватает коммуникационных модулей
- Могут применяться отдельные коммуникационные приложения
- Как должна быть сделана адресация электронной почты для получения ответов на эл. сообщения тем, кто в них нуждается?
 - Личные учетные записи электронной почты, запрещающие сотрудничающему персоналу чтение ответов на электронные сообщения или результатов лабораторных исследований, которые передаются в учреждение (например, в дом престарелых)
 - Использование счетов - как вы узнаете, что электронная почта была обработана должным образом, а не только прочитана кем-либо

Безопасность и электронные коммуникации в системе здравоохранения

- Информация о здоровье, которая передается из физически контролируемой сети учреждения, должна быть закодирована
 - затрудняет общение посредством электронной почты с пациентами, а также с другими учреждениями
- Ключи кодов должны часто быть установлены для каждого участника общения в связи с недостаточной службой PKI (PKI = Public Key Infrastructure)
- Ключи шифрования должны иметь ограниченный срок (обычно меняются каждые 2 года)
 - не всегда имеется автоматическая служба получения нового шифровочного ключа



Проблемы использования паролей

- Люди допускают коллег одолжить пароль, если они забыли свой пароль
- Если это система, то вы знаете, кто получил доступ к ЭИБ?
- Студенты получают возможность заимствовать пароли
- Врачи, которые работают только краткое время - они получают свой пароль?
- Пароли часто легко угадать, они бывают записаны и легко доступны для других



Угрозы при мобильном доступе к ЭИБ

- Если информация о состоянии здоровья хранится в мобильном компьютере, любой, кто получает доступ к компьютеру, может получить доступ к информации, если она не зашифрована
- Если мобильный компьютер, который подключен к сети больницы и системе ЭИБ через Интернет украден, например из автомобиля, укравший человек получает доступ к системе ЭИБ



Угрозы при мобильном доступе к ЭИБ

- Прослушивание мобильной связи
- Мобильная сеть не работает или имеет плохое качество
- Батарейка села
- Распечатка взята другими
- Вирус приходит в сеть больницы через мобильный компьютер, потому что он был подключен к Интернету через незащищенное соединение
- Подключение VPN от многопользовательского ноутбука - вызов



Доступ к ЭИБ других учреждений

- Должен быть разрешен доступ персоналу другой больницы к системе ЭИБ?
- Вызовы
 - Каждое учреждение несет ответственность за безопасность своей собственной системы ЭИБ и конфиденциальности данных пациентов в их системах
 - Большинство случаев компьютерного злоупотребления совершаются инсайдерами
 - При каких обстоятельствах может контролер контролировать сотрудников другой организации? Путем контрактов?
 - Кто должен быть наказан, если кто-то из другого учреждения нарушает безопасность?
 - Как можно управлять одной из больниц сотрудниками другой больницы?
 - В одной больнице разные пользователи имеют разные права доступа. Какие права доступа должны иметь люди в другой больнице?



Доступ к ЭИБ других учреждений (II)

- Если специалист из Окружной больницы выезжает в местную больницу для лечения пациента, которого он лечил в НОБ, к какой системе ЭИБ он должен получить доступ: к системе в местной больнице или к системе в НОБ?
- Как требования к документации должны быть восприняты – например, в какой системе ЭИБ лечение должно быть задокументировано?



Доступ к ЭИБ других учреждений (III)

Некоторые необходимые условия для
возможного межведомственного доступа

- Национальный (или окружной) регистр всех отделений, участковых врачей, домов медсестринского ухода и пр.
- Региональный/окружной или национальный регистр всех работников здравоохранения: профессия, место работы каждого и сертификат РКІ, который может использоваться для контроля доступа (среди прочего)
- Документация о согласии пациента или отсутствии согласия, в ЭИБ
- Система контроля доступа может комбинировать все эти темы



Какой должен быть уровень безопасности?

- На этот вопрос нет универсального ответа, кроме как **ОЦЕНКА РИСКОВ!**



Зачем оценка рисков?

- Цель оценки рисков – выявить возможные угрозы и просчитать, насколько они серьезны. Это делает возможным внедрение необходимых контрмер для достижения приемлемого уровня риска



Оценка рисков для информационной безопасности должна быть выполнена с учетом

- Конфиденциальности
- Доступности
- Целостности
- Качества



Нарушение конфиденциальности

- Для того, чтобы определить гарантии в отношении защиты конфиденциальности, необходимо оценить:
 - Насколько сензитивны данные, которые мы хотим защитить?
 - Каковы последствия нарушения конфиденциальности?
 - Кто авторизованные и неавторизованные пользователи?
 - Каковы технические аспекты?
 - Кто заинтересован в этих данных? Почему?
 - Как сбалансировать потребности пользователей с ограничениями безопасности?



Доступность и нарушение конфиденциальности

- Для того, чтобы определить доступность и гарантии целостности, необходимо определить:
 - Насколько важно то, что информация доступна для пациентов или медицинского персонала, когда они хотят прочитать или зарегистрировать информацию
 - Насколько важно, что информация о пациенте передается соответствующему медицинскому персоналу немедленно?
 - Если информация будет направлена позже, если переадресация на медицинских работников не представляется возможной на данный момент
 - Если это возможно, исключить, свести к минимуму или просто уменьшить угрозу недоступности, и сколько это стоит?
 - Есть ли какие-либо известные потенциальные угрозы целостности



Допустимый уровень доступности

- Различные уровни приемлемого риска доступности должны быть отнесены к разным критичным категориям систем и приложений
- => Разные требования к доступности для различных категорий критичности



Примеры приоритетов различных категорий критичности

Приоритет	Тип информационной системы	Описание критичности
1	Центр приема острых сообщений (999/113)	Системы, отсутствие которых может быть катастрофичным для пациента
2	Рентгенологические, лабораторные, переключения, интранет, email(?), internet(?)	Системы информации, которые могут иметь решающее значение для жизни или здоровья пациентов
3	ЭИБ	Системы с информацией, которая может быть важной для обеспечения правильного и эффективного лечения
4	Административные системы, офисные приложения, email(?)	Административная поддержка систем с высоким приоритетом
5	Internet(?)	Административная поддержка систем с низким приоритетом

Процесс управления рисками

Систематическое применение политики управления, процедур и практики для решения задач

- коммуникации,
- создания контекста,
- идентификации, анализа, лечения, мониторинга и обзора **рисков**

(From AS/NZS 4360:2004, sec. 1.3.21)



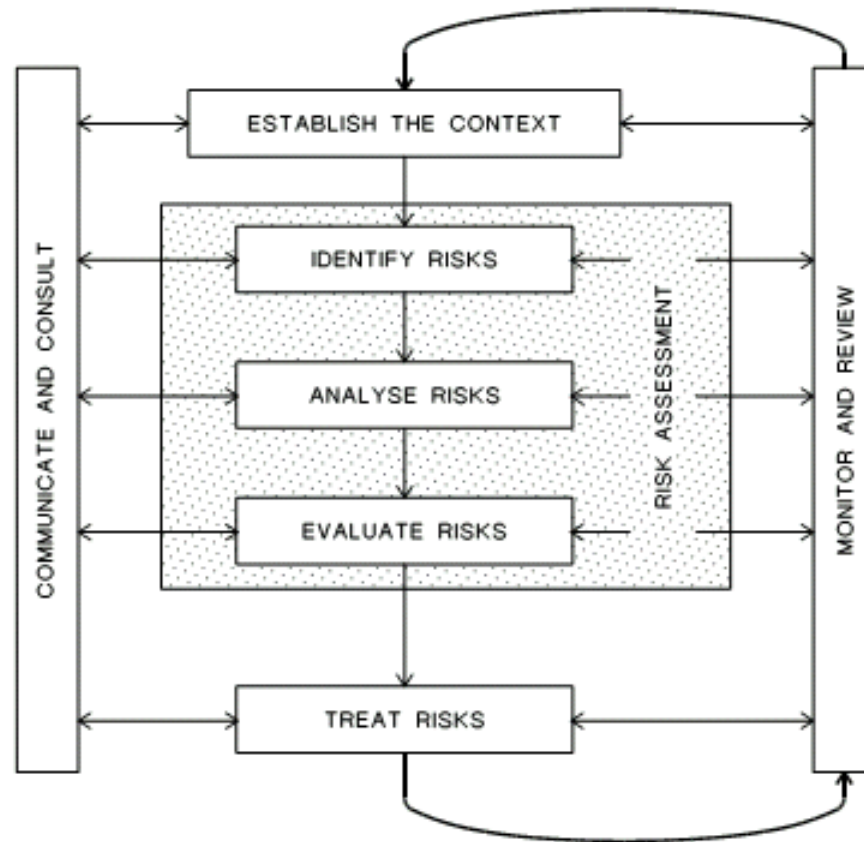


FIGURE 2.1 RISK MANAGEMENT PROCESS - OVERVIEW



Кто должен (или может) руководить анализом рисков?

Предпочтительнее кто-то вне системы или услуг,
которые должны быть оценены

Почему?

- Сложно быть критичным к своему собственному «ребенку»
- Принимающие решения чаще прислушиваются к внешним экспертам
- Если отдел ИТ выполняет анализ рисков, руководство может заподозрить отдел в заинтересованности получить больше денег для приобретения, например, нового интересного оборудования

В любом случае, лучше использовать лидера оценки внутренних рисков, чем не выполнять оценку рисков вообще!



Кто должен принимать участие в оценке рисков?

- Руководитель оценки рисков
- Секретарь оценки рисков
- Соответствующие заинтересованные стороны (фаза планирования)
- Представители пользователей системы или услуг должны быть выслушаны
- Лицо (лица) со знанием технических решений
- Лицо (лица), имеющие опыт обеспечения безопасности



Шаг 1: планирование

Создать план оценки рисков:

- определить цель оценки – ТоЕ (см. следующий слайд)
- определить временные рамки и сроки
- определить необходимые ресурсы (которые должны участвовать)
- получить обязательства от соответствующих заинтересованных сторон
- получить обязательства от руководителей персонала, который необходим в оценке рисков (IT-персонал и врачи всегда заняты!)
- собрать необходимую информацию о системе или приложении для оценки (документация)
- определить критерии приемлемого риска
- определить уровни последствий, уровень вероятности и уровни риска

Примеры ограничений ToE

(ToE: Target of Evaluation/Цель анализа)

- Внутренние процедуры безопасности
- Физическая безопасность
- ЭИБ, PAS, рентгенологическая система, система заказов, система заявок, системы и процедуры логина
- Связь с внешней сетью
- Связь с отраслевыми офисами или партнерами
- Использование модема/ISDN
- Использование Интернета
- Использование эл. почты
- Контракт с теми, кто запускает систему/использует удаленную систему
- Процедуры резервного копирования
- Процедуры восстановления HW или удаления HW



Примеры того, что надо защищать (активы)

- Жизнь и здоровье пациентов
- Информацию о пациентах (конфиденциальность, целостность и/или доступность)
- Репутацию учреждения или сотрудников
- Аппаратные средства и программное обеспечение



Идентификация уязвимости

- Примеры уязвимости
 - Связь с Интернетом или другими внешними сетями
 - Недостаточность политики безопасности и процедур безопасности
 - Старая версия OS и приложений, и недостаточность процедур в отношении исправления и обновления систем
 - **Низкий уровень защиты паролей**
 - Легкий доступ во внутренние системы для неавторизованного персонала
 - Недостаток персонала с навыками IT и безопасности



Определение критериев приемлемого риска

Примеры приемлемого риска

- Вероятность того, что другие работники помимо тех, кто принимает участие в лечении пациента, получают доступ к истории болезни пациента, не должна быть выше, чем раз в то время (см. определение на следующем слайде)
- Вероятность того, что внешние лица получают доступ к записям о здоровье пациента, переданным по электронной почте или видеоконференции, не должна быть больше, чем «редко»
- Вероятность того, что ЭИБ недоступна в течение более 15 минут для чтения, или более 2 часов для внесения записей, не должна быть выше, чем «редко»




Примеры определений вероятности

Описание вероятности	Вероятностный рейтинг	Простота
Исключительно редко	Возникновение реже, чем <ul style="list-style-type: none"> • 0.001 % во время пользования услугой • Каждые 2 года 	
Редко	Возникновение <ul style="list-style-type: none"> • Между 0.001 % и 0.01 % во время пользования услугой • Чаше, чем каждые 2 года, но реже, чем 3 раза в год 	<ul style="list-style-type: none"> • <i>Сотрудники</i> с хорошими ресурсами и комплексными знаниями о контрмероприятиях, дающих результаты • <i>Внешние</i> с хорошими ресурсами и комплексными знаниями о контрмероприятиях, с помощью от сотрудников, дающие результаты
Иногда	Возникновение <ul style="list-style-type: none"> • Между 0.01 % и 0.1 % во время пользования услугой • Чаше, чем 3 раза в год, но реже, чем раз в месяц 	<ul style="list-style-type: none"> • <i>Сотрудники</i> с нормальными ресурсами, нормальными знаниями о контрмероприятиях, дающие результаты • <i>Внешние</i> с хорошими ресурсами, хорошими/полными знаниями о контрмероприятиях, дающие результаты
Часто	Возникновение <ul style="list-style-type: none"> • Между 0.1 % и 20 % во время пользования услугой • Чаше, чем раз в месяц, но реже, чем ежедневно 	<ul style="list-style-type: none"> • <i>Сотрудники</i> с нормальными ресурсами без знаний о контрмероприятиях, случайные • <i>Внешние</i> с небольшими или нормальными ресурсами, нормальными знаниями о контрмероприятиях, дающие результаты
Почти постоянно	Возникновение <ul style="list-style-type: none"> • Между 20 % и 100 % во время пользования услугой • Чаше, чем раз в день 	<ul style="list-style-type: none"> • <i>Сотрудники</i> с небольшими ресурсами, без знаний о контрмерах, спорадические • <i>Внешние</i> с небольшими или нормальными ресурсами, нормальными знаниями о контрмерах, спорадические

Примеры определения последствий

Размер последствий	Описание
Минимальные	<ul style="list-style-type: none">• Недоступность системы ЭИБ менее, чем 4 часа• Нет несанкционированного разглашения данных пациента
Умеренные	<ul style="list-style-type: none">• недоступность системы ЭИБ 4-24 часа• раскрытие информации о пациенте в ограниченном размере
Большие	<ul style="list-style-type: none">• Недоступность ЭИБ более 24 часов• Нарушение целостности медицинских данных, которые могут вызвать проблемы в жизни пациента или репутации больницы (правовой, моральной и экономической)• Неавторизованный доступ в полную систему ЭИБ.



Шаг 2: идентификация рисков

Могут применяться различные методы

- Идентифицировать угрозы/возможные неожиданные инциденты
 - Управляемая или контролируемая мозговая атака
 - Ведомость технического контроля
 - Опрос
- Выявление причин и факторов уязвимости
 - Опрос
 - Анкетирование
 - Ведомость технического контроля



Намеки на идентификацию угроз

Основано на **аспектах безопасности**

(конфиденциальность, целостность, доступность, качество)

Нарушения могут быть:

- Случайные или сознательные действия
 - *преднамеренные – случайные – от окружающей среды*
- От аутсайдеров, инсайдеров или "свыше"
- С влиянием или без влияния человеческого фактора



Таблица угроз

Id	Угроза, неожиданный случай	Причина	Вероятность	Последствие	Уровень риска	Комментарии
k1	Информация о здоровье послана не тому получателю	В системе зарегистрирован неправильный адрес				
K2	Неавторизованный доступ в медицинский реестр	Пользователь забыл выйти из системы, и следующий пользователь компьютера получил доступ				
k3	Неавторизованный доступ в медицинский реестр	Пользователь оставил записку с его паролем под клавиатурой				
k4	Злоумышленники получили доступ к сензитивной информации	Имя пользователя и пароль легко определить				

Шаг 3: анализ рисков

- Оценка последствий
- Вероятность / частота оценок
- Расчет уровня риска



Таблица угроз

Id	Угроза, неожиданный случай	Причина	Вероятность	Последствие	Уровень риска	Комментарии
k1	Информация о здоровье послана не тому получателю	В системе зарегистрирован неправильный адрес	Редко	Умеренно		
k2	Неавторизованный доступ в медицинский реестр	Пользователь забыл выйти из системы, и следующий пользователь компьютера получил доступ	Часто	Умеренно		
k3	Неавторизованный доступ в медицинский реестр	Пользователь оставил записку с его паролем под клавиатурой	Часто	?		
k4	Злоумышленники получили доступ к сензитивной информации	Имя пользователя и пароль легко определить	Редко	Большое		

Определить уровень риска

Уровень риска – продукт вероятности и последствий

- Определить уровень риска
- Определить уровень риска по каждой угрозе
 - Инструмент: матрица риска



Определение уровня риска

Уровень риска:	Рекомендации вмешательства:
Экстремальный риск	Необходимо значительное улучшение системы безопасности
Высокий риск	Старший менеджер должен определить, продолжить сервис работать или он должен быть остановлен до внедрения улучшений
Умеренный риск	Определить ответственного за мониторинг рисков
Низкий риск	С рисками можно справиться путем рутинных процедур

Вероятность					
Последствия	<i>Крайне редко</i>	<i>Редко</i>	<i>Иногда</i>	<i>Часто</i>	<i>Почти всегда</i>
<i>Минимальны</i>					
<i>Умеренные</i>		k1		k2	
<i>Большие</i>		k4			

Шаг 4: оценка рисков

- Оценить по отношению к приемлемому уровню риска
 - Какие риски приемлемы, какие – нет
- Классифицировать и определить приоритетность
 - Можно взглянуть на отношения между рисками



Шаг 5: Управление рисками

- Определить вид вмешательства
- Оценить возможности альтернативного воздействия



Варианты управления рисками

Возможные подходы

- a) избежание риска
- b) сокращение риска
(например, сокращение вероятности и/или последствий)
- c) удаление риска
- d) сохранение риска

Возможные варианты управления

- Изменения требований к безопасности
- Изменения политики безопасности, например, политики изменения паролей
- Изменения системной архитектуры
- Стратегии тестирования
- Стратегии мониторинга



План лечения риска

Id	Неприемлемый риск	Контрмеры	Ответственность	Dead-line	Статус
K2	Неавторизованный доступ в медицинский реестр	Автоматический выход спустя 15 минут бездействия. Подготовка кадров и повышение информированности пользователей	<Имя> IT-отдел, человек, ответственный за IT безопасность	<дата>	
K4	Злоумышленники получают доступ к конфиденциальной информации, потому что имя пользователя и пароль легко получить	Более строгая политика паролей. Обучение кадров, повышение информированности пользователей	<Имя> IT-отдел, человек, ответственный за IT безопасность	<дата>	
					

Управление информационной безопасностью

Включает в себя:

- Систему внутреннего контроля за бизнесом
- Цели безопасности и стратегия безопасности
- Документацию по конфигурации системы информационных технологий
- Оценку рисков (планы, анализ рисков и отчеты)
- Описание или обзор обязанностей по отношению к информационной безопасности
- Процедуры обработки нарушений безопасности
- Процедуры повышения подготовки кадров
- Подпрограммы для работы ИТ-систем, техническое обслуживание и безопасность
- Контракты или соглашения с внешними партнерами



Механизмы конфиденциальности

Потенциальные механизмы контроля за доступом

- Механизмы аутентификации (удостоверение личности)
 - Имя пользователя и пароль
 - Смарт-карты
 - Неконтактные карты
 - eToken
 - Калькулятор одноразовых паролей
 - Биометрика (отпечатки пальцев, скан сетчатки)
- Процедуры авторизации (кто должен получить доступ и к чему?)
- Контрольный список доступа (кто для чего авторизован?)



Прочие механизмы безопасности

- Модернизация и безопасность починки систем и приложений
- Сведите к минимуму использование административным пользователям
- Не допускать запуска неавторизованных приложений
- Шифрование
- Межсетевые экраны
- Системы обнаружения вторжений
- Антивирусные и антиспам-системы
- Безопасный серверных комнат (профессиональные кражи, огнестойкость, защита от наводнения, меры против отключения электроэнергии)
- Процедуры резервного копирования



Риски безопасности – некоторые примеры

- Email
 - Входящие вирусы
 - Данные пациента могут быть уничтожены
 - Данные пациента могут быть в результате «несчастливого случая» посланы неавторизованному получателю
- Доступ в интернет с того же сервера или сети, как системы ЭИБ или другой критичной системы (хакеры, вирусы)
- Слабые процедуры паролей (*очень часто*)
- Слишком много паролей для запоминания
- Изменение паролей слишком часто



Риски безопасности – некоторые примеры

- Принтеры легко доступные для кого угодно (люди не забирают свои распечатки достаточно быстро)
- Медицинский персонал не выходит из системы при покидании компьютера (слишком много времени, чтобы войти в систему в следующий раз, когда они собираются использовать компьютер => кто задокументировал, что?)
- Отказы пользователей: Пользователи не достаточно обучены в использовании компьютерных систем и приложений
- Недостаточная информированность пользователей
- о рисках безопасности



ССЫЛКИ

- Protecting the Confidentiality of Health Information – A background paper prepared by Lise Rybowski, The George Washington University, July 1998

http://www.nhpf.org/library/issue-briefs/IB724_Confidentiality_9-18-98.pdf

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html



Прочие ссылки на работу с рисками

Австралийский и Новозеландский стандарты по работе с рисками:

- Risk Management, Standards Association of Australia, AS/NZS 4360:1999
- Описание австралийского стандарта можно скачать здесь:

http://www.broadleaf.com.au/tutorials/Tut_Standard.pdf



Прочие ссылки на работу с рисками

Статья описывает процесс анализа риска и использование методологий на практике:

- “Risk analysis of information security in a mobile instant messaging and presence system for healthcare”

http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6T7S-4KPX940-1&_coverDate=08%2F23%2F2006&_alid=482875308&_rdoc=1&_fmt=&_orig=search&_qd=1&_cdi=5066&_sort=d&_view=c&_acct=C000030698&_version=1&_urlVersion=0&_userid=596705&md5=fb916db8b5994ffeb88c22987907b043

Статьи можно найти на:

- http://www.elsevier.com/wps/find/journaldescription.cws_home/506040/description#description Кликни на “Full text in ScienceDirect” правой кнопкой, потом на “Articles in Press” левой. Потом смотрите в «поиске» слово “Risk” в названиях и “Henriksen” в авторах

