ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56850— 2015/IEC/TR 80001-2-2:2012

Информатизация здоровья

МЕНЕДЖМЕНТ РИСКОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 2-2

Руководство по выявлению и обмену информацией о защите медицинских приборов, рисках и управлении рисками

IEC/TR 80001-2-2:2012
Application of risk management for IT-networks incorporating medical devices — Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
(IDT)

Издание официальное

Москва
Стандартинформ
2016

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Министерства здравоохранения Российской Федерации» (ЦНИИОИЗ Минздрава) и Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации «Фирма «ИНТЕРСТАНДАРТ» на основе собственного аутентичного перевода на русский язык международного документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Минздрава — постоянным представителем ISO ТС 215

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 30 декабря 2015 г. № 2242-ст

4 Настоящий стандарт идентичен международному документу IEC/TR 80001-2-2:2012 «Информатизация здоровья. Менеджмент рисков в информационно-вычислительных сетях с медицинскими приборами. Часть 2-2. Руководство по выявлению и обмену информацией о защите медицинских приборов, рисках и управлении рисками» (IEC/TR 80001-2-2:2012 «Application of risk management for IT-networks incorporating medical devices — Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (подраздел 3.5)

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

МЭК 80001-1, посвященный применению МЕНЕДЖМЕНТА РИСКА к ИТ-сетям с медицинскими приборами, предоставляет информацию о ролях, ответственностях и действиях, необходимых для МЕНЕДЖМЕНТА РИСКА. Настоящий стандарт содержит дополнительное руководство по выбору ВОЗМОЖНОСТИ ЗАЩИТЫ (выявлению и обсуждению) как в ПРОЦЕССЕ МЕНЕДЖМЕНТА РИСКА, так и в контактах заинтересованных сторон и соглашениях.

Информативный набор распространенных, высокоуровневых ВОЗМОЖНОСТЕЙ ЗАЩИТЫ, представленный в настоящем стандарте, служит точкой отсчета для обсуждения, посвященного защите, между вендором и покупателем или между представителями большой группы заинтересованных лиц, вовлеченных в проект МЕДИЦИНСКОЙ ИТ СЕТИ. Масштабы применения охватывают ОТВЕТСТВЕННЫЕ ОРГАНИЗАЦИИ всевозможных размеров, так как каждая осуществляет оценку РИСКА с учетом возможностей и решает, что учитывать, а что нет, основываясь на устойчивости к РИСКУ и планировании ресурсов. Настоящий стандарт может применяться при подготовке документации, предназначенной для предоставления информации по ВОЗМОЖНОСТЯМ ЗАЩИТЫ изделия и его возможностям. Данная документация может быть использована ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ в качестве входной информации для организации ее ПРОЦЕССА по МЭК 80001 или для формирования основ СОГЛАШЕНИЙ ОБ ОТВЕТСТВЕННОСТИ для заинтересованных сторон. Другие стандарты МЭК 80001-1 содержат в себе пошаговое руководство по ПРОЦЕССУ МЕНЕДЖМЕНТА РИСКА. Более того, ВОЗМОЖНОСТИ ЗАЩИТЫ служат толчком к выявлению и более подробному описанию средств защиты, например, тех, которые установлены в одном из многих стандартов защиты, которыми руководствуется ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ или производитель МЕДИЦИНСКОГО ПРИБОРА (например, ИСО 227799:2008, ИСО/МЭК 27001:2005, ИСО/МЭК 27002:2005, ИСО/МЭК 27005:2011, серия стандартов ИСО 22600, серия стандартов ИСО 13606, и ИСО/HL7 10781:2009, охватывающий функциональную модель электронной системы медицинских карт). Настоящий стандарт сохраняет независимость общего подхода к структуре средств управления. В настоящем стандарте предлагается только структура для выявления и предоставления информации ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ (называемой в данном документе Медицинской Организацией — МО), производителем МЕДИЦИНСКОГО ПРИБОРА (ПМП) и ИТ-вендором.

Выделенные в настоящем стандарте возможности охватывают выявление совокупности средств управления, которые обеспечивают сохранение конфиденциальности и охрану от вредоносного проникновения, которое может приводить к нарушению целостности или доступности системы/данных. По мере возникновения необходимости возможности могут добавляться или получать дальнейшее развитие. Средства управления предназначены для охраны как данных, так и систем, но особое внимание уделяется охране как ЛИЧНЫХ ДАННЫХ, так и их подраздела, называемого ДАННЫМИ О ЗДОРОВЬЕ. Оба этих специальных термина были корректно определены во избежание любых отсылок к специальным законам (например, уязвимые данные ЕС, электронная защищенная информация о состоянии здоровья США (USA ePHI)).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

МЕНЕДЖМЕНТ РИСКОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 2-2

Руководство по выявлению и обмену информацией о защите медицинских приборов, рисках и управлении рисками

Health informatics. Risk management for IT-networks incorporating medical devices. Part 2-2. Guidance for the disclosure and communication of medical device security needs, risks and controls

Дата введения — 2016—11—01

1 Область применения

Настоящий стандарт формирует основной подход для выявления связанных с защитой возможностей и РИСКОВ, информация о которых необходима для управления РИСКОМ при подключении МЕДИЦИНСКИХ ПРИБОРОВ к ИТ СЕТЯМ, а также для представленного в МЭК 80001-1 взаимодействия (диалога) между заинтересованными организациями по вопросам защиты, которое сопровождает МЕНЕДЖМЕНТ РИСКА процесса соединения с ИТ СЕТЬЮ. Настоящий стандарт предоставляет информативный набор распространенных, высокоуровневых, связанных с защитой возможностей, полезных с точки зрения нужд пользователя, с указанием рассматриваемых для них типов средств управления безопасностью, а также РИСКОВ, которые приводят к использованию этих средств управления. ПРЕДНАЗНАЧЕННОЕ ИСПОЛЬЗОВАНИЕ и местные факторы определяют, какие именно возможности будут использоваться в диалоге о РИСКЕ.

Описания возможностей, представленные в настоящем стандарте, предназначены для:

a) медицинской организации (МО),

b) производителей МЕДИЦИНСКИХ ПРИБОРОВ (ПМП), а также

c) ИТ вендоров.

Данные описания служат основой для обсуждения РИСКА и назначения соответствующих ролей и ответственностей для выполнения менеджмента РИСКА. Данное обсуждение, ведущееся среди «партнеров» по РИСКУ, служит основой для одного или нескольких СОГЛАШЕНИЙ ОБ ОТВЕТСТВЕННОСТИ, как это установлено в МЭК 80001-1.

Настоящий стандарт предоставляет подробные описания возможностей, связанных с защитой, с намерением обеспечить любой прибор или его использование хотя бы одним дополнительным элементом спецификации для каждой возможности. Эти описания часто связаны с местом расположения и конкретным применением и ссылаются на соответствующие стандарты, посвященные РИСКУ и средствам управления защиты.

На данном начальном этапе стандартизации по МЭК 80001-1, ВОЗМОЖНОСТИ ЗАЩИТЫ в настоящем стандарте предоставляют распространенную, простую классификацию средств управления безопасностью, в особенности подходящих для МЕДИЦИНСКИХ ИТ СЕТЕЙ и подключенных к ним приборов. Этот список не направлен на формирование или поддержку использования строгих средств управления, основанных на стандартах ИТ защиты, и связанных с ними программ сертификации и обеспечения, рассматриваемых в других ИСО стандартах (например, ИСО/МЭК 15408 и его общие критерии оценки безопасности информационных технологий). Настоящий стандарт не содержит достаточно подробного описания конкретных технических требований для случая запроса предложений

Издание официальное

или документа о выявлении защиты изделия. Однако классификация и структура могут применяться для организации таких требований, а также лежащих в их основе деталей, которых достаточно для обмена информацией при приобретении и для ПРОЦЕССА интеграции МЕДИЦИНСКОГО ПРИБОРА или компонента ИТ оборудования. Необходимо подчеркнуть, что настоящий стандарт предназначен быть основой для обсуждения и соглашения, достаточной для начального формирования МЕНЕДЖМЕНТА РИСКА проекта. Кроме того, защита рассматривается только в контексте организационной политики защиты. Обе политики:

a) политика защиты медицинской организации (МО) и

b) политика защиты изделия и услуг производителя МЕДИЦИНСКОГО ПРИБОРА (ПМП)

находятся вне области применения настоящего стандарта. Кроме этого, настоящий стандарт не затрагивает клинические исследования, требующие защиты выборочного раскрытия ЛИЧНЫХ ДАННЫХ или ДАННЫХ О ЗДОРОВЬЕ.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты и документы. Для датированных ссылок следует использовать указанное издание. Для недатированных ссылок — последнее издание указанного документа, включая все поправки к нему.

МЭК 80001-1:2010, Применение менеджмента риска для ИТ СЕТЕЙ с медицинскими приборами. Часть 1. Роли, ответственности и действия (IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities).

3 Термины и определения

В настоящем стандарте используются следующие термины и определения

3.1 **ЗАЩИЩЕННОСТЬ СИСТЕМЫ И ДАННЫХ** (DATA AND SYSTEM SECUIRTY): Рабочее состояние МЕДИЦИНСКОЙ ИТ СЕТИ, в котором информационные ресурсы (данные и системы) обоснованно защищены от нарушения конфиденциальности, полноты и доступа.

[МЭК 80001-1:2010, статья 2.5. Определение модифицированное — два примечания из оригинального документа, неотъемлемые для понимания области применения определения, были удалены]

3.2 **ЭФФЕКТИВНОСТЬ** (EFFECTIVENESS): Способность достигать намеченных результатов по отношению к пациенту и ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ.

[МЭК 80001-1:2010, статья 2.6]

3.3 **УПРАВЛЕНИЕ СОБЫТИЕМ** (EVENT MANAGEMENT): ПРОЦЕСС, который гарантирует, что все события, негативно влияющие или способные негативно повлиять на работу ИТ СЕТИ, фиксируются, оцениваются и обрабатываются контролируемым способом.

[МЭК 80001-1:2010, статья 2.7]

3.4 **ВРЕД** (HARM): Физическая травма или ущерб здоровью людей, или имуществу, или окружающей среде, а также снижение ЭФФЕКТИВНОСТИ или нарушение ЗАЩИЩЕННОСТИ СИСТЕМЫ И ДАННЫХ.

[МЭК 80001-1:2010, статья 2.8]

3.5 **ОПАСНОСТЬ** (HAZARD): Потенциальный источник ВРЕДА.

[МЭК 80001-1:2010, статья 2.9]

3.6 **ОПАСНАЯ СИТУАЦИЯ** (HAZARDOUS SITUATION): Обстоятельства, при которых люди, имущество или окружающая среда подвержены одной или нескольким ОПАСНОСТЯМ.

[МЭК 14971:2007, статья 2.4]

3.7 **ДАННЫЕ О ЗДОРОВЬЕ** (HEALTH DATA). ЛИЧНЫЕ ДАННЫЕ, указывающие на состояние физического или психического здоровья.

Примечание — Вышеописанное в общих чертах определяет в рамках настоящего стандарта личные данные и их подраздел ДАННЫЕ О ЗДОРОВЬЕ, что позволяет пользователям настоящего стандарта легко применять эти понятия к разным нормативным актам и регламентам о конфиденциальности данных. Например, в Европе, такие требования могут быть приняты, а термин может быть заменен на «Персональные данные» и «Уязвимые данные». В США термин ДАННЫЕ О ЗДОРОВЬЕ может быть заменен на «Защищенную информацию о здоровье (PHI)», а также, при необходимости, могут быть внесены поправки и в сам текст.

3.8 **ПРЕДНАЗНАЧЕННОЕ ИСПОЛЬЗОВАНИЕ** (INTENDED USE): Применение изделия, ПРОЦЕССА или службы в соответствии с техническими условиями, инструкциями и информацией, предоставленной производителем.

[МЭК 80001-1:2010, статья 2.10]

3.9 **ИНТЕРОПЕРАБЕЛЬНОСТЬ** (INTEROPERABILITY): Свойство, позволяющее разнообразным системам и компонентам работать вместе для достижения установленной цели.

[МЭК 80001-1:2010, статья 2.11]

3.10 **ИТ СЕТЬ** (INFORMATION TECHNOLOGY NETWORK, IT-NETWORK): Система или системы, состоящие из взаимодействующих узлов и каналов передачи данных, предназначенные для обеспечения проводной или беспроводной передачи данных между двумя или более установленными узлами коммуникации.

[МЭК 80001-1:2010, статья 2.12. Определение модифицированное — два примечания из начального определения не были сохранены]

3.11 **ОСНОВНЫЕ СВОЙСТВА** (KEY PROPERTIES): Три управляемые характеристики риска (БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ и ЗАЩИЩЕННОСТЬ СИСТЕМЫ И ДАННЫХ) МЕДИЦИНСКИХ ИТ СЕТЕЙ.

[МЭК 80001-1:2010, статья 2.13]

3.12 **МЕДИЦИНСКИЙ ПРИБОР** (MEDICAL DEVICE): Любой инструмент, устройство, приспособление, машина, прибор, имплантат, реагент или калибратор в пробирке, программное обеспечение, материал или другие подобные, связанные с ними изделия:

a) предполагаемые производителем для применения к человеку, отдельно или в сочетании друг с другом для одной или более заданных целей, таких как:

- диагностика, профилактика, контроль, лечение или облегчение течения заболеваний,
- диагностика, контроль, лечение, облегчение травмы или компенсация последствий травмы,
- исследования, замещения, изменения или поддержка анатомического строения или физиологических процессов,
- поддержание и сохранение жизни,
- предупреждение беременности,
- дезинфекция медицинских приборов,
- предоставление информации для медицинских и диагностических целей, посредством исследований проб в пробирке, полученных из тела человека, и

b) не реализующие свое основное предназначение в или на теле человека с помощью фармакологических, иммунологических или метаболических средств, но чья основная функция может поддерживаться подобными мерами.

Примечания

1 Определение прибора для исследований в лабораторных условиях включает, например, реагенты, бужизмеритель, приборы забора и хранения образцов, контрольные материалы и связанные с этим инструменты и приспособления. Данные, полученные с помощью такого прибора диагностики в лабораторных условиях, могут использоваться в целях диагностики, контроля или сравнения. В некоторых юрисдикциях отдельные приборы лабораторной диагностики, включая реагенты и подобные им, могут подчиняться отдельным правилам и положениям.

2 Изделия, которые, в некоторых юрисдикциях, могут быть приняты за медицинские приборы, но к которым еще не существует согласованного подхода, это:

- средства помощи инвалидам и людям с ограниченными возможностями;
- приборы для лечения/диагностики болезней и травм животных;
- аксессуары для медицинских приборов (см. примечание 3);
- дезинфицирующие вещества;
- приборы, использующие ткани животных и людей, которые могут соответствовать описанным выше определениям, но используются для других направлений.

3 Аксессуары, специально предназначенные производителями для использования совместно с медицинским прибором, для которого они были разработаны, для реализации цели медицинского прибора, должны подчиняться тем же процедурам GHT (Целевая группа глобальной гармонизации), которые применяются к самому медицинскому прибору. Например, аксессуар классифицируется так, как будто он является медицинским прибором. Это может привести к различию в классификациях аксессуара и прибора, для которого он был разработан.

4 Компоненты медицинских приборов в общих случаях контролируются через систему управления качеством производителя и процедуры оценки соответствия прибора. В некоторых юрисдикциях, компоненты включаются в определение «медицинского прибора».

[МЭК 80001-1:2010, статья 2.14]

3.13 **МЕДИЦИНСКАЯ ИТ СЕТЬ** (MEDICAL IT-NETWORK): ИТ СЕТЬ, к которой подключен хотя бы один МЕДИЦИНСКИЙ ПРИБОР.

[МЭК 80001-1:2010, статья 2.16]

3.14 **ОПЕРАТОР** (OPERATOR): Лицо, работающее с оборудованием.

[МЭК 80001-1:2010, статья 2.18]

3.15 **ЛИЧНЫЕ ДАННЫЕ** (PRIVATE DATA): Любая информация, связанная с идентифицированной личностью или личностью, доступной для идентификации.

3.16 **ПРОЦЕСС** (PROCESS): Совокупность взаимосвязанных и взаимодействующих действий, преобразующих входы в выходы.

[МЭК 80001-1:2010, статья 2.19]

3.17 **ОСТАТОЧНЫЙ РИСК** (RESIDUAL RISK): РИСК, остающийся после выполнения мер по УПРАВЛЕНИЮ РИСКОМ.

[МЭК 80001-1:2010, статья 2.20]

3.18 **СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ** (RESPONSIBILITY AGREEMENT): Один или более документов, которые совместно определяют все ответственности для всех значимых заинтересованных сторон.

[МЭК 80001-1:2010, статья 2.21. Определение модифицированное — примечание к начальному определению, содержащее примеры, не было сохранено.]

3.19 **ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ** (RESPONSIBILE ORGANIZATION): Юридическое или физическое лицо, ответственное за использование и обслуживание МЕДИЦИНСКОЙ ИТ СЕТИ.

Примечание — В настоящем стандарте во избежание путаницы, связанной с понятием ответственности за обеспечение защиты, ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ из МЭК 80001-1 именуется медицинской организацией (МО).

[МЭК 80001-1:2010, статья 2.23. Определение модифицированное — примечание к начальному определению, содержащее примеры, не было сохранено. К определению было добавлено другое примечание.]

3.20 **РИСК** (RISK): Комбинация вероятности причинения ВРЕДА и его тяжести.

[МЭК 80001-1:2010, статья 2.23]

3.21 **АНАЛИЗ РИСКА** (RISK ANALYSIS): Систематическое использование доступной информации для выявления ОПАСНОСТЕЙ и количественной оценки РИСКА.

[МЭК 80001-1:2010, статья 2.24]

3.22 **ОЦЕНКА РИСКА** (RISK ASSESSMENT): Общий процесс, включающий в себя АНАЛИЗ РИСКА и ОЦЕНИВАНИЕ РИСКА.

[МЭК 80001-1:2010, статья 2.25]

3.23 **УПРАВЛЕНИЕ РИСКОМ** (RISK CONTROL): ПРОЦЕСС принятия решений и выполнения мер по уменьшению рисков до установленных уровней или поддержания рисков внутри установленного диапазона.

[МЭК 80001-1:2010, статья 2.26]

3.24 **ОЦЕНИВАНИЕ РИСКА** (RISK EVALUATION): ПРОЦЕСС сравнения количественно оцененного РИСКА, с заданными критериями РИСКА для определения значимости РИСКА.

[МЭК 80001-1:2010, статья 2.27]

3.25 **МЕНЕДЖМЕНТ РИСКА** (RISK MANAGEMENT): Систематическое применение политик, процедур и практических методов менеджмента для решения задач анализа, оценивания, управления и контроля РИСКА.

[МЭК 80001-1:2010, статья 2.28]

3.26 **БЕЗОПАСНОСТЬ** (SAFETY): Отсутствие недопустимого РИСКА физической травмы или ущерба здоровью людей, или ущерба имуществу, или окружающей среде.

[МЭК 80001-1:2010, статья 2.30]

3.27 **ВОЗМОЖНОСТЬ ЗАЩИТЫ** (SECURITY CAPABILITY): Широкая категория технических, административных или организационных средств для управления РИСКАМИ, связанными с конфиденциальностью, целостностью, доступностью и отслеживаемостью данных и систем.

3.28 **ВЕРИФИКАЦИЯ** (VERIFICATION): Подтверждение на основе предоставления объективных свидетельств того, что установленные требования были выполнены.

[МЭК 80001-1:2010, статья 2.32. Определение модифицированное — три примечания к оригинальному определению не были сохранены]

4 Использование ВОЗМОЖНОСТЕЙ ЗАЩИТЫ

4.1 Структура записи о ВОЗМОЖНОСТИ ЗАЩИТЫ

Раздел ВОЗМОЖНОСТИ ЗАЩИТЫ, представленный ниже (раздел 5), рассматривает общие ВОЗМОЖНОСТИ ЗАЩИТЫ, которые могут быть включены в МЕДИЦИНСКИЙ ПРИБОР или ИТ компонент. Для каждой возможности предложено обозначение из четырех букв для удобства предоставления ссылки и табуляции. Каждый подраздел предоставляет различную информацию о возможно применимом средстве управления защитой или категорию ПРОЦЕССА. Описание каждой возможности содержит:

- ссылки к источникам информации о данной возможности (т. е. применимые стандарты, политики и справочные материалы; в данном случае МО и ПМП должны учитывать как международные стандарты защиты, так и применимые стандарты отдельных стран на элементы защиты, представленные в NIST 800-39/53/66/... (США), NEN 7510 (Нидерланды), требования ASIP (Франция), закон о защите персональной информации и руководство по менеджменту безопасности системы медицинской информации (Япония) и т. д.);
- основную цель возможности защиты (т. е. цель требования) и
- заявление о том, что пользователю (поставщику медицинских услуг) необходима данная возможность.

Часто перечисленные ВОЗМОЖНОСТИ ЗАЩИТЫ формируют основу для обсуждения в кругу участников СОГЛАШЕНИЯ ОБ ОТВЕТСТВЕННОСТИ. Эти обсуждения и принимающиеся по их результатам соглашения, предназначены для свойств, ролей и ответственностей, распределенных между заинтересованными сторонами и касающихся РИСКОВ для защиты.

4.2 Руководство по использованию ВОЗМОЖНОСТЕЙ ЗАЩИТЫ в ПРОЦЕССЕ МЕНЕДЖМЕНТА РИСКА

Все ВОЗМОЖНОСТИ ЗАЩИТЫ являются потенциальными возможностями УПРАВЛЕНИЯ РИСКОМ. Выбор возможностей УПРАВЛЕНИЯ РИСКОМ следует за выявлением потребности в снижении РИСКА для защиты. В МЭК/ТО 80001-2-1:2012 предоставлено пошаговое подробное описание ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА, в котором выбор, реализация и ВЕРИФИКАЦИЯ средств УПРАВЛЕНИЯ РИСКОМ осуществляется на шагах 6—8.

ВОЗМОЖНОСТИ ЗАЩИТЫ рассматривают варианты УПРАВЛЕНИЯ РИСКОМ для защиты следующим образом:

- «цель требований» содержит список возможных РИСКОВ для защиты, которые могут быть снижены с помощью ВОЗМОЖНОСТИ ЗАЩИТЫ;
- раздел, посвященный «потребности пользователя», содержит информацию о возможных аспектах, подлежащих рассмотрению при использовании этой ВОЗМОЖНОСТИ ЗАЩИТЫ.

Крайне необходимо отметить, что конкретное решение защиты, разработанное для определенного прибора для одного сценария использования, может не подходить для другого. ПРЕДНАЗНАЧЕННОЕ ИСПОЛЬЗОВАНИЕ МЕДИЦИНСКОГО ПРИБОРА, подключенного к МЕДИЦИНСКОЙ ИТ СЕТИ, несет в себе информацию о том, какие ВОЗМОЖНОСТИ необходимо выбрать и на каком уровне им требуется поддержка. Иногда это ведет к важному включению ВОЗМОЖНОСТЕЙ ЗАЩИТЫ, например, использование имен пользователей и паролей в приборах, соединенных с сетью, содержащих данные о пациентах. В других случаях, контекст ПРЕДНАЗНАЧЕННОГО ИСПОЛЬЗОВАНИЯ исключает целый класс средств управления безопасностью; например, небольшое встроенное программное устройство, такое как прибор контроля SPO2, не нуждается в установке на самом приборе встроенного журнала аудита системы защиты. Требования защиты, применимые в контексте конкретного ПРЕДНАЗНАЧЕННОГО ИСПОЛЬЗОВАНИЯ и в конкретном окружении, никогда не должны применяться без рассмотрения их возможного влияния на БЕЗОПАСНОСТЬ и ЭФФЕКТИВНОСТЬ изделия.

4.3 Связь между МЕНЕДЖМЕНТОМ РИСКА, выполняемым в соответствии с ИСО 14971, и МЕНЕДЖМЕНТОМ РИСКА для защиты

Для получения информации о применении МЕНЕДЖМЕНТА РИСКА для обеспечения защиты на организационном уровне см. ИСО/МЭК 27001:2005, ИСО/МЭК 27002:2005, ИСО/МЭК 27799:2008. Для случаев подключения МЕДИЦИНСКОГО ПРИБОРА к ИТ СЕТИ можно применить ИСО/МЭК 27005:2011, из которого ПРОЦЕССЫ МЕНЕДЖМЕНТА РИСКА для ИТ защиты могут быть использованы дополнительно к ПРОЦЕССУ МЕНЕДЖМЕНТА РИСКА из ИСО 14971, чтобы соответство-

вать МЭК 80001-1:2010 (т. е. БЕЗОПАСНОСТИ, ЭФФЕКТИВНОСТИ и ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМЫ). В МЭК/ТО 80001-2-1:2012 предоставлено подробное пошаговое руководство по выполнению МЕНЕДЖМЕНТА РИСКА.

МЭК 80001-1:2010 в определение ВРЕДА включает ОСНОВНЫЕ СВОЙСТВА: БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ и нарушение ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМ. Предложение «..нарушение ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМ», определяющее ВРЕД, равносильно выполнению действий в области ИТ защиты (например, в системе защиты от кибератак). При рассмотрении ОПАСНОСТЕЙ в защите ИТ, уязвимость системы может привести к нарушению (посредством вторжения). Похожим образом, угрозой может быть что-либо, что представляет опасность для ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМЫ. Здесь проходит параллель между ОПАСНОСТЬЮ и возможным источником ВРЕДА. Проще говоря, угрозы используют уязвимости, что может привести к вторжению (известному источнику возможного ВРЕДА) или, как отмечено в ИСО/МЭК 27005:2011, «РИСК для защиты информации связан с возможностью того, что угрозы будут реализовываться, используя уязвимости информационного средства или группы информационных средств, и таким образом причинять ВРЕД организации».

Настоящий стандарт использует термины, связанные с защитой и РИСКОМ, как из области ИТ, так и из области МЕНЕДЖЕМНТА РИСКА МЕДИЦИНСКИХ ПРИБОРОВ (на основе ИСО 14971). Таблица 1 может быть использована для установления связи между терминологией, связанной с защитой ИТ, и терминологией, основанной на ИСО 14971. Данная связь не является точной, но позволяет сопоставить концепции.

Таблица 1 — Связь между терминологией, связанной с защитой ИТ, и терминологией, основанной на ИСО 14971

МЕНЕДЖМЕНТ РИСКА для ИТ защиты	МЕНЕДЖМЕНТ РИСКА, основанный на ИСО 14971
Уязвимость — признанная незащищенность в защите, которая, в случае присутствия угрозы, может привести к ухудшению обеспечения информации данных и систем	Атрибут системы, который ведет к возможности причинения ВРЕДА (в особенности данным и системам), т.е. является ОПАСНОСТЬЮ, возникающей из атрибута, явно подверженного использованию во вредоносных целях (в терминах ИТ)
Угроза — нечто (преднамеренное или случайное), что способно причинить ВРЕД системам и организациям	Обстоятельство или событие, которое может повлечь за собой ВРЕД, т. е. ОПАСНОСТЬ, возникающая из уязвимости, плюс обстоятельство или событие, которое является ее инициатором (в ИТ она часто предполагает участие фактора угрозы)
Незащищенность — ситуация, которая может повлечь за собой причинение ВРЕДА	ОПАСНАЯ СИТУАЦИЯ
Вторжение — программное обеспечение или набор команд, создающий брешь в защите *Угроза* + *уязвимость* + «*активация*» → ВРЕД	Экземпляр ВРЕДА ОПАСНОСТЬ+ОПАСНАЯ СИТУАЦИЯ+«последовательность событий» → ВРЕД
РИСК — влияние неопределенности на достижение целей. [ИСО/МЭК 27005:2011]	РИСК — комбинация вероятности причинения вреда и его тяжести. [ИСО 14971:2007]
Контрмеры, гарантии безопасности, средства управления безопасностью	Возможности УПРАВЛЕНИЯ РИСКОМ (в ИТ они иногда именуются ослаблением РИСКОВ, осуществляемой при логическом обосновании АНАЛИЗОМ РИСКА)
Нарушение конфиденциальности, целостности или доступности систем и данных (включает брешь в защите личных данных)	ВРЕД

5 ВОЗМОЖНОСТИ ЗАЩИТЫ

5.1 Автоматический выход из системы — ALOF

Применение: Стандарт. Нет.
Политика. Местная ИТ политика МО.

Справочный материал: Нет.

Цель требований: Уменьшить РИСК получения несанкционированного доступа к ДАННЫМ О ЗДОРОВЬЕ с рабочего места, оставленного без присмотра.
Предотвратить неправильное использование, если система или рабочее место не используются в течение периода времени.

Потребность пользователя: Несанкционированные пользователи не могут получить доступ к ДАННЫМ О ЗДОРОВЬЕ с рабочего места, оставленного без присмотра.
Сеансы санкционированных пользователей должны автоматически завершаться или блокироваться по прошествии заранее установленного промежутка времени. Это уменьшает РИСК несанкционированного доступа к ДАННЫМ О ЗДОРОВЬЕ, когда санкционированный пользователь покидает рабочее место, не завершая сеанс и не запирая экран или комнату.
Автоматический выход из системы должен включать в себя очистку ДАННЫХ О ЗДОРОВЬЕ со всех экранов по мере надобности.
Местный санкционированный ИТ администратор должен иметь возможность отключить эту функцию и установить срок действия (учитывающий хранитель экрана)
Хранитель экрана с коротким временем бездействия или активирующийся «быстрой клавишей» может являться дополнительным свойством. Эта очистка экрана ДАННЫХ О ЗДОРОВЬЕ может быть вызвана, когда на протяжении короткого времени не была нажата ни одна клавиша (например, от 15 с до нескольких минут). Это не завершит сеанс пользователя, но снизит РИСК случайного наблюдения информации.
Желательно, чтобы клинические пользователи могли избежать потери незавершенной работы по причине автоматического выхода из системы.
Рекомендуется подробное указание характеристик ALOF, которые позволяют различать (а) выход из системы и (б) блокировку экрана с возможностью восстановления сеанса.

5.2 Средства управления аудитом — AUDT

Применение: Профиль. Профиль IHE ATNA (Профиль интеграции журнал аудита и аутентификация узлов) [IHE ATNA profile (Audit Trail and Node Authentication Integration Profile)].
Техническая основа рентгенологии IHE (IHE Radiology Technical Framework).
Политика. Местная ИТ политика МО.

Справочный материал: NEMA (Национальная ассоциация производителей электрооборудования): S&P Аудит (NEMA: S&P Auditing).

Цель требований: Установить согласованный подход к надежному аудиту того, кто и что делает с ДАННЫМИ О ЗДОРОВЬЕ, чтобы позволить ИТ отделу МО контролировать использование этих данных, применяя общеиспользуемые подходы, стандарты и технологию.
Наша индустрия пришла к согласию в том, что ИТ МО предпочитает поддержку профиля журнала аудита IHE.
Цель аудита (от IHE). Позволить сотруднику службы безопасности организации вести аудит деятельности для оценки ее соответствия политике защиты данной области, а также для обнаружения случаев неподобающего поведения, и для облегчения обнаружения неправильного создания, получения доступа, модификации и удаления закрытой медицинской информации (PHI).

Потребность пользователя: Возможность записывать и изучать деятельность системы по средством ведения журналов аудита с помощью прибора, для отслеживания доступа к системе и ДАННЫМ О ЗДОРОВЬЕ, а также их модификации и удаления.

Поддержка использования либо в качестве изолированного архива данных (регистрирующего файлы аудита в своей собственной файловой системе) или, в случае такой конфигурации, отправляющего зарегистрированную информацию отдельному, управляемому МО центральному архиву данных.

Поддержка создания и сопровождения аудита поддерживается соответствующими инструментами проверки аудита.

Защита данных аудита по мере необходимости (в особенности, если эти данные содержат сами персональные данные).

Отсутствие возможности удалять или редактировать данные аудита.

Так как данные аудита скорее всего содержат персональные данные и/или ДАННЫЕ О ЗДОРОВЬЕ, то вся обработка (например, получение доступа, хранение и передача) должна подчиняться соответствующим средствам управления.

5.3 Авторизация — AUTH

Применение: Примечание — Основывается на аутентификации, но эти два понятия не следует путать.

Стандарт. ANSI/INCITS 359-2004 Управление доступом, основанное на ролях (ANSI/INCITS 359-2004 Role-Based Access Control).

Существуют общие подходы, которые могут быть полезны для рассматриваемого случая:

Общий подход к технической ИТ инфраструктуре IHE. Журнал аудита и аутентификация узлов (ATNA) / Аутентификация корпоративных пользователей (EUA) / Контроль процесса авторизации пользователей (XUA) [IHE IT Infrastructure Technical Framework — Audit Trail and Node Authentication (ATNA) / Enterprise User Authentication (EUA) / Cross Enterprise User Assertion (XUA)];

IETF (Рабочая группа инженеров Интернет): Защита транспортного уровня передачи данных (TLS) 1.2 (RFC 5246) [IETF: Transport Layer Security (TLS) 1.2 (RFC 5246)];

ITU-T (Сектор стандартизации телекоммуникаций в составе международного телекоммуникационного общества): Рекомендация X.509. «Информационная технология. Взаимодействие открытых систем. Директория. Инфраструктура сертификата открытого ключа и атрибута» [ITU-T: Recommendation X.509. "Information technology — Open Systems Interconnection — The directory: Public-key and attribute certificate frameworks].

Политика. Местная ИТ политика МО

Справочный материал: Белая книга IHE (Интегрированное учреждение здравоохранения). Управление доступом (IHE White Paper — Access Control).

Общий подход к технической ИТ инфраструктуре IHE Журнал аудита и аутентификация узлов (ATNA).

ИСО/TS 22600-1:2006, Информатизация здоровья. Привилегированный менеджмент и управление доступом. Часть 1. Обзор и политика менеджмента (ISO/TS 22600-1:2006 Health informatics — Privilege management and access control — Part 1: Overview and policy management).

ИСО/TS 13606-4:2009, Информатизация здоровья. Электронная система передачи медико-санитарной документации. Часть 4. Защита (ISO/TS 13606-4:2009 Health informatics — Electronic health record communication — Part 4: Security)

Цель требований: Следуя принципу минимизации данных, предоставить управление доступом к ДАННЫМ О ЗДОРОВЬЕ и функциям только в той степени, насколько это необходимо для выполнения задач МО в соответствии с ПРЕДНАЗНАЧЕННЫМ ИСПОЛЬЗОВАНИЕМ прибора.

Потребность пользователя: Избежать несанкционированный доступ к данным и функциям с целью (1) сохранить конфиденциальность системы и данных, целостность и доступность, а также (2) чтобы остаться в рамках разрешенного использования данных и систем.

В согласии с ИТ политикой МО и основываясь на аутентифицированной идентификации отдельных пользователей, возможность авторизации позволяет каждому пользователю получать доступ только к одобренным данным и выполнять с помощью прибора только одобренные функции.

Согласно политике организации санкционированные пользователи включают в себя МО и обслуживающий персонал.

МЕДИЦИНСКИЕ ПРИБОРЫ, как правило, поддерживают систему, основанную на разрешениях, которая предоставляет доступ к функциям системы и данным в соответствии с ролью запрашивающего доступ пользователя МО (управление доступом, основанное на ролях, RBAC). Например:

— ОПЕРАТОРЫ могут выполнять назначенные им задачи, используя все надлежащие для этого функции прибора (например, контроль или сканирование пациентов).

— Персонал службы качества (например, радиолог) может принимать участие во всех надлежащих испытаниях качества и контроля качества.

— Обслуживающий персонал может получать доступ к системе, включающий поддержку деятельности этого персонала, такую как профилактическое обслуживание, расследование проблем и устранение этих проблем.

Авторизация позволяет МО эффективно предоставлять медицинское обслуживание и в то же время (1) сохранять защищенность системы и данных и (2) придерживаться принципа надлежащей минимизации данных. Авторизация может управляться локально или же в масштабах предприятия (например, с помощью централизованного руководства).

Примечание — В случаях, когда ПРЕДНАЗНАЧЕННОЕ ИСПОЛЬЗОВАНИЕ не подразумевает время, достаточное для начала и завершения сеанса использования прибора (например, в случае использования высокой пропускной способности), местной ИТ политикой может быть разрешено ослабление контроля авторизации, допуская, что физический доступ контролируется и ограничивается в достаточной мере.

5.4 Конфигурация свойств системы защиты — CNFS

Применение: Стандарт. Нет.
Политика. Местная ИТ политика МО.

Справочный материал: Нет.

Цель требований: Дать МО возможность определять, как задействовать ВОЗМОЖНОСТИ ЗАЩИТЫ изделия, чтобы удовлетворить их требования к политике и/или рабочему процессу.

Потребность пользователя: Местному санкционированному ИТ администратору требуется возможность выбирать между использованием и не использованием ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ЗАЩИТЫ изделия. Это может включать в себя взаимодействие аспектов управления привилегиями с средством управления ФУНКЦИОНАЛЬНОЙ ВОЗМОЖНОСТЬЮ ЗАЩИТЫ.

5.5 Усовершенствование системы защиты изделия от кибератак — CSUP

Применение: Руководство. Руководство OIS по созданию отчетов об уязвимостях в защите и ответным мерам на их появление V2.0 1-е сентября 2004 (OIS Guidelines for Security Vulnerability Reporting and Response V2.0 1 September 2004).
Политика. Местная ИТ политика МО.

Справочный материал: NEMA SPC Установление исправлений на готовое программное обеспечение, использующееся в медицинских информационных системах. Октябрь 2004 (NEMA SPC Patching off-the-shelf software used in medical information systems. October 2004).

Цель требований: Создать унифицированный метод выполнения работы. Установка / усовершенствование пакетов исправлений для системы защиты выполняется персоналом на рабочем месте, и, вероятно, санкционированным персоналом МО (в случае установки скачиваемых пакетов исправлений).

Потребность пользователя: Установка пакетов исправлений, предоставленных посторонней организацией, на медицинские изделия при первой выдавшейся возможности и в соответствии с регламентом, требующим:
- назначение наивысшего приоритета исправлениям, адресованным уязвимостям, связанным с высоким уровнем РИСКА, которые определяются в результате объективного, официального, документально отраженного, процесса ОЦЕНИВАНИЯ РИСКА уязвимости, осуществленного ПМП;
- обеспечение вендором медицинских изделий и поставщиком медицинских услуг продолжительного безопасного и эффективного клинического функционирования их изделий; обеспечение понимания местного регламента для МЕДИЦИНСКОГО ПРИБОРА (в общих случаях запрещена установка изменений на МЕДИЦИНСКИЕ ПРИБОРЫ без четких прописанных инструкций от ПМП);
- проведения надлежащего испытания для обнаружения любых непредвиденных последствий установки исправления на медицинский продукт (для рабочих характеристик или функциональности), которые могут подвергнуть ПАЦИЕНТА опасности;
- предоставления пользователям, в особенности ИТ персоналу МО и службе МО, упреждающей информации об оцененных/подтвержденных пакетах исправлений.

5.6 Идентификация ДАННЫХ О ЗДОРОВЬЕ — DIDT

Применение: Стандарт. NEMA DICOM (Формирование цифровых изображений и обмен ими в медицине) Дополнение 142. Профили деидентификации клинического исследования (NEMA DICOM Supplement 142: Clinical Trial De-identification profiles).
NEMA DICOM Дополнение 55. Конфиденциальность уровня атрибутов (включая деидентификацию) 5 сентября 2002 (Финальный текст) [NEMA DICOM Supplement 55: Attribute level confidentiality (including De-identification) 5 Sept 2002 (Final text)].
ИСО 25237:2008, Информатизация здоровья. Псевдонимизация (ISO 25237:2008, Health Informatics — pseudonimization).

Примечание — Псевдонимизация и использование любой разновидности идентификационных кодов для пациентов позволяет деидентифицировать данные и таким образом, не является деидентификационным методом.

Политика. Местная ИТ политика МО

Справочный материал: Суини Л. 2002. K-анонимность: модель для системы охраны личной информации. Международный журнал, посвященный неопределенности, нечеткости и системам, основанным на знаниях. Выпуск 10(5), 557-570 (Sweeney, L. 2002. *K*-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledgebased systems, 10(5), 557-570).

Цель требований: Способность оборудования (прикладного программного обеспечения или дополнительного инструментария) непосредственно удалять информацию, позволяющую идентифицировать ПАЦИЕНТОВ.
Удаление данных перед возвращением изделия на завод; создание архитектуры, позволяющей удаленное обслуживание без доступа к/раскрытия ДАННЫХ О ЗДОРОВЬЕ; внутризаводской карантин, присвоение меток и обучение.

Потребность пользователя: Пользователь медицинского изделия, инженеры по обслуживанию и отдел маркетинга должны иметь возможность деидентифицировать ДАННЫЕ О ЗДОРОВЬЕ для разнообразных целей, не требующих информации о личности ПАЦИЕНТА.

5.7 Резервное копирование данных и аварийное восстановление — DTBK

Применение: Стандарт. Нет.
Политика. Местная ИТ политика МО.

Справочный материал: ИСО/МЭК 20000-2:2012, Планирование и испытание непрерывности обслуживания (ISO/IEC 20000-2:2012, Service continuity planning and testing).

Цель требований: Обеспечить возможность для поставщика медицинских услуг продолжать вести свое предприятие после повреждения или уничтожения данных, оборудования или программного обеспечения.

Потребность пользователя: Достаточная гарантия того, что постоянные системные настройки и постоянные ДАННЫЕ О ЗДОРОВЬЕ, хранящиеся в изделиях могут быть восстановлены после отказа системы или нарушения, таким образом, что предприятие могло продолжить функционировать.

Примечание — Данное требование может не подходить для небольших, бюджетных приборов и может, на практике, зависеть от способности собирать новые, значимые данные во время следующего цикла приобретения (например, потеря данных о низкой частоте сердечных сокращений, связанная с прерывистым сигналом беспроводного подключения)

5.8 Экстренный доступ — EMRG

Применение: Стандарт. Нет.
Политика. Местная ИТ политика МО.

Справочный материал: NEMA SPC Белая книга. Разбитие стекла (NEMA SPC White paper: Breakglass).

Цель требований: Обеспечить возможность доступа к охраняемым ДАННЫМ О ЗДОРОВЬЕ в случае экстренной ситуации, требующей немедленного доступа к хранящимся ДАННЫМ О ЗДОРОВЬЕ.

Потребность пользователя: В экстренных ситуациях пользователь медицинского изделия должен иметь возможность получить доступ к ДАННЫМ О ЗДОРОВЬЕ без персонального идентификатора (id) и аутентификации (функции разбивания стекла).

Экстренный доступ должен быть обнаружен, зафиксирован и отражен в отчете. Предпочтительно, эта функциональная возможность должна включать какое-нибудь средство моментального уведомления системного администратора или медицинского персонала (в дополнении к записи результатов аудита).
Экстренный доступ должен требовать и записывать идентификационную информацию самоудостоверенного пользователя в том виде, в котором она вводится (без аутентификации).
МО может разрешить это с помощью процедурного подхода, используя учетную запись конкретного пользователя или функции системы.
Администратор должен иметь возможность включать/выключать любые экстренные функции, предоставляемые продуктом, зависящие от технических или процедурных средств управления, которые требуются.

5.9 Целостность и достоверность ДАННЫХ О ЗДОРОВЬЕ — IGAU

Применение:	Стандарт. Нет. Политика. Местная ИТ политика МО.
Справочный материал:	NEMA Аудит защиты и неприкосновенности частной жизни (NEMA Security and Privacy Auditing).
Цель требований:	Обеспечить сохранность ДАННЫХ О ЗДОРОВЬЕ от изменения или уничтожения несанкционированными методами, а также гарантировать, что эти данные поступили от их создателя. Обеспечить целостность ДАННЫХ О ЗДОРОВЬЕ.
Потребность пользователя:	Пользователь хочет подтверждение того, что ДАННЫЕ О ЗДОРОВЬЕ являются надежными и не измененными в результате злонамеренного вмешательства. Решением является использование как несъемных, так и съемных носителей информации.

5.10 Обнаружение вредоносного программного обеспечения и защита от него — MLDP

Применение:	Стандарт. Нет. Политика. Местная ИТ политика МО.
Цитата из регламента:	Защита от вредоносного программного обеспечения (Решаемая проблема). Процедуры принятия мер предосторожности, обнаружения и уведомления (создания отчетов) о вредоносном программном обеспечении.
Справочный материал:	NEMA Защита медицинских информационных систем от вредоносного программного обеспечения (NEMA Defending Medical Information Systems Against Malicious Software).
Цель требований:	Изделие обеспечивает потребности регулирования, а также МО и пользователя, в обеспечении эффективной и единой поддержки предотвращения, обнаружения и удаления вредоносного программного обеспечения. Это является неотъемлемым шагом в обеспечении надлежащего глубокого подхода к защите. Обновление прикладного программного обеспечения для борьбы с вредоносным ПО, поддержание актуальности массивов данных, содержащих шаблоны вредоносного программного обеспечения, своевременная установка исправлений для приложений. Для удовлетворения требований регламента качества часто требуется испытание для ВЕРИФИКАЦИИ работы прибора на соответствие ПРЕДНАЗНАЧЕННОМУ ИСПОЛЬЗОВАНИЮ и требованиям БЕЗОПАСНОСТИ, осуществляемое после обновления программного обеспечения.

Потребность пользователя: МО должна обнаруживать традиционное вредоносное программное обеспечение также как и несанкционированное программное обеспечение, которое может нарушать корректную работу прибора/системы.

5.11 Аутентификация узлов — NAUT

Применение: Профиль. Профиль IHE ATNA. Профиль интеграции журнала аудита и аутентификация узла.
Политика. NEMA/COCIR/JIRA Объединенный комитет по вопросам защиты и неприкосновенности частной жизни (Joint Security and Privacy). Белая книга (предстандарт технического комитета). Управление сертификатами аутентификации компьютеров, 10 февраля, 2005 (Committee draft White Paper: *Management of Machine Authentication Certificates,* 10 February 2005).
Проект политики защиты института SANS (институт системного администрирования, аудита сети и защиты) [SANS Security Policy Project].
Местная ИТ политика МО.

Справочный материал: Нет.

Цель требований: Политика аутентификации должна быть гибкой, чтобы иметь возможность адаптироваться к местной ИТ политики МО. Использование, по мере необходимости, аутентификации узлов при передаче ДАННЫХ О ЗДОРОВЬЕ.

Потребность пользователя: Возможность управления межкомпьютерными учетными записями на медицинском оборудовании для защиты доступа к ДАННЫМ О ЗДОРОВЬЕ.
Поддержка независимого и центрального администрирования.
Поддержка аутентификации узлов в соответствии с отраслевыми стандартами.
Обнаружение и предотвращение фальсификации (необходимо предоставить невозможность отказа от авторства).

5.12 Аутентификация личности — PAUT

Применение: Профиль. Профиль IHE ATNA (Профиль журнала аудита и интеграции аутентификации узлов).
Профиль IHE PWP (Персональный телефонный справочник) [IHE PWP profile (Personal White Pages].
IHE EUA (Аутентификация корпоративных пользователей).
IHE XUA (Контроль процесса авторизации пользователей).
Политика. Проект политики защиты SANS.
Местная ИТ политика МО.

Справочный материал: Нет.

Цель требований: Политика аутентификации должна быть гибкой для того, чтобы адаптироваться к местной ИТ политике МО. Требование аутентификации личности при предоставлении доступа к ДАННЫМ О ЗДОРОВЬЕ должно быть логически обоснованным в каждом конкретном случае.
Иметь возможность контролировать доступ к приборам, ресурсам сети и ДАННЫМ О ЗДОРОВЬЕ, а также создавать журналы аудита с невозможностью отказа от авторства. Данное свойство должно позволить однозначно и с уверенностью идентифицировать личность, пытающуюся получить доступ к сети, прибору или ресурсу.

Примечание — Это требование смягчено в процессе выполнения «разбивания стекла». См. «Экстренный доступ».

Потребность пользователя: Создание и использование уникальных учетных записей для пользователей и управление доступом, основанное на ролях (RBAC, местное и удаленное) к прибору, подключенному к сети, для управления и контроля доступа к сети и ее деятельности.
Возможность управлять учетными записями на медицинском оборудовании обеспечения защиты доступа к ДАННЫМ О ЗДОРОВЬЕ.
Пользователю может потребоваться связать персональные установки с учетными записями пользователей. Это может помочь приборам и системам, используемым множеством ОПЕРАТОРОВ, отделов или даже множеством организаций здравоохранения (МО). Необходима поддержка независимого и центрального администрирования.
Однократная идентификация и использование одного пароля для всех рабочих мест.
Обнаружение и предотвращение фальсификации (необходимо предоставить невозможность отказа от авторства).

5.13 Физические замки на приборе — PLOK

Применение: Стандарт. Нет.
Политика. Местная ИТ политика МО.

Справочный материал: Нет.

Цель требований: Гарантировать, что несанкционированный доступ не нарушит конфиденциальность системы или данных, целостность и доступность.

Потребность пользователя: Достаточная гарантия того, что ДАННЫЕ О ЗДОРОВЬЕ, хранящиеся в изделиях или носителях были и остаются защищены в соответствии с уязвимостью и объема записей данных на приборе.
Достаточная безопасность систем от злонамеренного вмешательства или удаления компонентов, которое может нарушить целостность, конфиденциальность или доступность.
Злонамеренное вмешательство (включая удаление прибора) обнаружимо.

5.14 Влияние компонентов третьей стороны на весь жизненный цикл изделия — RDMP

Применение: Стандарт. Нет.
Политика. Местная ИТ политика МО.

Цитата из регламента: Нет.

Справочный материал: Нет.

Цель требований: МО требуется понимание защиты на протяжении всего жизненного цикла МЕДИЦИНСКОГО ПРИБОРА.
Планы ПМП предполагают, что их изделия считаются поддерживаемыми на протяжении их жизненного цикла, согласно внутренним системам контроля качества и внешнему регламенту.
Изделия предоставляются с четко установленным ожидаемым сроком службы.
Целью является упреждающее управление влиянием жизненного цикла компонентов на весь жизненный цикл всего изделия. Такое коммерческое готовое программное обеспечение, предоставляемое сторонней организацией, включает в себя операционные системы, системы баз данных, генераторы отчетов, компоненты MIP и т. д. (предполагается, что существующее PCP уже контролирует износ аппаратных компонентов).
Сторонняя организация в данном случае также включает в себя внешних поставщиков защиты для уязвимых компонентов с их собственным жизненным циклом и поддерживающими программами.

Потребность пользователя: Контракты, политика и регламент МО требуют от вендора сопровождения/поддержки системы на протяжении жизни изделия.
Когда компоненты платформы начинают устаревать должно выполняться их обновление и усовершенствование.
Различные МО поставщики услуг демонстрируют проявление особой осторожности при необратимом удалении ДАННЫХ О ЗДОРОВЬЕ перед списыванием (списывании по причине брака, повтором использовании, перепродаже или переработке) приборов. Подобная деятельность должна фиксироваться и подвергаться аудиту.
Отдел продаж и обслуживания должен быть уведомлен о поддержке защиты предоставляемой для каждого изделия на протяжении его жизненного цикла.

5.15 Усиление защиты системы и приложений — SAHD

Применение: Стандарт. Нет.
Политика. Местная ИТ политика МО.
Проект политики института SANS.

Справочный материал: Читальный зал для литературы по информационной защите института SANS (Пошаговые руководства).
Инструменты защиты и исходные показатели CIS (Центр эталонов интернет-безопасности и инструментов обеспечения защиты).

Цель требований: Отладить средства управления защитой МЕДИЦИНСКОГО ПРИБОРА и/или прикладного программного обеспечения таким образом, чтобы защищенность была максимальна («усилена»), но при этом осуществлялось ПРЕДНАЗНАЧЕННОЕ ИСПОЛЬЗОВАНИЕ прибора.
Минимизировать векторы атак и совокупную площадь атак посредством закрытия портов; удаления службы и т. д.

Потребность пользователя: Пользователю требуется стабильная система, предоставляющая только те службы, установленные ПРЕДНАЗНАЧЕННЫМ ИСПОЛЬЗОВАНИЕМ и требующиеся для его осуществления, с минимумом сопроводительной деятельности.
ИТ отделу МО требуется, чтобы системы, подключенные к их сети, были обеспечены защитой при доставке, а также усилены для защиты от неправильного использования и атак.
Желательно, чтобы пользователь информировал ПМП о предполагаемых нарушениях защиты и очевидных слабостях пользовательского оборудования.

5.16 Руководящие указания по защите — SGUD

Применение: Стандарт. Нет.
Политика. Местная ИТ политика МО.

Справочный материал: Заявление производителя о раскрытии информации о защите медицинского прибора (MDS2) [Manufacture Disclosure Statement for Medical Device Security (MDS2)].

Цель требований: Обеспечить доступность руководства по защите для ОПЕРАТОРОВ и администраторов системы. Желательно предоставление отдельных пособий для ОПЕРАТОРОВ и АДМИНИСТРАТОРОВ (включая отдел продаж и обслуживания ПМП), так как это позволяет только администраторам сохранять за собой понимание всего административного функционала.

Потребность пользователя: ОПЕРАТОР должен обладать четкой информацией о своих ответственностях и о защищенном способе работы с системой.

Администратору требуется информация об управлении, настройке и контроле системы (т. е. список средств управления, записей аудита и т. д.)
Администратору необходимо четкое понимание функциональных возможностей защиты, чтобы позволить ему выполнение ОЦЕНКИ РИСКА для ДАННЫХ о ЗДОРОВЬЕ в соответствии с надлежащими нормативными требованиями.
Отдел продаж и обслуживания также нуждается в информации о ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЯХ системы и защищенном способе работы.
Желательно, чтобы пользователь знал, когда и как необходимо информировать ПМП о предположительных нарушениях безопасности и очевидных слабостях в пользовательском оборудовании.

5.17 Конфиденциальность хранения ДАННЫХ о ЗДОРОВЬЕ — STCF

Применение: Стандарты. NEMA DICOM Часть 15. Профили управления защитой и системой (NEMA DICOM Part 15: Security and System Management Profiles).
NEMA DICOM Дополнение 51. Защита носителей информации (NEMA DICOM Supplement 51: Media security).
NEMA DICOM Дополнение 55. Конфиденциальность уровня атрибутов (включая деидентификацию), 5 сентября, 2002 (Финальный текст).
Политика. Местная ИТ политика МО.

Справочный материал: Шнайер Б. 1996, Практическая криптография. Второе издание. John Wiley & Sons, Нью-Йорк (Schneier B. 1996. Applied Cryptography, Second Edition. John Wiley & Sons, New York, NY.).

Цель требований: ПМП устанавливает технические средства управления для ослабления возможного нарушения целостности и конфиденциальности ДАННЫХ о ЗДОРОВЬЕ, хранимых на изделиях или съемных носителях.

Потребность пользователя: Достаточная гарантия того, что ДАННЫЕ о ЗДОРОВЬЕ, хранящиеся на изделиях или носителях были и остаются защищены.
На основе результатов АНАЛИЗА РИСКА должна рассматриваться возможность использования шифрования для ДАННЫХ о ЗДОРОВЬЕ, хранящихся на МЕДИЦИНСКИХ ПРИБОРАХ.
В случае ДАННЫХ о ЗДОРОВЬЕ, хранящихся на съемных носителях, шифрование может послужить защитой конфиденциальности/целостности для пользователей медицинских изделий, но также и для инженеров служб и приложений ПМП, собирающих медицинские данные.
Механизм для управления ключами шифрования согласуется с обычным использованием, доступом к услугам, экстренным доступом типа «разбивания стекла».
В методе и стойкости шифрования учитывается объем (масштаб сбора/агрегации) и уязвимость данных.

5.18 Конфиденциальность передачи данных — TXCF

Применение: Профиль. Профиль IHE ATNA (Профиль интеграции журнал аудита и аутентификация узлов).
Политика. Местная ИТ политика МО.

Справочный материал: NEMA SPC Сертификаты, белая книга (NEMA SPC Certificates white paper).
NEMA DICOM Часть 15. Профили управления защитой и системой.
IETF: Защита уровня передачи данных в сетевой рабочей группе RFC 5246, август 2008. Протокол TLS версия 1.2 (IETF: Transport Layer Security in Network Working Group RFC 5246) August 2008: The TLS Protocol Version 1.2).

ITU-T. Рекомендация X.509. «Информационная технология. Взаимодействие открытых систем. Директория. Инфраструктура сертификата открытого ключа и атрибута» (ITU-T: Recommendation X.509. «Information technology — Open Systems Interconnection — The directory: Public-key and attribute certificate frameworks»)

Цель требований: ПРИБОР соответствует местным законам, регламенту и стандартам (например, USA HIPAA (закон об обеспечении доступности и подотчетности в медицинском страховании), национальным законам, основанным на EU 95/46/EC) в соответствии с потребностями МО для обеспечения конфиденциальности передаваемых ДАННЫХ О ЗДОРОВЬЕ.

Потребность пользователя: Гарантия сохранения конфиденциальности ДАННЫХ о ЗДОРОВЬЕ во время передачи этих данных между аутентифицированными узлами. Это позволяет осуществлять передачу ДАННЫХ о ЗДОРОВЬЕ через относительно открытые сети и/или окружение, где действует крепкая ИТ политика МО обеспечения целостности и конфиденциальности ДАННЫХ о ЗДОРОВЬЕ.
В стандарте МЭК/ТО 80001-2-3:2012 представлено больше информации о МЕНЕДЖМЕНТЕ РИСКА для систем беспроводных сетей.

5.19 Целостность передачи данных — TXIG

Применение: Профиль. Профиль IHE ATNA (Профиль интеграции журнала аудита и аутентификация узлов).
Политика. Местная ИТ политика МО.

Справочный материал: NEMA SPC Сертификаты, белая книга.
NEMA DICOM Часть 15. Профили управления системой и защитой.

Цель требований: Прибор должен обеспечивать защиту целостности передаваемых ДАННЫХ о ЗДОРОВЬЕ.

Потребность пользователя: Обеспечение сохранения целостности ДАННЫХ о ЗДОРОВЬЕ во время передачи. Это позволяет осуществлять передачу ДАННЫХ о ЗДОРОВЬЕ через относительно открытые сети и/или окружение, где действует крепкая ИТ политика МО обеспечения целостности и конфиденциальности ДАННЫХ о ЗДОРОВЬЕ.

6 Пример подробной спецификации для ВОЗМОЖНОСТИ ЗАЩИТЫ. Аутентификация личности — PAUT

Предшествующий раздел «ВОЗМОЖНОСТИ ЗАЩИТЫ» содержал описание базовых возможностей, а также потребности пользователей и исходные материалы. При реальном применении возможность описывается более подробно в инструкции по защите от несанкционированного доступа ПМП или в запросе МО на получение информации о защите изделия. Ниже приводится пример выявления информации ПМП для возможности «Аутентификация личности». Для целевого МЕДИЦИНСКОГО ПРИБОРА выявленная информация указывает на наличие или отсутствие данной ВОЗМОЖНОСТИ ЗАЩИТЫ.

PAUT. Аутентификация личности

Термин «пользователь» предполагает лицо, осуществляющее уход за пациентом и/или выполняющее функции управления сетью и защитой в медицинской организации.

Цель требований: Политика аутентификации должна быть гибкой для того, чтобы адаптироваться к местной ИТ политике МО. Требование аутентификации личности при предоставлении доступа к ДАННЫМ О ЗДОРОВЬЕ должно быть логически обоснованным в каждом конкретном случае.

	Иметь возможность контролировать доступ к приборам, ресурсам сети и ДАННЫМ О ЗДОРОВЬЕ, а также создавать журналы аудита с невозможностью отказа от авторства. Данное свойство должно позволить однозначно и с уверенностью идентифицировать личность, пытающуюся получить доступ к сети, прибору или ресурсу. Примечание — Это требование смягчено в процессе выполнения «разбивания стекла». См. «экстренный доступ».
Потребность пользователя:	Создание и использование уникальных учетных записей для пользователей и управление доступом, основанное на ролях (RBAC, местное и удаленное) к прибору, подключенному к сети, для управления и контроля доступа к сети и ее деятельности. Возможность управлять учетными записями на медицинском оборудовании обеспечения защиты доступа к ДАННЫМ О ЗДОРОВЬЕ. Пользователю может потребоваться связать персональные установки с учетными записями пользователей. Это может помочь приборам и системам, используемым множеством ОПЕРАТОРОВ, отделов или даже множеством организаций здравоохранения (МО). Необходима поддержка независимого и центрального администрирования. Однократная идентификация и использование одного пароля для всех рабочих мест. Обнаружение и предотвращение фальсификации (необходимо предоставить невозможность отказа от авторства).
PAUT.1	Изделие поддерживает обработку учетных записей пользователей, администрируемую локально (на приборе). Возможность для ИТ отдела МО и, если необходимо, для инженера по обслуживанию, позволяющая управлять учетными записями локальных пользователей.
PAUT.2	Использование центрального администрирования МО для учетных записей пользователей в соответствии с профилем IHE EUA.
PAUT.3	Поддержка идентификации множества одновременных пользователей (например, ОПЕРАТОР + практикующий врач) для управления доступом, основанного на ролях.
PAUT.4	Однократная идентификация для методов, использующих множество рабочих станций или для одной рабочей станции, на которой работает множество приложений.
PAUT.6	Поддержка быстрого переключения пользователей. Поддержка данной функции уменьшает затраты времени на задачу входа и выхода пользователей из системы.

7 Перечень ссылочных документов

Данный раздел подробно описывает краткие ссылки, использованные в разделе 5.

Ссылочный документ	Название
CIS	Центр эталонов интернет-безопасности и инструментов обеспечения защиты (The Center for Internet Security Benchmarks and Security Tools), http://cisecurity.org/
DICOM	Формирование цифровых изображений и обмен ими в медицине, финансированное NEMA (Digital Imaging and Communications in Medicine sponsored by NEMA). Стандарты. NEMA DICOM Часть 15. Профили управления защитой и системой (NEMA DICOM Part 15: Security and System Management Profiles).

Продолжение

Ссылочный документ	Название
	NEMA DICOM Дополнение 55. Конфиденциальность уровня атрибутов (включая деидентификацию) 5 сентября 2002 (Финальный текст) [NEMA DICOM Supplement 55: Attribute level confidentiality (including De-identification) 5 Sept 2002 (Final text)]. NEMA DICOM Дополнение 51. Защита носителей информации (NEMA DICOM Supplement 51: Media security). NEMA DICOM Дополнение 142: Профили деидентификации клинического исследования (NEMA DICOM Supplement 142: Clinical Trial De-identification profiles).
IETF	Рабочая группа инженеров Интернет (The Internet Engineering Task Force). Документы. Рабочая группа сети RFC 5246 Август 2008: Протокол TLS Версия 1.2 (Network Working Group RFC 5246 August 2008: The TLS Protocol Version 1.2:), http://www.ietf.org/rfc/rfc5246.txt
IHE	Интегрированное учреждение здравоохранения (IHE Integrated Healthcare Enterprise), http://www.ihe.net/Technical_Framework/. Примечание — Об ATNA см. http://wiki.ihe.net/index.php?title=Audit_Trail_and_ Node_ Authentication. Профиль интеграции журнала аудита и аутентификация узлов (ATNA) спроектирован для поддержки управления доступом посредством ограничения доступа к сети между узлами и разрешения доступа к каждому узлу только санкционированным пользователям (прошедшими местную аутентификацию). Он включает в себя Аутентификацию Пользователей, Аутентификацию Соединения, Журнал Аудита и поддерживает: - Защищенные Узлы, - Архив данных аудита, и - Сервер времени. Данные средства предназначены обеспечивать поддержку времени, аутентификации узлов и запись событий аудита. Это основывается на стандартах, созданных в IETF, посвященных Технической основе ИТ инфраструктуры, включая стандарты для Защищенных Коммуникаций (Secure Communications), Передачи записей аудита (Audit Log Transport), Сообщение записей аудита (Audit Log Message). Среди этих стандартов: RFC 5246, WS-I Базовый профиль защиты 1.1 (WS-I Basic Security Profile 1.1), RFC 5424, RFC 5425, RFC 5426, RFC 3164, RFC 3881, DICOM: Дополнение 95 (ИСО 12052 ftp://medical.nema.org/medical/dicom/final/sup95_ft.pdf).
Местная ИТ политика МО	Политика, утвержденная организацией пользователя изделия, в которой установлено допустимое использование информационной технологии
NEMA SPC	Объединенный комитет по вопросам защиты и неприкосновенности частной жизни NEMA/COCIR/JIRA, http://www.medicalimaging.org/ policyandpositions/jointsecurityand-privacy-committee-2/. Технические документы: SPC Аудит защиты и неприкосновенности частной жизни в информационных технологиях в здравоохранении (SPC Security and Privacy Auditing in Health Care Information Technology). SPC Разбитие стекла: Метод получения экстренного доступа к системам здравоохранения. Декабрь 2004 (SPC Break-Glass: An approach to granting emergency access to health care systems. December 2004). SPC Защита медицинских информационных систем от вредоносного программного обеспечения. Декабрь 2003. SPC Установление исправлений на готовое программное обеспечение, использующееся в медицинских информационных системах, Октябрь 2004 (SPC Defending medical information systems against malicious software. December 2003. SPC Patching off-the-shelf software used in medical information systems, October 2004). SPC Интерфейс удаленного обслуживания. Решение (A). Версия 2: безопасность IP в Интернете с помощью цифровых сертификатов, Декабрь 2003 (SPC Remote Service Interface — Solution (A) — Version 2: IPSec over the Internet Using Digital Certificates, December 2003).
ITU	Сектор стандартизации телекоммуникаций в составе международного телекоммуникационного общества ITU-T Рекомендация X.509 (11/2008) ИСО/МЭК 9594-8:2008 (ITU International Telecommunication Union Telecommunication Standardization Section (ITU-T) Recommendation X.509 (11/2008) ISO/IEC 9594-8:2008), http://www.itu.int/itut/recommendations/index.aspx?ser=X

Окончание

Ссылочный документ	Название
OSI	Публикация организации, специализирующейся на Интернет Безопасности (OIS Organization for Internet Safety), http://www.oisafety.org/: OIS Руководство по созданию отчетов об уязвимостях в защите и принятию ответных мер V2.0 1 Сентября 2004 (OIS Guidelines for Security Vulnerability Reporting and Response V2.0 1 September 2004, http://www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf)
SANS	SANS — Институт системного администрирования, аудита, сети и защиты [The SANS (SysAdmin, Audit, Network, Security) Institute], http://www.sans.org. Проект политики защиты института SANS (The SANS Security Policy Project) — «...все, что вам необходимо для стремительного развития и реализации политики защиты информации»: http://www.sans.org/resources/policies/. Читальный зал для литературы по информационной защите института SANS: http://www.sans.org/reading_room/
Шнайер	Брюс Шнайер 1996 Практическая криптография, Второе издание. John Wiley & Sons, Нью-Йорк. (Schneier B. 1996. Applied Cryptography, Second Edition. John Wiley & Sons, New York, NY). Если вы планируете использовать данную книгу, то найдите в интернете список опечаток, так как в тексте присутствуют хорошо известные ошибки
WEDI	Рабочая группа по защите и неприкосновенности частной жизни в электронном обмене данными SNIP [Workgroup for Electronic Data Interchange Security and PrivacyWorkgroup (SNIP)]. Технические документы: WEDI-SNIP Введение в последнюю версию последнего правила защиты. Январь 2004 (WEDI-SNIP Introduction to Security Final Rule Final Version —January 2004): (требуется членство) http://www.wedi.org. WEDI-SNIP ЗАЩИТА: Технические документы для прояснения журнала аудита. Версия 5.0, Ноябрь 7, 2003 (WEDI-SNIP SECURITY: Audit Trail Clarification White Paper Version 5.0 November 7, 2003) (требуется членство) http://www.wedi.org

8 Другие источники информации

8.1 Общие положения

Данный раздел содержит некоторые описания и ссылки на стандарты и другие источники информации, которые также рассматривают перечни возможностей защиты МЕДИЦИНСКИХ ПРИБОРОВ или приложений. Центральные темы каждого из этих источников незначительно отличаются и потому, эти источники следует применять внимательно, учитывая их исходный контекст.

8.2 Заявление производителя о раскрытии информации о защите медицинского прибора (MDS2)

Заявление производителя о раскрытии информации о защите медицинского прибора — разработано HIMSS для получения ВОЗМОЖНОСТЕЙ ЗАЩИТЫ МЕДИЦИНСКОГО ПРИБОРА. Данная форма в настоящий момент обсуждается на ПРОЦЕССЕ открытого международного согласования, контролируемом NEMA и HIMSS. См. http://www.himss.org/content/files/MDS2FormInstructions.pdf.

8.3 Анкета о защите приложений (ASQ)

Анкета о защите приложений разработана HIMSS для получения возможностей обеспечения защиты и неприкосновенности частной жизни для информационных систем. См. http://www.himss.org/asp/topics_FocusDynamic.asp?faid=212.

8.4 Комиссия по сертификации для информационных технологий в здравоохранении (CCHIT)

Сертификационная комиссия для информационных технологий в здравоохранении (CCHIT) является признанным аттестационным органом (RCB), занимающимся электронными медицинскими архивами и связанными с ними сетями, а также является независимой, добровольной, частной инициативой.

Нашей миссией является ускорение освоения медицинских информационных технологий посредством создания действенной, надежной и поддерживаемой программы сертификации.

8.5 Функциональный электронный медицинский архив (EHR), http://www.cchit.org/get_certifiedHL7

Целью рабочей группы EHR является осуществление миссии HL7 по проектированию стандартов для поддержки обмена информацией о клинических решениях и терапиях, а также с целью заложить основу для общенациональной ИНТЕОПЕРАБЕЛЬНОСТИ, тем самым, предоставляя общеязыковые параметры, которые могут использоваться при разработке систем, поддерживающих электронные архивы. См. http://www.hl7.org/ehr/.

8.6 Общие критерии ИСО/МЭК 15408

Общие критерии. ИСО/МЭК 15408 (все части), в которых содержится описание функциональных возможностей системы.

9 Стандарты и подходы

В настоящем стандарте используются ссылки на стандарты и подходы, список которых предоставлен в Библиографии. Описанные ниже организации являются источниками дополнительной информации.

NSA — Агентство национальной безопасности Соединенных Штатов (US National Security Agency).
Руководства NSA по конфигурации систем защиты,
http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml

IETF — Рабочая группа инженеров Интернет (The Internet Engineering Task Force)
Документы:
Рабочая группа сети RFC 5246, Август 2008, Протокол TLS Версия 1.2 (Network Working Group RFC 5246 August 2008: The TLS Protocol Version 1.2),
http://www.ietf.org/rfc/rfc5246.txt

SANS — SANS — институт системного администрирования, аудита, сети и защиты [The SANS (SysAdmin, Audit, Network, Security) Institute], http://www.sans.org.
Проект политики защиты института SANS (The SANS Security Policy Project) — «...все, что вам необходимо для стремительного развития и реализации политики защиты информации..», http://www.sans.org/resources/policies/.
Читальный зал для литературы по информационной защите института SANS, http://www.sans.org/reading_room/.
Словарь по защите SANS, http://www.sans.org/securityresources/glossary.php.

WEDI — Рабочая группа по защите и неприкосновенности частной жизни в электронном обмене данными SNIP [Workgroup for Electronic Data Interchange Security and PrivacyWorkgroup (SNIP)].
Технические документы:
WEDI-SNIP Введение в последнюю версию последнего правила защиты. Январь 2004 (WEDI-SNIP Introduction to Security Final Rule Final Version — January 2004),
(требуется членство).
WEDI-SNIP ЗАЩИТА. Технические документы для разъяснения журнала аудита. Версия 5.0, 7 ноября 2003 (WEDI-SNIP SECURITY: Audit Trail Clarification White Paper Version 5.0 November 7, 2003), (требуется членство).

IHE — Интеграция учреждения здравоохранения (IHE Integrating the Healthcare Enterprise), http://www.ihe.net/Technical_Framework/.
Профиль IHE ATNA (Профиль интеграции журнала аудита и аутентификации узлов) [Audit Trail and Node Authentication Integration Profile].
IHE EUA (Аутентификация корпоративных пользователей) [Enterprise User Authentication].
IHE RAD TF (Журнал аудита рентгенологии) предварительная версия для открытого обсуждения [(Radiology Audit Trail) draft version for public comment].

Приложение А
(справочное)

Типовой сценарий, демонстрирующий обмен информацией о защите

А.1 Обмен информацией о характеристиках защиты. Введение

Настоящее приложение содержит документы, обмен которыми осуществляется на первом этапе обмена информацией о характеристиках защиты между гипотетическим производителем МЕДИЦИНСКОГО ПРИБОРА (ПМП — корпорация Виджет) и медицинской организацией (МО — больница Нью Тауна). Рассматриваемое изделие — Рабочая станция DICOM, называемая «FOOBAR 2.0».

ПМП получил запрос от МО на предоставление информации о FOOBAR 2.0 по МЭК 80001. А.2 содержит начальное взаимодействие ПМП о ВОЗМОЖНОСТЯХ ЗАЩИТЫ FOOBAR 2.0. Далее следует пересмотр «предложенных» МО характеристик защиты, вместе с ее комментариями и дополнительными вопросами.

Настоящее приложение содержит простой пример, демонстрирующий, какую информацию ПМП FOOBAR предоставило бы медицинской организации, рассматривающей приобретение или интеграцию FOOBAR. Подобная информация может быть предоставлена ПМП по соглашению о неразглашении с МО или ПМП может опубликовать возможности на интернет-сайте МО. Как бы там ни было, это будет являться первым «предложением» с подробной информацией о ВОЗМОЖНОСТЯХ ЗАЩИТЫ рассматриваемого МЕДИЦИНСКОГО ПРИБОРА. Подобным же образом ответ МО является первым ответом для ПМП, предназначенным определить области общего соглашения и понимания, проблемы, которые не были очевидны в документе, и вопросы, которые необходимо разрешить в последующих взаимодействиях

Разумеется, соглашение о приобретении, установке и сопровождении включает в себя гораздо больше информации. В качестве общего контекста для данного примера упрощенного приобретения МЕДИЦИНСКОГО ПРИБОРА и, в дальнейшем, проекта подключения FOOBAR к медицинской ИТ СЕТИ были выделены основные шаги, которым можно следовать при выполнении МЕНЕДЖМЕНТА РИСКА для защиты (более подробную информацию см. в МЭК 80001-1):

a) МО запрашивает или находит сводную информацию о характеристиках защиты ПМП (раздел А.2);

b) МО исследует отчет о характеристиках защиты FOOBAR и дает письменный ответ раздел А.3);

c) МО связывается с ПМП и получает ответы, касающиеся деталей, не раскрытых в отчете о FOOBAR;

d) МО принимает решение приобрести прибор и ПМП решает разрешить это приобретение, откладывая рассмотрение некоторых элементов приобретения на потом. МО принимает решение о добросовестности ПМП как партнера, основываясь на полученных данных о защите и диалоге с самим ПМП;

e) осуществляются различные элементы планирования и выполнения проекта, включая четкое СОГЛАШЕНИЕ об ОТВЕТСТВЕННОСТИ с учетом МЕНЕДЖМЕНТА РИСКА подключения к ИТ СЕТИ. МО и ПМП не скрывают информацию о том, как должен осуществляться менеджмент различных РИСКОВ. Менеджмент некоторых рисков осуществляется характеристиками защиты самого прибора, а ослабление других требует использование средств МО для управления защитой (технически и/или административно). Для подготовки осуществляется предварительная оценка ОСТАТОЧНОГО РИСКА. Данный шаг может входить в приобретение, но также может и предшествовать ему;

f) МО приобретает систему FOOBAR и контракты для поддержки проекта по подключению/интеграции;

g) МО проводит анализ РИСКОВ и выявляет и осознает ОСТАТОЧНЫЙ РИСК. В тех случаях, когда РИСК является допустимым, с учетом пользы от подключения FOOBAR, выполняется проект по интеграции прибора, подключаемого к МЕДИЦИНСКОЙ ИТ СЕТИ МО;

h) FOOBAR действует в условиях менеджмента РИСКА, как часть МЕДИЦИНСКОЙ ИТ СЕТИ МО;

i) вместе с необходимыми соглашениями с поставщиками услуг для FOOBAR начинается выполнение постоянных действий, связанных с возникающими уязвимостью, контролем, УПРАВЛЕНИЕМ СОБЫТИЯМИ;

j) списывание устройств и систем хранения рассматривается в процедурах, содержащих требования к уничтожению данных, ведению журнала и аудиту ПРОЦЕССА списывания.

Примечание — Это типовой вариант развития событий с соглашением только двух сторон. В реальной жизни могут участвовать другие вовлеченные стороны, такие как вендоры, специалисты-интеграторы сторонней организации и т. п. По каждому фактическому шагу будет приниматься решение индивидуально.

Для того чтобы было понятно, что представленный ниже текст является примером гипотетического обмена информацией, страницы документа, полученного от производителя (ПМП) и содержащего характеристики защиты, выделены синей рамкой. Страницы документа, который больница (МО) отправляет ПМП и который содержит ответ о характеристиках защиты, имеют оранжевую рамку.

***Отказ от ответственности**. Данный вариант развития событий предоставляется без гарантии, в явной или не явной форме, включая, но не ограничиваясь, любыми гарантиям о годности к продаже, завершен-*

ности и пригодности для определенной цели. Весь РИСК в отношении качества и рабочих характеристик предоставленной информации ложиться на вас.

В примере описан вымышленный прибор (FOOBAR 2.0), а также данный пример предназначен предложить способ инициации диалога о защите между ПМП и МО.

А.2 Отчет производителя (ПМП) о характеристиках защиты. «Предложение»

Последующие страницы являются заявлением ПМП о защите изделия FOOBAR 2.0, организованным в соответствии с рекомендациями Технического Отчета о Защите из МЭК 80001-1 (рекомендация настоящего стандарта). Данное заявление начинается с выражения заинтересованности медицинской организации. ПМП отвечает на нее (электронным) письмом с прикрепленным к нему документом, содержащим характеристики защиты FOOBAR 2.0.

Джоан Ковальски, CISSP
Сотрудник службы ИТ защиты
Больница общего профиля Нью Тауна
Дорогая мисс Ковальски,

Благодарим Вас за проявленный интерес к рабочей станции FOOBAR 2.0 DICOM PACS. Мы получили подписанное вами соглашение о неразглашении и настоящим направляем Вам копию, подписанную нами.

Вы также найдете в письме подробную информацию о защите FOOBAR 2.0, представленную в форме, соответствующей Техническому отчету о защите по МЭК 80001-1. Мы всегда стараемся соблюдать ясность и последовательность в общении с нашими клиентами по проблемам риска в вопросах защиты, и я уверен, что данный конфиденциальный документ соответствует вашим потребностям.

Конечно же, защита может быть очень сложной проблемой в случае подключения нового медицинского прибора к ИТ сети больницы. Мы надеемся продолжить работать с Вами для разрешения любых вопросов или проблем, с которыми Вы столкнетесь при рассмотрении вопроса приобретения и интеграции нашего изделия в Вашу Медицинскую ИТ сеть.

Благодарим Вас за проявленный интерес к использованию продукции Корпорации Виджет в ваших технологических планах. Мы надеемся работать с Вами над этим важным приобретением и полной интеграцией изделия в действующую сеть.

Пожалуйста, дайте мне знать, если у Вас имеются какие-либо вопросы касательно наших функциональных возможностей защиты и/или рисков, которые могут возникать в этом современнейшем изделии.

С наилучшими пожеланиями,
Хосе Армас
Менеджер по продажам продукции FOOBAR,
Корпорация Виджет
копия:
1 Подписанное с двух сторон Соглашение о неразглашении, датируемое 1 мая, 2010 г.
2 Отчет о характеристиках защиты FOOBAR 2.0 (МЭК 80001-1).

Документ, содержащий характеристики защиты FOOBAR 2.0, описанные в соответствии с МЭК 80001-1. Предложение ПРОИЗВОДИТЕЛЯ

А. Краткое определение предусмотренного Назначения прибора FOOBAR 2.0

Усовершенствованная станция наблюдения DICOM «FOOBAR 2.0» подсоединена к сети DICOM и позволяет ее пользователям получать доступ к изображениям и данным DICOM 3.0, находясь за пределами рентгенологического отделения или центра визуализации, для того, чтобы проводить анализ подобных медицинских отчетов и изображений.

FOOBAR 2.0 способен выбирать медицинские данные либо из предназначенного для этой цели удаленного архива, существующего в сети DICOM или из местного жесткого диска.

Благодаря возможностям своей собственной памяти, FOOBAR 2.0 может отображать медицинские данные, даже находясь за пределами сети DICOM.

В прибор включены возможности защиты, которые обеспечивают управление доступом к данным медицинской визуализации, в зависимости от привилегий пользователя; записи о получении доступа вносятся в журнал аудита.

В. Подробная спецификация ВОЗМОЖНОСТЕЙ ЗАЩИТЫ

В подробно описанных ниже возможностях защиты каждая возможность обозначена четырехбуквенным акронимом ВОЗМОЖНОСТИ ЗАЩИТЫ. Чтобы облегчить обмен информацией о конкретных характеристиках ВОЗМОЖНОСТИ ЗАЩИТЫ, каждой характеристики назначен идентификатор, составленный из идентификатора и порядкового номера из двух цифр. Это предназначено помочь в обсуждениях и письменном обмене информацией о конкретных характеристиках.

ALOF. Автоматический выход из системы

Цель. Уменьшить РИСК получения несанкционированного доступа к ДАННЫМ о ЗДОРОВЬЕ с рабочего места, оставленного без присмотра. Предотвратить неправильное использование, если система или рабочее место не используется в течение некоторого периода времени.

Идентификатор	Возможность
/ALOF.01/	Хранитель экрана запускается автоматически через пять минут после последнего удара по клавише/движения мышью. Замечание — Местный авторизованный ИТ администратор может задать время задержки для данного действия и даже отключать хранитель экрана
/ALOF.02/	Хранитель экрана очищает все отображаемые ДАННЫЕ о ЗДОРОВЬЕ с экрана
/ALOF.03/	Хранитель экрана не выводит пользователя из системы/не прекращает сеанс
/ALOF.04/	Пользователю требуется снова войти в систему после активации хранителя экрана
/ALOF.05/	Сеанс пользователя завершается автоматически через 60 минут после последнего удара клавиши/движения мышью/взаимодействия с сенсорным экраном. Замечание — Местный авторизованный ИТ администратор может задать время задержки для данного действия и даже отключать автоматический выход из системы

AUDT. Средства управления аудитом

Цель. Установить согласованный подход к надежному аудиту того, кто и что делает с ДАННЫМИ О ЗДОРОВЬЕ, чтобы позволить ИТ отделу МО контролировать использование этих данных, применяя общеизвестные подходы, стандарты и технологию.

Идентификатор	Возможность
/AUDT.01/	О получении доступа, модификации или удалении любых ДАННЫХ о ЗДОРОВЬЕ делается запись, которая хранится в специализированном архиве DICOM
/AUDT.02/	О загрузке ДАННЫХ о ЗДОРОВЬЕ (в собственную память прибора) делается запись, которая хранится в специализированном архиве DICOM
/AUDT.03/	В случае, если прибор используется за пределами сети DICOM, то доступ к любым ДАННЫМ о ЗДОРОВЬЕ хранится в собственной памяти прибора
/AUDT.04/	После повторного подсоединения прибора к DICOM-сети, журнал аудита, который велся во внутренней памяти прибора во время автономной работы, синхронизируется со специализированным удаленным архивом DICOM
/AUDT.05/	Ссылается на /CNFS.01/: все изменения ВОЗМОЖНОСТЕЙ ЗАЩИТЫ фиксируются в журнале аудита прибора

CNFS. Конфигурация свойств системы защиты

Цель. Дать МО возможность определять, как задействовать ВОЗМОЖНОСТИ ЗАЩИТЫ изделия, чтобы удовлетворить их требования к политике и/или рабочему процессу.

Идентификатор	Возможность
/CNFS.01/	Местный авторизованный ИТ администратор может устанавливать/отключать доступные ВОЗМОЖНОСТИ ЗАЩИТЫ прибора
/CNFS.02/	Ссылается на /AUDT.05/: в случае, когда местный авторизованный ИТ администратор устанавливает/отключает/изменяет настройки доступных ВОЗМОЖНОСТЕЙ ЗАЩИТЫ прибора, его действие фиксируется в журнале аудита

DTBK. Резервное копирование данных и аварийное восстановление

Цель. Обеспечить возможность для поставщика медицинских услуг продолжать вести свое предприятие после повреждения или уничтожения данных, оборудования или программного обеспечения.

Идентификатор	Возможность
/DTBK.01/	FOOBAR 2.0 предоставляет (встроенную) функцию резервного копирования для хранения системных настроек на внешнем подключаемом запоминающем устройстве большой емкости (например, на USB-накопителе)
/DTBK.02/	FOOBAR 2.0 предоставляет (встроенную) функцию резервного копирования для хранения журналов аудита на внешнем подключаемом запоминающем устройстве большой емкости (например, на USB-накопителе)
/DTBK.03/	Журналы аудита соответствующим образом шифруются для предотвращения потери конфиденциальной информации, содержащей ДАННЫЕ о ЗДОРОВЬЕ (такие как имя пациента, DOB и т. д.)
/DTBK.04/	Резервное восстановление хранящихся локально ДАННЫХ о ЗДОРОВЬЕ может быть выполнено только с возвращением данных на специализированный удаленный архив DICOM. Логическое обоснование. Для обеспечения сохранения непротиворечивости ДАННЫХ о ЗДОРОВЬЕ требуется ограничивающий функционал

DIDT. Идентификация ДАННЫХ О ЗДОРОВЬЕ

Цель. Способность оборудования (прикладного программного обеспечения или дополнительного инструментария) непосредственно удалять информацию, позволяющую идентифицировать ПАЦИЕНТОВ.

Идентификатор	Возможность
/DIDT.01/	FOOBAR 2.0 не поддерживает никакие средства прямого удаления информации, которые позволяют идентифицировать ПАЦИЕНТА

STCF. Конфиденциальность хранения ДАННЫХ о ЗДОРОВЬЕ

Цель. Производитель принимает необходимые меры для того, чтобы несанкционированный доступ не нарушал целостность и конфиденциальность ДАННЫХ о ЗДОРОВЬЕ, хранящихся на изделиях или съемных носителях.

Идентификатор	Возможность
/STCF.01/	ДАННЫЕ о ЗДОРОВЬЕ, хранящиеся в собственной памяти FOOBAR 2.0 зашифрованы. Использующийся алгоритм: AES (Rijndael), Стойкость шифрования: 256 БИТ. Замечание — Данная настройка не может быть изменена местным ИТ администратором
/STCF.02/	Защищенные/зашифрованные ДАННЫЕ о ЗДОРОВЬЕ доступны только после удачной загрузки. См. также /MLDP.04/
/STCF.03/	Дешифруются только требующиеся ДАННЫЕ о ЗДОРОВЬЕ (требующиеся для текущего взаимодействия/использования/отображения). Неиспользуемые на данный момент ДАННЫЕ о ЗДОРОВЬЕ остаются зашифрованными
/STCF.04/	Загрузочный раздел, операционная система, временные данные или внутреннее запоминающее устройство большой емкости и т. д. также шифруются. Используемый алгоритм: AES (Rijndael), Стойкость шифрования: 256 БИТ. Замечание — Данная настройка не может быть изменена местным ИТ администратором
/STCF.05/	Случайные сбои питания в системе не влияют на шифрование ДАННЫХ о ЗДОРОВЬЕ, хранящихся на запоминающем устройстве большой емкости. Не при каких обстоятельствах выполнения работы незашифрованные ДАННЫЕ о ЗДОРОВЬЕ не присутствуют на внутреннем запоминающем устройстве большой емкости
/STCF.06/	Соединение со специализированным удаленным архивом, находящимся в сети DICOM, может быть установлено с помощью VPN

EMRG. Экстренный доступ

Цель. Обеспечить возможность доступа к охраняемым ДАННЫМ О ЗДОРОВЬЕ в случае экстренной ситуации, требующей немедленного доступа к хранящимся ДАННЫМ О ЗДОРОВЬЕ.

Идентификатор	Возможность
/EMRG.01/	Наличие функции разбивания стекла. Даже без персонального идентификатора (id) пользователя и медицинской аутентификации пользователь может получить доступ к ДАННЫМ о ЗДОРОВЬЕ. Замечание — Необходимо помнить, что данная функция может быть изменена/отключена местным ИТ администратором
/EMRG.02/	Использование функции разбивания стекла /EMRG.01/ требует использование общего идентификатора (id) пользователя и аутентификации (для предотвращения получения доступа к ДАННЫМ о ЗДОРОВЬЕ пациентами или сторонними наблюдателями)
/EMRG.03/	Каждое использование функции разбивания стекла /EMRG.01/ будет занесено в журнал аудита
/EMRG.04/	О каждом использовании функции разбивания стекла /EMRG.01/ может автоматически создаваться отчет для установления учетной записи пользователя, например посредством электронной почты (eMail)

SGUD. Руководства по защите

Цель. Обеспечить доступность руководства по защите для ОПЕРАТОРОВ и администраторов системы. Желательно предоставление отдельных пособий для ОПЕРАТОРОВ и АДМИНИСТРАТОРОВ (включая отдел продаж и обслуживания ПМП), так как это позволяет только администраторам сохранять за собой понимание всего административного функционала.

Идентификатор	Возможность
/SGUD.01/	Руководство по защите для ОПЕРАТОРА включено в инструкции по использованию FOOBAR 2.0. См. главу 13
/SGUD.02/	Руководство по защите для администратора включено в техническую информацию FOOBAR 2.0. См. главу 17

IGAU. Целостность и достоверность ДАННЫХ о ЗДОРОВЬЕ

Цель. Обеспечить сохранность ДАННЫХ О ЗДОРОВЬЕ от изменения или уничтожения несанкционированными методами, а также гарантировать, что эти данные поступили от их создателя. Обеспечить целостность ДАННЫХ О ЗДОРОВЬЕ.

Идентификатор	Возможность
/IGAU.01/	ДАННЫЕ о ЗДОРОВЬЕ, хранящиеся в памяти большой емкости FOOBAR 2.0 для отображения данных за пределами сети DICOM, защищены с помощью надлежащей контрольной суммы (SHA1), чтобы обеспечить целостность данных
/IGAU.02/	Предоставлены ВОЗМОЖНОСТИ по резервному копированию. См. главу, посвященную DTBK: Резервное копирование данных и аварийное восстановление

MLDP. Обнаружение вредоносного программного обеспечения и защита от него

Цель. Изделие обеспечивает потребности регулирования, а также МО и пользователя, в обеспечении эффективной и единой поддержки предотвращения, обнаружения и удаления вредоносного программного обеспечения. Это является неотъемлемым шагом в обеспечении надлежащего глубокого подхода к защите.

Идентификатор	Возможность
/MLDP.01/	Все несущественные порты сети FOOBAR 2.0 закрыты. Замечание 01 — Более подробную информацию см. в технической информации FOOBAR 2.0, в руководстве по защите для администратора (глава 17). См. /SGUD.02/ Замечание 02 — Данная функциональная возможность не может быть изменена местным ИТ администратором
/MLDP.02/	Операционная система, установленная на загрузочном устройстве FOOBAR 2.0, защищена от санкционированных/несанкционированных изменений. После перезагрузки система возвращается в свое изначальное состояние. Замечание — Данная функциональная возможность не может быть изменена местным ИТ администратором

Окончание

Идентификатор	Возможность
/MLDP.03/	Все значимые файлы защищены с помощью надлежащей контрольной суммы (SHA1) и проверяются при загрузке. В случае обнаружения ошибки система не запускается, а выдает сообщение об ошибке. Замечание — Данная функциональная возможность не может быть изменена местным ИТ администратором
/MLDP.04/	Защищенные/зашифрованные ДАННЫЕ о ЗДОРОВЬЕ доступны только после успешной загрузки. См. также /STCF.01/. Замечание — Данная функциональная возможность не может быть изменена местным ИТ администратором

PAUT. Аутентификация личности

Цель. Политика аутентификации должна быть гибкой для того, чтобы адаптироваться к местной ИТ политике МО. Требование аутентификации личности при предоставлении доступа к ДАННЫМ О ЗДОРОВЬЕ должно быть логически обоснованным в каждом конкретном случае.

Идентификатор	Возможность
/PAUT.01/	FOOBAR 2.0 поддерживает местное и глобальное управление учетными записями. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0, в руководстве по защите для администратора (глава 17)
/PAUT.02/	FOOBAR 2.0 поддерживает закрытие учетных записей. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0, в руководстве по защите для администратора (глава 17)
/PAUT.03/	FOOBAR 2.0 поддерживает быстрое переключение пользователей. Поддержка данной функции уменьшает затраты времени на задачу входа и выхода пользователей из системы

PLOK. Физические замки на приборе

Цель. Гарантировать, что несанкционированный доступ не нарушит конфиденциальность, целостность и доступность ДАННЫХ о ЗДОРОВЬЕ, хранящихся на изделиях или съемных носителях.

Идентификатор	Возможность
/PLOK.01/	По причине выбранного метода шифрования FOOBAR 2.0 не требуются физическое запирание

CSUP. Усовершенствование системы защиты изделия от кибератак

Цель. Создать унифицированный метод выполнения работы. Установка/усовершенствование пакетов исправлений для системы защиты выполняется персоналом на рабочем месте, и, вероятно, санкционированным персоналом МО (в случае установки скачиваемых пакетов исправлений).

Идентификатор	Возможность
/CSUP.01/	Настоящим документом мы подтверждаем, что компания осуществляет внутренние процедуры для обследования рынка для определения текущих тенденций в области защиты от кибератак. В случае необходимости пакетов исправлений можно обращаться к технической поддержке. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0, в руководстве по защите для администратора (глава 17)
/CSUP.02/	Прибор спроектирован так, что мы (производитель) не позволяем МО устанавливать какие-либо несанкционированные патчи

RDMP. Влияние компонентов третьей стороны на весь жизненный цикл изделия

Цель. Планы ПМП предполагают, что их изделия считаются поддерживаемыми на протяжении их жизненного цикла, в соответствии с внутренним системам контроля качества и внешнему регламенту.

Идентификатор	Возможность
/RDMP.01/	Настоящим документом мы подтверждаем, что предоставляем сопровождение/поддержку системы на протяжении предположительного срока службы изделия. В случае необходимости сопровождения/ремонта/пакетов исправлений можно обращаться к технической поддержке. Замечание — Более подробную информацию см. в технической информации о FOOBAR 2.0 (глава 42)

SAHD. Усиление защиты системы и приложений

Цель. Минимизировать векторы атак и совокупную площадь атак посредством закрытия портов; удаления службы и т. д.

Идентификатор	Возможность
/SAHD.01/	Все ВОЗМОЖНОСТИ, предназначенные обеспечить стабильную систему, предоставляющую только те службы, которые установлены ПРЕДНАЗНАЧЕННЫМ ИСПОЛЬЗОВАНИЕМ и требуются для его осуществления с минимумом сопроводительной деятельности, а также для того, чтобы позволить поставщикам медицинских услуг/МО организациям подключить FOOBAR 2.0 к их сети рассматриваются в главе MLDP: Обнаружение вредоносного программного обеспечения и защита от него в технической информации о FOOBAR 2.0 (глава 38)

AUTH. Авторизация

Цель. Следуя принципу минимизации данных, предоставить управление доступом к ДАННЫМ О ЗДОРОВЬЕ и функциям в только той степени, насколько это необходимо для выполнения задач МО в соответствии с ПРЕДНАЗНАЧЕННЫМ ИСПОЛЬЗОВАНИЕМ прибора.

Идентификатор	Возможность
/AUTH.01/	Несмотря на описанные ниже административные функции, только персонал, санкционированный нами (производителем), имеет доступ к служебным функциям и функциональным возможностям. Кроме административных задач, разрешенных технической документацией, несанкционированному персоналу запрещается осуществлять дальнейший ремонт. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0
/AUTH.02/	Так называемый вход в систему в качестве администратора предоставляется в случае FOOBAR 2.0 для: - общего администрирования сервера; - установки обновлений/решения проблем; - добавления большого количества клиентов FOOBAR; - администрирования главных пользователей; - операций по резервному копированию
/AUTH.03/	Так называемый вход в качестве главного пользователя (Master User) настраивается заранее и может быть добавлен для: - внесения поправок в/объединения отчетов/данных пациентов; - восстановления потерянных отчетов; - администрирования общих пользователей; - редактирования и поддержки общей конфигурации применения FOOBAR

TXDF. Конфиденциальность передачи данных

Цель. ПРОИЗВОДИТЕЛЬ демонстрирует, что его оборудование соответствует множеству национальных стандартов и регламентов (например, USA HIPAA, национальным законам, основанным на EU 95/46/EC) в соответствии с потребностями МО для обеспечения конфиденциальности передаваемых ДАННЫХ О ЗДОРОВЬЕ.

Идентификатор	Возможность
/TXDF.01/	См. /STCF.06/. Соединение со специализированным удаленным архивом, находящимся в сети DICOM, может быть установлено с помощью VPN. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0 (глава 33)

Окончание

Идентификатор	Возможность
/TXDF.02/	По требованию. Мы (производитель) предоставим сертификаты, демонстрирующие соответствие действующему национальному регламенту. Так как подобные сертификаты варьируются в зависимости от страны, пожалуйста, обратитесь к технической службе для получения большей информации

TXIG. Целостность передачи данных

Цель. Прибор должен обеспечивать защиту целостности передаваемых ДАННЫХ о ЗДОРОВЬЕ.

Идентификатор	Возможность
/TXIG.01/	См. /STCF.06/: Соединение со специализированным удаленным архивом, находящимся в сети DICOM, может быть установлено с помощью VPN. Данная функциональная возможность гарантирует сохранение целостности ДАННЫХ о ЗДОРОВЬЕ на протяжении передачи данных и позволяет FOOBAR 2.0 передавать ДАННЫЕ о ЗДОРОВЬЕ через относительно открытые сети или окружение, в котором действует крепкая политика обеспечения целостности ДАННЫХ о ЗДОРОВЬЕ. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0 (глава 33)

А.3 Ответное сообщение МО на отчет о характеристиках системы защиты ПМП. «Ответ»

Представленный ниже текст является ответом Больницы Нью Тауна (МО) на заявление ВОЗМОЖНОСТЕЙ ЗАЩИТЫ изделия корпорации Виджет (ПМП) (представленном в А.2).

В целом Нью Таун доволен информацией о защите в том виде, в каком она была представлена, но существует несколько моментов и вопросов, которые следует разрешить перед тем как сотрудник службы ИТ защиты Нью Тауна предоставит закупочному комитету одобрение на совершение покупки.

Сотрудник службы ИТ защиты больницы Нью Тауна дает ответ, содержащий документ с характеристиками защиты FOOBAR 2.0 с комментариями (в крайней правой колонке, выделенными синим цветом). Ответ начинается с (электронного) письма.

Хосе Армас
Менеджер по продажам продукции FOOBAR
Корпорация Виджет

Дорогой, мистер Армас,

Благодарю Вас за подробный ответ на мой запрос информации о защите рабочей станции DICOM PACS FOOBAR 2.0 корпорации Виджет. Ваш, основанный на МЭК 80001-1 документ содержит множество полезной информации и является хорошим основанием для начала нашего проекта приобретения и установки перед подключением Рабочей станции PACS к медицинской ИТ-сети больницы Нью Тауна.

И хотя я высоко ценю ваши попытки привнести ясность и прозрачность в вопрос риска, у меня имеется несколько замечаний и вопросов. Я позволила себе добавить еще одну колонку к вашему документу с комментариями, расположенную справа от вашего описания характеристик защиты. В местах, где, по моему мнению, не достает свойства, я добавила ряд в соответствующий раздел. Кроме того, там, где мной было подтверждена возможность и ее необходимость для удовлетворения наших нужд, стоит комментарий «Принято к сведению». И хотя мы еще не готовы «Принять» эти возможности, мне представилось удобным использовать данное письмо для сосредоточения нашего внимания на других, более важных проблемах нашего первого обсуждения.

После того как вы пересмотрите прикрепленный документ, я предлагаю провести телеконференцию для разрешения пунктов, которые не сложно прояснить по телефону. В случае если отдел рентгенологии и отдел закупок больницы Нью Тауна решат приобрести и установить ваше оборудование, у нас появится множество возможностей для дальнейшего подробного рассмотрения рисков для защиты и средств ослабления рисков для планирования и реализации проекта интеграции.

Мое управление свяжется с Вами по вопросу последующего телефонного обсуждения.

С уважением, Джоан Ковальски, CISSP
Сотрудник службы ИТ защиты
Больница общего профиля Нью Тауна

Копия:
Ответ больницы Нью Тауна на отчет о характеристиках защиты FOOBAR 2.0 (МЭК 80001-1).

Характеристики защиты FOOBAR 2.0
— Ответ больницы Нью Тауна на предложение корпорации Виджет—

Данный пример содержит первую реакцию вымышленной медицинской организации — больницы общего профиля Нью Тауна. Данная МО обдумывает приобретение нескольких приборов FOOBAR 2.0. Данный раздел документа описывает реакцию/вопросы/проблемы в заявлении защиты производителя МЕДИЦИНСКОГО ПРИБОРА FOOBAR 2.0.

A Краткое описание больницы

Больница общего профиля Нью Тауна предлагает услуги в разных областях медицины. Дополнительный технический персонал оказывает поддержку практикующим врачам в областях неприкосновенности частной жизни и защиты. Рабочая станция FOOBAR будет установлена в пульмонологическом отделении интенсивной терапии для использования пульмонологами и консультантами по рентгенологии.

B Краткое описание сети

Сеть разделена на сегменты общей сети и сегменты специальной сети для медицинских изделий.

Администрирование системы и сети осуществляется местной командой хорошо обученных сетевых администраторов. Имеется программа обучения по вопросам юридических аспектов медицинских изделий.

C Краткое описание аспектов защиты

Стратегия обеспечения защиты сети полагается на смешенную стратегию охраны и контроля с помощью сенсорной сети.

Определенные области сети охраняются с помощью защитного оборудования для предотвращения заражения вредоносным программным обеспечением. Вся сеть целиком контролируется сенсорными сетями, которые уведомляют о заражениях вредоносным программным обеспечением, превышающих пороговый уровень.

Просим вас обратить внимание, что текст, выделенный **ЧЕРНЫМ**, представленный ниже в разделе 4, был предоставлен корпорацией Виджет для их прибора FOOBAR 2.0. Текст комментариев, выделенных СИНИМ *курсивом*, представленный ниже, является ответом персонала службы защиты больницы Нью Тауна.

D Подробная спецификация ВОЗМОЖНОСТЕЙ ЗАЩИТЫ

ALOF. Автоматический выход из системы

Цель. Уменьшить РИСК получения несанкционированного доступа к ДАННЫМ о ЗДОРОВЬЕ с рабочего места, оставленного без присмотра. Предотвратить неправильное использование, если система или рабочее место не используется в течении периода времени.

Идентификатор	Возможность	*Комментарии/потребности МО*
/ALOF.01/	Хранитель экрана запускается автоматически через пять минут после последнего удара по клавише/ движения мышью. Замечание — Местный авторизованный ИТ администратор может задать время задержки для данного действия и даже отключать хранитель экрана	*Принято к сведению МО* *Желателен более долгий период времени, так как диагностические операции имеют перерывы*
/ALOF.02/	Хранитель экрана очищает все отображаемые ДАННЫЕ о ЗДОРОВЬЕ с экрана	*Принято к сведению МО*
/ALOF.03/	Хранитель экрана не выводит пользователя из системы/не прекращает сеанс	*Принято к сведению МО*
/ALOF.04/	Пользователю требуется снова войти в систему после активации хранителя экрана	*Принято к сведению МО*
/ALOF.05/	Сеанс пользователя завершается автоматически через 60 мин после последнего удара клавиши/ движения мышью/взаимодействия с сенсорным экраном Замечание — Местный авторизованный ИТ администратор может задать время задержки для данного действия и даже отключать автоматический выход из системы	*Принято к сведению МО*

Окончание

Идентификатор	Возможность	*Комментарии/потребности МО*
		Дополнительно. Желательно, чтобы главная учетная запись обладала более высоким приоритетом чем учетная запись пользователя и могла войти в диалоговое окно сохраненного экрана

AUDT. Средства управления аудитом

Цель. Установить согласованный подход к надежному аудиту того, кто что делает с ДАННЫМИ о ЗДОРОВЬЕ, чтобы позволить ИТ отделу МО контролировать использование этих данных, используя общеизвестные подходы, стандарты и технологию.

Идентификатор	Возможность	*Комментарии/потребности МО*
/AUDT.01/	О получение доступа, модификации или удалении любых ДАННЫХ о ЗДОРОВЬЕ делается запись, которая хранится в специализированном архиве DICOM	*Для данного случая применения это свойство не требуется*
/AUDT.02/	О загрузке ДАННЫХ о ЗДОРОВЬЕ (в собственную память прибора) делается запись, которая хранится в специализированном архиве DICOM	*Для данного случая применения это свойство не требуется*
/AUDT.03/	В случае, если прибор используется за пределами сети DICOM, то доступ к любым ДАННЫМ о ЗДОРОВЬЕ хранится в собственной памяти прибора	*Для данного случая применения это свойство не требуется*
/AUDT.04/	После повторного подсоединения прибора к DICOM-сети, журнал аудита, который велся во внутренней памяти прибора во время автономной работы, синхронизируется со специализированным удаленным архивом DICOM	*Для данного случая применения это свойство не требуется*
/AUDT.05/	Ссылается на /CNFS.01/. Все изменения ВОЗМОЖНОСТЕЙ ЗАЩИТЫ фиксируются в журнале аудита прибора	*Для данного случая применения это свойство не требуется*

CNFS. Конфигурация свойств системы защиты

Цель. Дать МО возможность определять, как задействовать ВОЗМОЖНОСТИ ЗАЩИТЫ изделия, чтобы удовлетворить их требования к политике и/или рабочему процессу

Идентификатор	Возможность	*Комментарии/потребности МО*
/CNFS.01/	Местный авторизованный ИТ администратор может устанавливать/ отключать доступные ВОЗМОЖНОСТИ ЗАЩИТЫ прибора	*Принято к сведению МО*
/CNFS.02/	Ссылается на /AUDT.05/. В случае, когда местный санкционированный ИТ администратор устанавливает / отключает / изменяет настройки доступных ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ЗАЩИТЫ прибора, его действие фиксируется в журнале аудита	*Принято к сведению МО*
		МО не хватает важного свойства защиты (например, блокировки портов). Был создан план капиталовложений для расчета затрат на дополнительное оборудование, которое восполнило бы эти недостатки

DTBK. Резервное копирование данных и аварийное восстановление

Цель. Обеспечить возможность для поставщика медицинских услуг продолжать вести свое предприятие после повреждения или уничтожения данных, оборудования или программного обеспечения.

Идентификатор	Возможность	*Комментарии/потребности МО*
/DTBK.01/	FOOBAR 2.0 предоставляет (встроенную) функцию резервного копирования для хранения системных настроек на внешнем подключаемом запоминающем устройстве большой емкости (например, на USB-накопителе)	*Для данного случая применения это свойство не требуется*
/DTBK.02/	FOOBAR 2.0 предоставляет (встроенную) функцию резервного копирования для хранения журналов аудита на внешнем подключаемом запоминающем устройстве большой емкости (например, на USB-накопителе)	*Для данного случая применения это свойство не требуется*
/DTBK.03/	Журналы аудита соответствующим образом шифруются для предотвращения потери конфиденциальной информации, содержащей ДАННЫЕ о ЗДОРОВЬЕ (такие как имя пациента, DOB, и т. д.)	*Для данного случая применения это свойство не требуется*
/DTBK.04/	Резервное восстановление хранящихся локально ДАННЫХ о ЗДОРОВЬЕ может быть выполнено только с возвращением данных на специализированный удаленный архив DICOM. Логическое обоснование. Для обеспечения сохранения непротиворечивости ДАННЫХ о ЗДОРОВЬЕ требуется ограничивающий функционал	*Для данного случая применения это свойство не требуется*

DIDT. Идентификация ДАННЫХ О ЗДОРОВЬЕ

Цель. Способность оборудования (прикладного программного обеспечения или дополнительного инструментария) непосредственно удалять информацию, позволяющую идентифицировать ПАЦИЕНТОВ.

Идентификатор	Возможность	*Комментарии/потребности МО*
/DIDT.01/	FOOBAR 2.0 не поддерживает никакие средства прямого удаления информации, которые позволяют идентифицировать ПАЦИЕНТА	*Принято к сведению МО.* *Примечание — Для отдела закупок МО. Данная функциональная возможность прибора препятствует его использованию в исследованиях и преподавании*
		МО необходимо получить от ПМП точную спецификацию всех данных вложенных в файлы DICOM 3.0. Это незаменимо для написания собственных манипуляторов формата файлов организации (например, деидентификация, передача в исследовательский архив)

STCF. Конфиденциальность хранения ДАННЫХ о ЗДОРОВЬЕ

Цель. Производитель принимает необходимые меры для того, чтобы несанкционированный доступ не нарушал целостность и конфиденциальность ДАННЫХ о ЗДОРОВЬЕ, хранящихся на изделиях или съемных носителях.

Идентификатор	Возможность	*Комментарии/потребности МО*
/STCF.01/	ДАННЫЕ о ЗДОРОВЬЕ, хранящиеся в собственной памяти FOOBAR 2.0 зашифрованы. Использующийся алгоритм: AES (Rijndael), Стойкость шифрования: 256 БИТ. Замечание — Данная настройка не может быть изменена местным ИТ администратором	*Для МО требуется больше информации о ПРОЦЕССЕ генерации ключа.* *После того как генерация ключа производителем была завершена, необходимо выполнение ПРОЦЕССА, который бы разделял сторону, генерирующую ключ и тех, кто занимается аппаратной поддержкой, для предотвращения легальных проблем, связанных с неприкосновенностью частной жизни, в случаях, когда дефектный жесткий диск возвращается производителю для замены. Как выполняется управление ключом?*

Окончание

Идентификатор	Возможность	*Комментарии/потребности МО*
/STCF.02/	Защищенные/зашифрованные ДАННЫЕ о ЗДОРОВЬЕ доступны только после удачной загрузки. См. также /MLDP.04/	*Принято к сведению МО* *Требуется ли во время перезагрузки прибора вводить специальный пароль (какой либо еще кроме пароля учетной записи пользователя) для перехода в рабочее состояние?*
/STCF.03/	Дешифруются только требующиеся ДАННЫЕ о ЗДОРОВЬЕ (требующиеся для текущего взаимодействия/использования/отображения). Не используемые на данный момент ДАННЫЕ о ЗДОРОВЬЕ остаются зашифрованными	*Принято к сведению МО*
/STCF.04/	Загрузочный раздел, операционная система, временные данные или внутреннее запоминающее устройство большой емкости, и т. д. также шифруются. Используемый алгоритм: AES (Rijndael)/ Стойкость шифрования: 256 БИТ. Замечание — Данная настройка не может быть изменена местным ИТ администратором	*Принято к сведению МО*
/STCF.05/	Случайные сбои питания в системе не влияют на шифрование ДАННЫХ о ЗДОРОВЬЕ, хранящихся на запоминающем устройстве большой емкости. Не при каких обстоятельствах выполнения работы незашифрованные ДАННЫЕ о ЗДОРОВЬЕ не присутствуют на внутреннем запоминающем устройстве большой емкости	*Принято к сведению МО*
/STCF.06/	Соединение со специализированным удаленным архивом, находящимся в сети DICOM, может быть установлено с помощью VPN	*Принято к сведению МО*

EMRG. Экстренный доступ

Цель. Обеспечить возможность доступа к охраняемым ДАННЫМ о ЗДОРОВЬЕ в случае экстренной ситуации, требующей немедленного доступа к хранящимся ДАННЫМ о ЗДОРОВЬЕ.

Идентификатор	Возможность	*Комментарии/потребности МО*
/EMRG.01/	Наличие функции разбивания стекла. Даже без персонального идентификатора (id) пользователя и медицинской аутентификации пользователь может получить доступ к ДАННЫМ о ЗДОРОВЬЕ. Замечание — Необходимо помнить, что данная функция может быть изменена/отключена местным ИТ администратором	*Принято к сведению МО*
/EMRG.02/	Использование функции разбивания стекла /EMRG.01/ требует использование общего идентификатора (id) пользователя и аутентификации (для предотвращения получения доступа к ДАННЫМ о ЗДОРОВЬЕ пациентами или сторонними наблюдателями)	*Принято к сведению МО*
/EMRG.03/	Каждое использование функции разбивания стекла /EMRG.01/ будет занесено в журнал аудита	*Принято к сведению МО*
/EMRG.04/	О каждом использовании функции разбивания стекла /EMRG.01/ может автоматически создаваться отчет для установления учетной записи пользователя, например посредством электронной почты (eMail)	*Принято к сведению МО*

SGUD. Руководства по защите

Цель. Обеспечить доступность руководства по защите для ОПЕРАТОРОВ и администраторов системы. Желательно предоставление отдельных пособий для ОПЕРАТОРОВ и АДМИНИСТРАТОРОВ (включая отдел продаж и обслуживания ПМП), так как это позволяет только администраторам сохранять за собой понимание всего административного функционала.

Идентификатор	Возможность	*Комментарии/потребности МО*
/SGUD.01/	Руководство по защите для ОПЕРАТОРА включено в инструкции по использованию FOOBAR 2.0. См. главу 13	*Принято к сведению МО*
/SGUD.02/	Руководство по защите для администратора включено в техническую информацию FOOBAR 2.0. См. главу 17	*Принято к сведению МО*

IGAU. Целостность и достоверность ДАННЫХ о ЗДОРОВЬЕ

Цель. Обеспечить сохранность ДАННЫХ о ЗДОРОВЬЕ от изменения или уничтожения несанкционированными методами, а также гарантировать, что эти данные поступили от их создателя. Обеспечить целостность ДАННЫХ о ЗДОРОВЬЕ.

Идентификатор	Возможность	*Комментарии/потребности МО*
/IGAU.01/	ДАННЫЕ о ЗДОРОВЬЕ, хранящиеся в памяти большой емкости FOOBAR 2.0 для отображения данных за пределами сети DICOM, защищены с помощью надлежащей контрольной суммы (SHA1), чтобы обеспечить целостность данных	*МО осведомлена о недостатках алгоритма SHA1 и потому необходимо предоставить программное заявление о том, как производитель справляется с криптографическими проблемами защиты*
/IGAU.02/	Предоставлены ВОЗМОЖНОСТИ по резервному копированию. См. главу, посвященную DTBK: Резервное копирование данных и аварийное восстановление	*Принято к сведению МО*

MLDP. Обнаружение вредоносного программного обеспечения и защита от него

Цель. Изделие обеспечивает потребности регулирования, а также МО и пользователя, в обеспечении эффективной и единой поддержки предотвращения, обнаружения и удаления вредоносного программного обеспечения. Это является неотъемлемым шагом в обеспечении надлежащего глубокого подхода к защите.

Идентификатор	Возможность	*Комментарии/потребности МО*
/MLDP.01/	Все несущественные порты сети FOOBAR 2.0 закрыты. Замечание 01 — Более подробную информацию см. в технической информации FOOBAR 2.0, в руководстве по защите для администратора (глава 17). См. /SGUD.02/. Замечание 02 — Данная функциональная возможность не может быть изменена местным ИТ администратором	*Принято к сведению МО*
/MLDP.02/	Операционная система, установленная на загрузочном устройстве FOOBAR 2.0, защищена от санкционированных / несанкционированных изменений. После перезагрузки система возвращается в свое изначальное состояние. Замечание — Данная функциональная возможность не может быть изменена местным ИТ администратором	*МО требуется получить заявление производителя о том, каким образом обнаруживаются вредоносные модификации времени исполнения*
/MLDP.03/	Все значимые файлы защищены с помощью надлежащей контрольной суммы (SHA1) и проверяются при загрузке. В случае обнаружения ошибки, система не запускается, а выдает сообщение об ошибке. Замечание — Данная функциональная возможность не может быть изменена местным ИТ администратором	*Принято к сведению МО*
/MLDP.04/	Защищенные/зашифрованные ДАННЫЕ о ЗДОРОВЬЕ доступны только после успешной загрузки. См. также /STCF.01/. Замечание — Данная функциональная возможность не может быть изменена местным ИТ администратором	*Принято к сведению МО*

PAUT. Аутентификация личности

Цель. Политика аутентификация должна быть гибкой для того, чтобы адаптироваться к местной ИТ политике МО. Требование аутентификации личности при предоставлении доступа к ДАННЫМ о ЗДОРОВЬЕ должно быть логически обоснованным в каждом конкретном случае.

Идентификатор	Возможность	*Комментарии/потребности МО*
/PAUT.01/	FOOBAR 2.0 поддерживает местное и глобальное управление учетными записями. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0, в руководстве по защите для администратора (глава 17)	*МО необходима точная спецификация для соединения с центральными структурами аутентификации (например, PKI, IEEE 802.1X).* *Примечание — Предоставьте методические документы как можно скорее*
/PAUT.02/	FOOBAR 2.0 поддерживает закрытие учетных записей. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0, в руководстве по защите для администратора (глава 17)	*Может ли это выполняться удаленно или же ИТ администратору необходимо находиться у прибора FOOBAR?*
/PAUT.03/	FOOBAR 2.0 поддерживает быстрое переключение пользователей. Поддержка данной функции уменьшает затраты времени на задачу входа и выхода пользователей из системы	*Принято к сведению МО*

PLOK. Физические замки на приборе

Цель. Гарантировать, что несанкционированный доступ не нарушит конфиденциальность, целостность и доступность ДАННЫХ о ЗДОРОВЬЕ, хранящихся на изделиях или съемных носителях.

Идентификатор	Возможность	*Комментарии/потребности МО*
/PLOK.01/	По причине выбранного метода шифрования FOOBAR 2.0 не требуется физическое запирание	*Принято к сведению МО*
		МО интересуется, защищена ли клавиатура или же неразрешенное устройство перехвата вводимой с клавиатуры информации (key-logger) может с легкостью быть установлено между клавиатурой и корпусом компьютера
		На корпусе компьютера установлен замок? Можно ли с легкостью извлечь или заменить дисковые накопители?

CSUP. Усовершенствование системы защиты изделия от кибератак

Цель. Создать унифицированный метод выполнения работы. Установка/усовершенствование пакетов исправлений для системы защиты выполняется персоналом на рабочем месте и, вероятно, санкционированным персоналом МО (в случае установки скачиваемых пакетов исправлений).

Идентификатор	Возможность	*Комментарии/потребности МО*
/CSUP.01/	Настоящим документом мы подтверждаем, что компания осуществляет внутренние процедуры для обследования рынка для определения текущих тенденций в области защиты от кибератак. В случае необходимости пакетов исправлений можно обращаться к технической поддержке. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0, в руководстве по защите для администратора (глава 17)	*МО требуется следующая информация.* *1 Должен существовать и быть раскрыт ПРОЦЕСС того, как значимые усовершенствования защиты и стабильности отделяются от незначимых.* *2 Должен существовать и быть раскрыт ПРОЦЕСС, определяющий то, какие критерии должны выполняться для того, чтобы действия защиты от кибератак заслуживали CAPA-сообщения.* *3 Должен существовать и быть раскрыт ПРОЦЕСС, связанный с задержкой между объявлением от производителя операционной системы и реакций производителя МЕДИЦИНСКОГО ПРИБОРА*

Окончание

Идентификатор	Возможность	*Комментарии/потребности МО*
		4. Должен существовать и быть раскрыт ПРОЦЕСС того, как МО оповещается об угрозах кибератак
/CSUP.02/	Прибор спроектирован так, что мы (производитель) не позволяем МО устанавливать какие либо несанкционированные патчи	*Принято к сведению МО, а также в СОГЛАШЕНИЕ об ОТВЕТСТВЕННОСТИ будет добавлено заявление о том, что производитель несет полную ответственность за ВРЕД, причиненный пациентам, в связи с отсутствием подтверждения пакетов исправлений, требующих срочной установки*

RDMP. Влияние компонентов третьей стороны на весь жизненный цикл изделия

Цель. Планы ПМП предполагают, что их изделия считаются поддерживаемыми на протяжении их жизненного цикла, в соответствии внутренним системам контроля качества и внешнему регламенту.

Идентификатор	Возможность	*Комментарии/потребности МО*
/RDMP.01/	Настоящим документом мы подтверждаем, что предоставляем сопровождение/поддержку системы на протяжении предположительного срока службы изделия. В случае необходимости сопровождения/ремонта/пакетов исправлений можно обращаться к технической поддержке. Замечание — Более подробную информацию см. в технической информации о FOOBAR 2.0 (глава 42)	*Должен существовать и быть раскрыт ПРОЦЕСС того как МО будет проинформирована о датах окончания срока службы критически важных компонентов. Нам необходимо знать, когда усовершенствование защиты перестает быть возможным*

SAHD. Усиление защиты системы и приложений

Цель. Минимизировать векторы атак и совокупную площадь атак посредством закрытия портов; удаления службы, и т. д.

Идентификатор	Возможность	*Комментарии/ потребности МО*
/SAHD.01/	Все ВОЗМОЖНОСТИ предназначенные обеспечить стабильную систему, предоставляющую только те службы, которые установлены ПРЕДНАЗНАЧЕННЫМ ИСПОЛЬЗОВАНИЕМ и требуются для его осуществления с минимумом сопроводительной деятельности, а также для того, чтобы позволить поставщикам медицинских услуг/МО организациям подключить FOOBAR 2.0 к их сети рассматриваются в главе MLDP: Обнаружение вредоносного программного обеспечения и защита от него в технической информации о FOOBAR 2.0 (глава 38)	*Принято к сведению МО*

AUTH. Авторизация

Цель. Следуя принципу минимизации данных, предоставить управление доступом к ДАННЫМ о ЗДОРОВЬЕ и функциям в только той степени, насколько это необходимо для выполнения задач МО в соответствии с ПРЕДНАЗНАЧЕННЫМ ИСПОЛЬЗОВАНИЕМ прибора.

Идентификатор	Возможность	*Комментарии/потребности МО*
/AUTH.01/	Несмотря на описанные ниже административные функции, только персонал санкционированный нами (производителем) имеет доступ к служебным функциям и функциональным возможностям. Кроме административных задач, разрешенных технической документацией, несанкционированному персоналу запрещается осуществлять дальнейший ремонт. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0	*Заявление будет принято в СОГЛАШЕНИИ об ОТВЕТСТВЕННОСТИ*

Окончание

Идентификатор	Возможность	*Комментарии/потребности МО*
/AUTH.02/	Так называемый вход в систему в качестве администратора предоставляется в случае FOOBAR 2.0 для: - для общего администрирования сервера; - установки обновлений/решения проблем; - добавления большого количества клиентов FOOBAR; - администрирования главных пользователей; - операций по резервному копированию	
/AUTH.03/	Так называемый вход в качестве Главного Пользователя (Master User) настраивается заранее и может быть добавлен для: - внесения поправок в/объединения отчетов/данных пациентов; - восстановления потерянных отчетов; - администрирования общих пользователей; - редактирования и поддержки общей конфигурации применения FOOBAR	

TXDF: Конфиденциальность передачи данных

Цель. ПРОИЗВОДИТЕЛЬ демонстрирует, что его оборудование соответствует множеству национальных стандартов и регламентов (например, USA HIPAA, национальным законам, основанным на EU 95/46/EC) в соответствии с потребностями МО для обеспечения конфиденциальности передаваемых ДАННЫХ о ЗДОРОВЬЕ.

Идентификатор	Возможность	*Комментарии/потребности МО*
/TXDF.01/	См. /STCF.06/. Соединение со специализированным удаленным архивом, находящимся в сети DICOM, может быть установлено с помощью VPN. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0 (глава 33)	*МО требуется заявление о совместимости с конкретным VPN для определения истинной интероперабельности с существующими в МО VPN*
/TXDF.02/	По требованию. Мы (производитель) предоставим сертификаты, демонстрирующие соответствие действующему национальному регламенту. Так как подобные сертификаты варьируются в зависимости от страны, пожалуйста, обратитесь к технической службе для получения большей информации	*МО принимает к сведению и примет решение о требующихся сертификатах соответствия перед приобретением изделия*

TXIG. Целостность передачи данных

Цель. Прибор должен обеспечивать защиту целостности передаваемых ДАННЫХ о ЗДОРОВЬЕ.

Идентификатор	Возможность	*Комментарии/ потребности МО*
/TXIG.01/	См. /STCF.06/. Соединение со специализированным удаленным архивом, находящимся в сети DICOM, может быть установлено с помощью VPN. Данная функциональная возможность гарантирует сохранение целостности ДАННЫХ о ЗДОРОВЬЕ на протяжении передачи данных и позволяет FOOBAR 2.0 передавать ДАННЫЕ о ЗДОРОВЬЕ через относительно открытые сети или окружение, в котором действует крепкая политика обеспечения целостности ДАННЫХ о ЗДОРОВЬЕ. Замечание — Более подробную информацию см. в технической информации FOOBAR 2.0 (глава 33)	*Принято к сведению МО*

Дополнительные потребности больницы Нью Тауна

На данный момент не установлено никаких дополнительных потребностей, но больница Нью Тауна сохраняет за собой право ввести дополнительные потребности в процессе развития нашего диалога об изделии.

Приложение В
(справочное)

Примеры региональных спецификаций нескольких ВОЗМОЖНОСТЕЙ ЗАЩИТЫ

Ниже приведено несколько примеров возможностей адаптированных для регионального использования в США. Данные примеры приведены только для иллюстрации и не претендуют на полноту или на законченный вариант руководства для использования на территории США.

PAUT. Аутентификация личности

Применение:	Профиль. Профиль IHE ATNA (Профиль журнала аудита и интеграции аутентификации узлов). Профиль IHE PWP (Персональный телефонный справочник). IHE EUA (Аутентификация корпоративных пользователей). IHE XUA (Контроль процесса авторизации пользователей). Политика. Проект политики защиты SANS. Местная ИТ политика МО.
Требование источника:	Стандарт HIPAA, Правило обеспечения защиты[1)], § 164.312.(a)(1): «..Управление доступом. Реализовать техническую политику и процедуры для электронных информационных систем, которые поддерживает электронную защищенную информацию о здоровье, для того, чтобы сделать возможным получение доступа только для тех личностей или программного обеспечения, которому были предоставлены права доступа в соответствии с § 164.308. (a)(4)...»
Справочный материал:	2(i) Уникальная идентификация пользователя (требуется). Необходимо назначить уникальное имя и/или номер для идентификации и отслеживания личности пользователя. NIST SP 800-53 v3. AC3. Осуществление доступа (Access Enforcement) — механизмы осуществления доступа служат организациям для управления доступом между пользователями и объектами.
Зависит от:	AUDT, NAUT
Цель требований:	Политики аутентификации должны быть гибкими для того, чтобы адаптироваться к местной ИТ политике МО. Требование аутентификации личности при предоставлении доступа к ЗАЩИЩЕННЫМ ДАННЫМ о ЗДОРОВЬЕ (PHI) должно быть логически обоснованным в каждом конкретном случае.
Потребность пользователя:	Пользователям может потребоваться наличие возможности для создания и использования уникальных учетных записей для пользователей и управления доступом, основанное на ролях (RBAC, локальный и удаленный) к прибору, подключенному к сети, для управления и контроля доступа к сети и ее деятельности. Возможность управлять учетными записями на медицинском оборудовании для обеспечения защиты доступа к ЗАЩИЩЕННЫМ ДАННЫМ о ЗДОРОВЬЕ. Пользователю может потребоваться связать персональные установки с учетными записями пользователей. Это может помочь приборам и системам, используемым множеством ОПЕРАТОРОВ, отделов или даже множеством организаций здравоохранения (МО). Требуется поддержка независимого и центрального администрирования. Однократная идентификация и использование одного пароля для всех рабочих мест. Поддержка идентификации узла согласно промышленным стандартам. Обнаружение и предотвращение фальсификации личности/сущности (необходимо предоставить невозможность отказа от авторства).

NAUT. Аутентификация узлов

Применение:	Профиль. Профиль IHE (Интеграция учреждений здравоохранения) ATNA. Профиль журнал аудита и интеграции аутентификации узлов [IHE ATNA profile (Audit Trail and Node Authentication Integration Profile]. IHE EUA (Аутентификация корпоративных пользователей). IHE XUA (Контроль процесса авторизации пользователей).

[1)] Министерство здравоохранения и социального обеспечения, секретариат, 45 CFR, части 160, 162, и 164 Реформа медицинского страхования. Стандарты защиты. Окончательный регламент, 20 февраля, 2003 (Department of Health and Human Services, Office of the Secretary, 45 CFR, Parts 160, 162, and 164 Health Insurance Reform; Security Standards; Final Rule, February 20, 2003).

Политика. NEMA/COCIR/JIRA Объединенный комитет по вопросам защиты и неприкосновенности частной жизни (Joint Security and Privacy).
Технический документ. Проект стандарта, рассматриваемого техническим комитетом: «Управление сертификатами аутентификации компьютеров, 10 февраля, 2005» (Committee draft White Paper: Management of Machine Authentication Certificates, 10 February 2005).
Проект политики защиты института SANS (институт системного администрирования, аудита, сети и защиты) (SANS Security Policy Project).
Местная ИТ политика МО.

Требование источника: Стандарт HIPAA. Правило обеспечения защиты, § 164.312 Технические средства защиты. (a)(1): «..Управление доступом. Реализовать техническую политику и процедуры для электронных информационных систем, которые поддерживают электронную защищенную информацию о здоровье, для того, чтобы сделать возможным получение доступа только для тех личностей или программного обеспечения, которому были предоставлены права доступа в соответствии с § 164.308. (a)(4)...»

Справочный материал: NIST SP 800-53 v3
AC3. Осуществление доступа (Access Enforcement) — механизмы осуществления доступа служат организациям для управления доступом между пользователями и объектами

Зависит от: AUDT, PAUT

Цель требований: Политики аутентификации должны быть гибкими для того, чтобы адаптироваться к местной ИТ политике МО. Требование аутентификации личности при предоставлении доступа к ЗАЩИЩЕННЫМ ДАННЫМ о ЗДОРОВЬЕ (PHI) должно быть логически обоснованным в каждом конкретном случае.

Потребность пользователя: Возможность управлять учетными записями на медицинском оборудовании для обеспечения защиты доступа к ЗАЩИЩШЕННЫМ ДАННЫМ о ЗДОРОВЬЕ (PHI).
Однократная идентификация и использование одного пароля для всех рабочих мест.
Поддержка идентификации узла согласно промышленным стандартам.
Обнаружение и предотвращение фальсификации личности/сущности (необходимо предоставить невозможность отказа от авторства).

ALOF. Автоматический выход из системы

Применение: Стандарт. Нет.
Политика. Местная ИТ политика МО.

Требование источника: Стандарт HIPAA. Правило обеспечения защиты, § 164.312 Технические средства защиты. (a)(1): «..Управление доступом. Реализовать техническую политику и процедуры для электронных информационных систем, которые поддерживают электронную защищенную информацию о здоровье, для того, чтобы сделать возможным получение доступа только для тех личностей или программного обеспечения, которому были предоставлены права доступа в соответствии с § 164.308. (a)(4)...»
(2)(iii) (iii) Автоматический выход из системы (доступно). Необходимо реализовать электронные процедуры, служащие для прекращения электронного сеанса по прошествии заранее заданного времени бездействия.
NIST 800-53, Издание 3 — Дополнительное руководство. Блокировка сеанса является временным действием, которая выполняется в том случае, если пользователь прекращает работу и не осуществляет непосредственные действия с информационной системой, но не желает выходить из системы (завершать сеанс) из-за того, что его отсутствие является временным.
AC-11 БЛОКИРОВКА СЕАНСА. Управление. Информационная система:
a. предотвращает дальнейший доступ к системе с помощью запуска блокировки сеанса после [Установление периода времени, заданного организацией.] бездействия или при получении запроса от пользователя; и
b. сохраняет блокировку сеанса до тех пор, пока пользователь не восстановит доступ, используя утвержденные процедуры идентификации и аутентификации.

Справочный материал: Нет.

Зависит от: AUDT

Цель требований:	Уменьшить РИСК получения несанкционированного доступа к ЗАЩИЩЕННЫМ ДАННЫМ о ЗДОРОВЬЕ (PHI) с рабочего места, оставленного без присмотра. Предотвратить неправильное использование, если система или рабочее место не используется в течении периода времени.
Потребность пользователя:	Несанкционированные пользователи не могут получить доступ к ЗАЩИЩЕННЫМ ДАННЫМ о ЗДОРОВЬЕ (PHI) с рабочего места, оставленного без присмотра. Сеансы авторизованных пользователей должны автоматически завершаться или блокироваться по прошествии заранее установленного промежутка времени. Это уменьшает РИСК несанкционированного доступа к ЗАЩИЩЕННЫМ ДАННЫМ о ЗДОРОВЬЕ (PHI), если авторизованный пользователь покидает рабочее место, не завершая сеанс и не закрывая экран или комнату. Автоматический выход из системы должен включать в себя очистку ЗАЩИЩЕННЫХ ДАННЫХ о ЗДОРОВЬЕ (PHI) со всех экранов по мере необходимости. Местный авторизованный ИТ администратор должен иметь возможность отключать эту функцию и устанавливать время истечения срока (учитывая хранителя экрана). Использование хранителя экрана с коротким временем бездействия или активирующегося «быстрой клавишей» может являться дополнительным свойством. Такая очистка экрана с ДАННЫМИ о ЗДОРОВЬЕ может быть вызвана, если на протяжении короткого времени не была нажата ни одна клавиша (например, от 15 секунд до нескольких минут). Это не завершит сеанс пользователя, но снизит РИСК случайного наблюдения информации. Желательно, чтобы пользователи медицинского учреждения могли избежать потери незавершенной работы по причине автоматического выхода из системы.

Приложение С
(справочное)

Отображение ВОЗМОЖНОСТЕЙ ЗАЩИТЫ в C-I-A-A

В таблице С.1 представлен шаблон, отображающий для гипотетической МО степень, с которой каждая из перечисленных ВОЗМОЖНОСТЕЙ ЗАЩИТЫ связана с каждой основной характеристикой защиты (конфиденциальность, целостность, готовность и отслеживаемость) и поддерживает их организационные политики. Данный шаблон дает возможность ИТ профессионалам понять вклад соответствующих ВОЗМОЖНОСТЕЙ ЗАЩИТЫ в реализацию защиты.

Цифра «2» означает, что Возможность существенно повышает характеристику защиты политики. Пустое поле указывает на относительный нейтралитет и -1 означает, что Возможность снижает характеристику защиты политики (например, наличие Автоматического выхода из системы в действительности снижает доступность).

Таблица С.1 — Шаблон отображения гипотетической МО

Возможности	Характеристики защиты			
	Конфиденциальность	Целостность	Готовность	Отслеживаемость
ALOF. Автоматический выход из системы	2	2	–1	
AUDT. Средства управления аудитом	1	1		1
AUTH. Авторизация	2	2	–1	1
CNFS. Конфигурация свойств системы защиты	1	1	1	1
CSUP. Усовершенствование системы защиты изделия от кибератак	1	1	1	
DTBK. Резервное копирование данных и экстренное восстановление		1	2	
EMRG. Экстренный доступ			2	–1
DIDT. Деидентификация ДАННЫХ о ЗДОРОВЬЕ	2			
IGAU. Целостность и аутентификация ДАННЫХ о ЗДОРОВЬЕ		2		2
STCF. Конфиденциальность хранения ДАННЫХ о ЗДОРОВЬЕ	2			
MLDP. Обнаружение вредоносного программного обеспечения и защита от него	1	1	1	
NAUT. Аутентификация узлов	1			1
PAUT. Аутентификация личности	1			2
PLOK. Физические замки на приборе	1	1	1	
SGUD. Руководства по защите	1	1	1	1
SAHD. Усиление защиты системы и приложений	1	1	1	
RDMP. Влияние компонентов третьей стороны на весь жизненный цикл изделия				
TXDF. Конфиденциальность передачи данных	2			
TXIG. Целостность передачи данных		2		

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 80001-1:2010	—	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта (документа). Перевод данного международного стандарта (документа) находится в Федеральном информационном фонде технических регламентов и стандартов.		

Библиография

[1]	IEC 60300-3-9:1995	Dependability management — Part 3-9: Application guide — Risk analysis of technological systems[2)]
[2]	IEC 60601-1-6:2006	Medical electrical equipment — Part 1-6: General requirements for basic safety and essential performance — Collateral standard: Usability
[3]	IEC 60601-1-8:2006	Medical electrical equipment — Part 1-8: General requirements for basic safety and essential performance — Collateral standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems
[4]	IEC 61907:2009	Communication network dependability engineering
[5]	IEC 62304:2006	Medical device software — Software life cycle processes
[6]	IEC 80001-2-1	Application of risk management for IT-networks incorporating medical devices — Part 2-1: Step by step risk management of medical IT-networks — Practical applications and examples IEC 80001-2-3, Application of risk management for IT-networks incorporating medical devices — Part 2-3: Guidance for wireless networks
[7]	ISO/IEC 15408	Information technology — Security techniques — Evaluation criteria for IT security — Parts 1, 2, and 3 [«Common Criteria»]
[8]	ISO/IEC 20000-1:2011	Information technology — Service management — Part 1: Service management system requirements ISO/IEC 20000-2:2012, Information technology — Service management — Part 2: Guidance on the application of service management systems
[9]	ISO/IEC 27001:2005	Information technology — Security techniques — Information security management systems — Requirements
[10]	ISO/IEC 27002:2005	Information technology. Security techniques. Code of practice for information security management ISO/IEC 27005:2011,Information technology — Security techniques — Information security risk management
[11]	ISO 13485:2003	Quality management systems — Requirements for regulatory purposes ISO/TS 13606-4:2009, Health informatics — Electronic health record communication — Part 4: Security
[12]	ISO 14971:2007	Medical devices — Application of risk management to medical devices
[13]	ISO/TS 25238:2007	Health informatics — Classification of safety risks from health software
[14]	ISO 27799:2008	Health informatics — Information security management in health using ISO/IEC 27002
[15]	ISO/TR 27809:2007	Health informatics — Measures for ensuring patient safety of health software
[16]	IEEE 610.12:1990	IEEE Standard Glossary of Software Engineering Terminology
ASIP requirements		FR l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) [ASIP Santé, the shared healthcare information systems agency http://esante.gouv.fr/en] creating conditions to comply with Law No. 2002-303 of 4 March 2002 on patients' rights and quality care system
DICOM		Digital Imaging and Communications in Medicine (DICOM) National Electrical Manufacturers Association. http://medical.nema.org/dicom/
Japan Law/Guidance		JP Act on the Protection of Personal Information (PFD) http://www.caa.go.jp/seikatsu/kojin/index_en.html and Guideline for Medical Information System Safety Management http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html (Japanese only), Ministry of Health, Labour and Welfare, Japan
NEMA/COCIR/JIRA		Joint Security and Privacy Committee. See tutorials and white papers at http://www.medicalimaging.org/policy-and-positions/jointsecurity-and-privacy-committee-2/

[2)] Заменен на МЭК/ИСО 310101:2009, Менеджмент риска. Методики оценки риска.

NEN 7510	NL Nederlands Normalisatie-instituut Standard Medische informatica — Informatiebeveiliging in de zorg — Algemeen [Health Informatics — Information Security in the Healthcare Sector — General] http://www.nen.nl/web/Normshop/Norm/NEN-75102004-nl.htm
NIST 800 series	US National Institute of Standards and Technology Special Publications series on Computer Security http://csrc.nist.gov/publications/PubsSPs.html

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, информационная безопасность, менеджмент рисков, информационно-вычислительные сети, медицинские приборы

Редактор *А.Ф. Колчин*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.Е. Кругова*

Сдано в набор 23.05.2016. Подписано в печать 31.05.2016. Формат 60 ×84 1/8. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 5,20. Тираж 29 экз. Зак. 1355.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru