ВОПРОСЫ БЕЗОПАСНОСТИ И «ПРИВАТНОСТИ» В ИНТЕГРИРОВАННЫХ МЕДИЦИНСКИХ СИСТЕМАХ

А.Р. Дабагов

ЗАО «Медицинские технологии ЛТД»

Статья получена 23 июня 2014 г.

Аннотация. В работе обзорного характера рассматриваются некоторые вопросы безопасности и приватности, с уклоном в сторону обеспечения функционирования медицинских систем. В Приложении приводятся выдержки из документа Fips 200 (минимальные требования к безопасности). В заключении формулируются некоторые выводы.

Ключевые слова: безопасность, медицинская информатика.

Abstract. In the work, in a review manner some problems of security and privacy are discussed, partially they are of health systems functioning. In the Application, excerpts from Fips 200 (minimum security requirements) are supplied. In the conclusion, main findings of the article are outlined.

Keywords: security, medical Informatics.

Введение

В [1,2] мы рассматривали некоторые вопросы безопасности, а также постановку задачи информационной безопасности, как она обычно понимается в информационных системах. Мы подчеркивали, что безопасность информации является задачей комплексной, т.е. состоит из ряда пересекающихся подмножеств, или аспектов:

организационного,
политико-правового,
экономического,
промышленного,
криминологического,
информационного.

Теперь нам также необходимо учитывать и требование «приватности» (privacy) информации, т.е. к защиты информации частных лиц, к которым должен иметь доступ только ограниченный круг субъектов, которым она необходима. Мы рассмотрим этот вопрос в дальнейшем.

Некоторые определения

Информационная безопасность

- Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз, и
- состояние информации, информационных ресурсов и информационных систем, при котором в рамках некоторых непротиворечивых правил обеспечивается защита информации в планах ее целостности, конфиденциальности и доступности.

Защита информации

- Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
- Комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации.
- Под гарантированно защищенной системой будем понимать систему, *доказательно удовлетворяющую критериям принятой в организации политики безопасности.*[1]

Требования и оценки. Оценка защищенности организации-пользователя может быть сделана, учитывая все требования, разработанные для организации-пользователя и исходя из стандартизованных методик на базе стандарта

[1] Вообще говоря, следует разработать 3 документа: Концепцию (1), Политику (2) и Программу безопасности (3).

ИСО/МЭК 15408 "Общие критерии оценки безопасности информационных технологий" и имеющихся стандартизованных профилей защиты. Как известно, профили защиты - одно из основных понятий этого стандарта. В тексте оно определяется следующим образом: "профиль защиты…независимая от реализации совокупность требований безопасности для некоторой категории продуктов или ИТ-систем, отвечающая специфическим запросам потребителя". То-есть, другими словами, под профилями защиты понимаются конкретные наборы требований и критериев для тех или иных продуктов и систем ИТ, выполнение которых необходимо, однако, проверять (требования доверия) [3]

Угрозы и специфика. В [1,2],был описан примерный перечень нарушений безопасности (по типам нарушений) и примерный же интегральный ущерб от нарушений ИБ.

В последнее время характер нарушений ИБ меняется; так, мы не можем уже сказать, соблюдается ли в отношении «утечек» известный принцип Парето 20/80 (20% по техническим каналам, 80% все остальное). Меньше наблюдается вредоносных программ и кодов, написанных и внедряемых из чистого хулиганства (поскольку это не приносит прибыль), зато значительно более появляется вредоносных кодов, написанных исключительно для получения тем или иным образом незаконной прибыли либо нанесения ущерба потенциальным конкурентам, оказания на них «давления», либо по известным «внутреним» причинам. Не следует сбрасывать со счетов и описанные в [4] «каналы информации», к которым сейчас безусловно относится вся ИТ-инфраструктура.

В документе НИСТ 800-37 [5] отмечается, что *«Кибер-атаки на информационные системы сегодня становятся агрессивными, достаточно хорошо взаимоувязанными, организованными и финансируемыми. Во все большем числе задокументированных случаев, атаки являются очень сложными (sophisticated) Успешные атаки в государственном и частном секторе ИТ-систем могут приводить к серьезным или даже фатальным последствиям <…>. Учитывая все возрастающую опасность этих угроз,*

крайне необходимо, чтобы руководители всех уровней понимали свою ответственность за достижение достаточного уровня информационной безопасности и надлежащем администрировании информационных процессов относительно рисков, связанных с проблемами безопасности».

При переходе на более современные технологии, добавлении новых компонент и связанных с этим изменениях в архитектурах систем, могут возникать новые угрозы, которые в процессе жизненного цикла должны быть учтены.

В дополнение к общим угрозам безопасности [3], как уже отмечалось выше, типовые медицинские организации имеют ряд особенностей функционирования, отличающих их от прочих.

1. Несмотря на имеющиеся методики – см. напр. [6], может оказаться трудным оценить ценность информации и определить ее значимость в процессе деятельности и соответственные значения для матрицы рисков. Также трудно определить сам факт утечки через НСД к рабочей или иной информации. Поэтому остается на основании опыта других организаций a priori считать этот канал значительным и соответствующим образом строить политику безопасности.
2. Трудности проведения программной и аппаратной унификации. Иногда имеется программное обеспечение (модули) собственной разработки, функционирующее в определенной программно-аппаратной среде. Последнее затрудняет мониторинг и модернизацию, снижает уровни доверия. Имеющие место неисправности или иные события безопасности могут отражаться сразу на большом числе пользователей.
3. Трудности централизованного администрирования. Пользователи могут устанавливать специализированное программно-аппаратное обеспечение Это затрудняет мониторинг и обслуживание систем, кроме того, пользователи, как правило, имеют весьма поверхностное представление о безопасности.
4. ИБ на отдельно взятом предприятии повышается, если: а) используется

высококвалифицированный (но и с соответствующей оплатой) ИТ-персонал, либо персонал предприятия проходит соответствующую подготовку и тестирование в организациях по безопасности, а также проводится тестирование и сертификация оборудования с привлечением компетентных специалистов / организаций. Очевидно, сумма мер безопасности будет обходиться тем дороже, чем больше ИТ-оборудования находится на предприятии, чем шире должна быть его функциональность и жестче требования к надежности и безопасности. И наоборот, обеспечение требуемой ИБ будет значительно проще и дешевле, если основные функции работы с данными будут переданы специализированным ИТ-центрам, имеющим необходимый персонал и аппаратуру и организованным, например, на базе облачных либо «конвергентных» структур с предоставлением услуг «по требованию».

5. Необходимость защиты частных данных клиентов – приватность и необходимость сохранения врачебной тайны. Это требование выдвигается одним из первых для разработчиков медицинских систем. Более того – некоторые критические данные о состоянии здоровья пациента могут быть «закрытыми» от него самого и сообщаться только по решению родственников и/или лечащего врача. При этом доступ к данным должен быть легко открываем для медперсонала, например, в случае экстренной госпитализации либо из других клиник, с целью проведения удаленных консультаций, подготовки к госпитализации и др., а также в некоторых случаях и с мобильных систем – как например – «Скорой помощи». Вместе с тем данные должны быть открыты для статистической обработки и анализа, с целью повышения квалификации медперсонала и в некоторых иных случаях. При этом личная информация о пациенте должна быть надежно защищена.
6. Необходимость защиты связанной с пациентом служебной, в частности финансовой, информации.
7. При формировании согласованных наборов стандартов – профилей –

бизнес- и некоторые иные требования медицинских предприятий, равно как и отдельных лиц, поставщиками сервисов могут быть учтены только в общих чертах, а в информационном плане – с целью возможно болеее полной совместимости оборудования и удовлетворения общим требованиям безопасности.

Отделения могут иметь и свои локальные сети, объединяющие названные информационные и вычислительные ресурсы и имеющие выход в Интернет или другие локальные сети. Через эти каналы может быть налажено взаимодействие с другими центрами коллективного пользования, а также центрами хранения и резервирования данных.

Выход здесь видится в переходе на современные технологии, централизацию основного функционала ИТ, таким образом, максимальную централизацию и унификацию функций управления и контроля безопасности.

Определение. Политика безопасности - это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение информации в данной организации. Политика безопасности должна отражать уязвимость конкретной организации к различным типам инцидентов с безопасностью и делать приоритетными инвестиции в области наибольшей уязвимости. Политика безопасности должна быть одним из основных документов в этой сфере. этот документ должен основываться на Концепции безопасности, которая должна быть обсуждена и согласована со со всеми заинтересованными сторонами.

Основные правила Политики (по [7])

ТОЛЬКО АВТОРИЗОВАННЫЕ ПОЛЬЗОВАТЕЛИ

Только те пользователи, которые уполномочены на доступ к информации в системе, могут иметь доступ к системе.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Пользователи должны быть идентифицированы в системе и пройти процедуру аутентификации

ТОЛЬКО ТЕ, КОМУ НЕОБХОДИМО ЗНАТЬ

Система должна ограничивать доступ к ресурсам в соответствии со служебными обязанностями пользователей.

ПОДОТЧЕТНОСТЬ (неотказуемость, non-repudiation)

Пользователи несут ответственность за свои действия в системе. Все критические действия уполномоченных пользователей автоматически должны быть запротоколированы.

ЗАЩИТА ОТКРЫТОЙ ИНФРАСТРУКТУРЫ

Все объекты открытой инфраструктуры должны быть выделены, классифицированы и защищены исходя из требований деловой (бизнес) системы.

ЗАЩИТА ПРИ ПОВТОРНОМ ИСПОЛЬЗОВАНИИ ОБЪЕКТОВ (там, где необходимо)

Защита памяти и системных кэшей от возможного неавторизованного считывания.

ТЕСТИРОВАНИЕ

Система имеет средства проверки конфигурации и функций безопасности.

МИНИМАЛЬНАЯ ДОСТАТОЧНОСТЬ

Только те сервисы, процессы и потоки, которые действительно необходимы для функционирования системы и обслуживания пользователей, могут существовать в системе.

АУДИТ И СИГНАЛЫ ТРЕВОГИ

Система имеет в своем составе обеспечение, позволяющее регистрировать и хранить сообщения о событиях имеющих отношение к безопасности. Система должна оперативно реагировать на некоторые критические события, список которых определяется администратором безопасности (активный аудит). В случае возникновения критических ситуаций система вырабатывает по особым правилам сигналы тревоги либо автоматически блокирует источник угрозы. Все записи аудита должны быть защищены.

ФУНКЦИОНАЛЬНОСТЬ ПУТИ ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ

Предотвращение перехвата имен и паролей пользователей троянскими и

иными программами.

УПРАВЛЕНИЕ ДОВЕРИТЕЛЬНЫМИ ОТНОШЕНИЯМИ

Поддержка набора ролей (разных типов учетных записей) для разных уровней работы в системе.

НОТАРИЗАЦИЯ

Проверка сертификатов должна осуществляться доверенной третьей стороной

ПРИВАТНОСТЬ

Должна обеспечиваться конфиденциальность личных данных и материалов пациентов и персонала.

Политикой безопасности организации предусматривается ведение реестра информационных ценностей. Администраторы безопасности вкупе с администрацией предприятия должны вести постоянный список систем , сетей, компьютеров и баз данных, использующихся в организации. Организации должны объединить этот список с результатами работ по классификации (категоризации) данных.

Как отмечалось выше, типовые медицинские организации имеют свои особенности функционирования. Необходимо гарантировать защиту всех информационных ценностей, и то, что текущая ИВС (информационно-вычислительная сеть) организации может быть быстро восстановлена после инцидента с безопасностью. Каждый сетевой администратор и/или персонал автоматизированных рабочих мест должен вести учет информационных систем в его зоне ответственности. Список должен включать в себя все существующую аппаратную часть ИВС, программы, электронные документы, базы данных и каналы связи.

Для каждой информационной ценности должна быть описана следующая информация:

тип: оборудование, программа, данные,

используется в системе общего назначения или критическом приложении,

ответственный за данную информационную ценность,

ее физическое или логическое местоположение,

учетный номер, если возможно.

Для того чтобы разработать эффективную политику безопасности, информация, хранимая или обрабатываемая в организации, должна быть *классифицирована* в соответствии с ее критичностью к потере конфиденциальности. На основе этой классификации потом можно легко разработать политику для разрешения (или запрещения) доступа к Интернету или для передачи информации по Интернету.

Большинство организаций используют такие классы, как "Коммерческая тайна" и "Для служебного пользования" . Классы, используемые в политике информационной безопасности, должны быть согласованы с другими существующими классами.

Для всех возможных угроз безопасности ИВС организации должна строиться и периодически актуализоваться матрица профиля риска [7]. На ее основе определяются наиболее уязвимые места и вырабатываются меры по минимизации рисков на основе разумной достаточности. При этом обеспечению непрерывности функционирования ИВС организации придается первостепенное значение.

Сервисы, предоставляемые ИВС типовой организации, и ее структура должны быть оптимизированы с целью достижения приемлемой стойкости защиты при минимуме затрат. На основе этой оптимизации строится матрица использования средств безопасности для защиты сервисов [7], которая должна быть идентичной матрице ИС/ИТ [8] Профиля безопасности типовой организации, разрабатываемого по методике [8].

Для предотвращения неавторизованной модификации конфигурации систем (особенно относящихся к группам повышенного риска) должна иметься некоторая форма гарантий целостности. Обычно для рабочей конфигурации системы вычисляются контрольные суммы или криптографические хэш-функции, которые хранятся потом на защищенном носителе. Каждый раз, когда

конфигурация модифицируется, необходимо обновить контрольные суммы файлов и сохранить их надежным образом.

Документация. На все системы, их архитектуру, элементы и программное обеспечение должна иметься документация, которая хранится у уполномоченных лиц.

Должны быть разработаны документы, предусматривающие последовательность действий при различных событиях безопасности. Все такие события должны протоколироваться, при этом должна быть предусмотрена сохранность записей аудита. Администраторы безопасности обязаны вести журналы учета событий безопасности и проводить соответствующие расследования.

При необходимости могут разрабатываться политики безопасности для отдельных информационных сервисов.

Должна быть определена периодичность пересмотра Политики безопасности с внесением в нее изменений в случае необходимости.

Технологии защиты информационных систем начали развиваться относительно недавно, но сегодня уже существует значительное число теоретических моделей, позволяющих описывать практически все аспекты безопасности и обеспечивать средства защиты формально подтверждённой алгоритмической базой. Из теории систем, однако, известно, что при объединении компонент, изменении архитектур, методов обработки информации и других изменениях происходит усложнение систем, свойства которых, вообще говоря, не могут являться простой суммой свойств их компонент, кроме того, сложность описания (модели) такой системы должна примерно соответствовать сложности самой системы. Поэтому от «доказательных» оценок легче бывает перейти к другим методикам, основанным, например, на оценках рисков. При этом ситуация может быть облегчена надлежащим выбором модели безопасности. Как уже отмечалось, теоретические исследования в области защиты информационных систем зачастую носят разрозненный характер и не составляют комплексной теории

безопасности [9]

Среди моделей политик безопасности можно выделить три класса: дискреционные (произвольные), мандатные (нормативные), и смешанные политики, представляющие собой некоторые комбинации первых двух. Упомянем кратко только некоторые из них.

Модель LWM (Low WaterMark)

Является конкретизацией модели Б-Л и рассматривает варианты, когда изменения для уровня секретности в решетке MLS возможны; поток информации разрешен только в одну сторону (подробнеее [10].

Ролевая модель

RBAC-модель была официально представлена в 1992 году Ferraiolo и Kuhn. В настоящее время это достаточно широко используемая модель безопасности для управления доступом к ОС, программно-аппаратному обеспечению и другим ресурсам системы. Ролевую политику безопасности нельзя отнести ни к дискреционным, ни к мандатным, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов [11]. Поэтому ролевая модель представляет собой совершенно особый тип политики, основанной на компромиссе между гибкостью управления доступом, характерной для дискреционных моделей, и жесткостью правил контроля доступа, присущей мандатным моделям.

Некоторая аппаратура (например часть сетевых коммутаторов Nexus) также поддерживает RBAC. В модели RBAC доступ предоставляется на основе записей о роли отдельных пользователей в организации. Существенным преимуществом модели является то, что администратор может добавлять, изменять или удалять пользователей, выполнять некоторые другие привилегированные команды не входя в аккаунт системного администратора либо суперпользователя, что упрощает администрирование больших систем и снижает риски. В то же время одним из недостатков является то, что эта модель (RBAC) разрабатывалась независимо для различных ОС и некоторых СУБД.

Последнее обстоятельство затрудняет администрирование комплексов, использующих несколько различных ОС, а также СУБД. В качестве решения к настоящему времени разработаны специальные унифицирующие права доступа программы, что дает возможность централизованного управления пользователями и уменьшает вероятность ошибок при администрировании прав доступа, которые могут возникнуть в средах, в которых доступны несколько систем. Также RBAC, через настройку либо использование инструментария сторонних производителей, организации могут снизить требования для рутинных задач, разгружая тем самым системных администраторов высшего звена. Преимущества и недостатки RBAC, вместе с возможностями использования расширений RBAC рассмотрены в [3] и многих других работах (напр. [11, 12]. Несмотря на ряд очевидных преимуществ, использование ролевой модели в больших системах может иметь нетривиальные особенности и должно быть тщательно продуманным решением в контексте применяемой политики и заданий безопасности. [8, 12]

Как указано в [3], ролевое управление доступом (Role-Based Access Control, RBAC) представляет собой универсальный каркас, нейтральный по отношению к конкретной дисциплине разграничения доступа и предназначенный в первую очередь для упрощения администрирования информационных систем с большим числом пользователей и различных ресурсов.

Логический контроль доступа на основе атрибутов (NIST Special Publication 800-162) .[14]

Attribute Based Access Control (ABAC) [14]: логический контроль доступа где разрешение на доступ выполнять набор к-л операций определяется с помощью оценки атрибутов, связанных с субъектом, объектом, запрошенной операцией, и, в ряде случаев, переменными из окружающей среды (время, IP-адрес и др.) в контексте политики, правил или отношения, которые описывают допустимые операции для данного набора атрибутов.

Атрибуты являются характеристиками, которые определяют специфические аспекты субъекта, объекта, условий окружения и/или запрошенных действий,

преопределенных и предварительно назначенных авторизованным лицом. Атрибуты состоят из опциональной категории, определяющей класс информации, задаваемый атрибутом, Имя, и значение (напр., Class=HospitalRecordsAccess, Имя=PatientInformationAccess, Значение=MFBusinessHoursOnly).

Субъект является активной сущностью (как правило, пользователь, процесс, или устройство), которое вызывает потоки информации между объектами или изменения состояния системы. Он может быть пользователем, запросом, или механизмом (процессом), действующим от имени пользователя или запроса. «Субъект» может быть неперсональной сущностью, такой как система или процесс, запущенный от имени конкретного человека или организации. Субъектам могут быть присвоены атрибуты, определяющие имя, организационную принадлежность, гражданство и др.

Объект-это пассивная относящаяся к операционной системе сущность (напр., устройство, файл, запись, таблица, процесс, программа, сеть, домен), содержащее или принимающее информацию. Доступ к объекту подразумевает доступ к содержащейся в нем информации. Это может быть ресурс запрашиваемого лица, а также что-либо, на чем работа может быть выполнена со стороны субъекта, в том числе данные, приложения, службы, устройства и сети. Объекты обычно требуют какую-либо форму ограничения доступа для неавторизованных пользователей. Операция есть выполнение какой-либо функции над объектом (чтение, запись, изменение, удаление, выполнение, административный доступ). Политика – представление правил либо отношений, определяющих подмножество разрешенных для субъекта операций. Определение ABAC наглядно представлено на рис. 1, где ABAC ACM (ACM – механизм контроля доступа) сначала принимает запрос субъекта (пользователя), затем проверяет атрибуты субъекта и объекта согласно политике (ACM), наконец определяет, какие операции субъект может выполнить над объектом. В последнем случае возникают также вопросы, что должна делать система, если условия (например, окружения) изменились,

например, в процессе проведения действий над объектом. Также возникают вопросы, связанные с возможной операцией восстановления (возможно, частичной) системы – как будет организовано восстановление прав (матриц) доступа и может ли это повлиять на соблюдение правил политики безопасности. Последний вопрос актуален и в случае применения других моделей защиты, как например, RBAC.

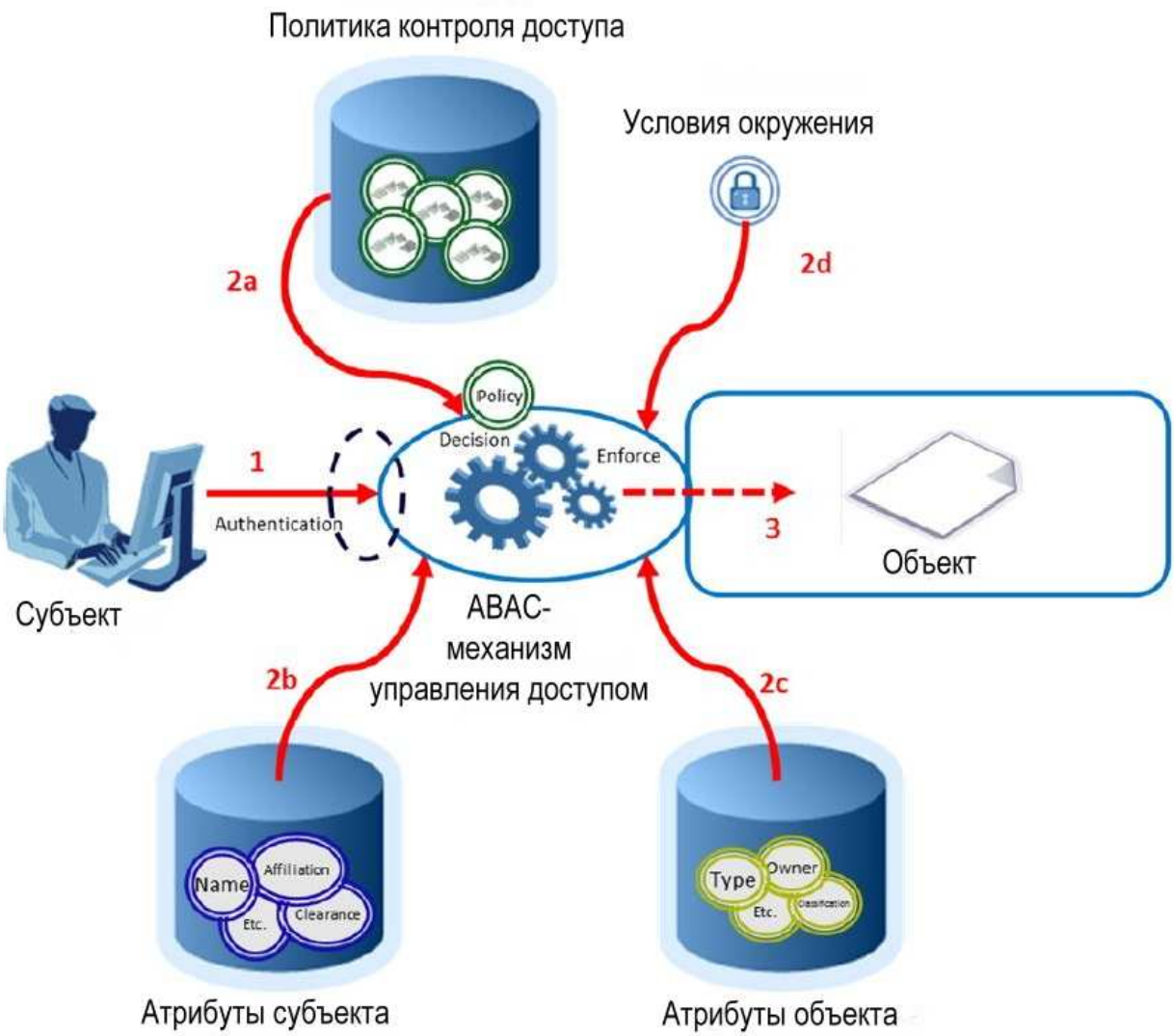

Рис. 5.5. Базовый сценарий контроля доступа в ABAC. 1.Субъект запрашивает доступ к объекту. 2.Механизм контроля доступа проверяет: а-правила; б-атрибуты субъекта; в- атрибуты объекта; г- условия окружения для определения авторизации (права) объекта на запрашиваемые действия (по [14]).

ABAC – системы также могут быть использованы для усиления дискреционной и мандатной политик управления и контроля доступа. Более

того, ABAC системы делают воможным реализацию риск-адаптированной модели контроля доступа, Risk-Adaptable Access Control (RadAC) , когда величины рисков имеют в системе переменные значения. (подробнее см в [14)] и там же список литературы). Подобная модель также способна отслеживать текущую ситуацию и принимать решение о правах доступа к объектам на основе всей имеющейся информации с учетом применяемой Политики безопасности.

Система управления рисками является неотъемлемым компонентом системы обеспечения информационной безопасности. В общем случае эта система предназначена минимизировать возможные негативные последствия применения информационных технологий и обеспечить возможность выполнения предприятием его бизнес-функций, то есть, говоря другими словами, непрерывность функционирования. Согласно стандарту NIST 800-30 система управления рисками должна быть интегрирована в систему управления жизненным циклом ИТ. На основе оценки рисков могут быть опроделены **категории** подлежащей защите информации (см. также Приложение).

Категоризация на основе порядковой шкалы ценностей

с введением решетки ценностей относительно бинарного отношения ≤ [6]. Этот подход лежит в основе государственных стандартов защиты информации, (так называемая решетка MLS - Multilevel Security). Решетка строится как прямое произведение линейной решетки L и решетки SC подмножеств множества X:

$$(\alpha,\beta)\leq(\alpha',\beta')\Leftrightarrow\alpha\subseteq\alpha',\beta\leq\beta'$$

где (α,β) элементы произведения, $\beta\in L$ - линейная решетка, $\alpha\in SC$ - решетка подмножеств некоторого множества X, а верхняя и нижняя границы определяются следующим образом:

$$(\alpha,\beta)\oplus(\alpha',\beta')\Leftrightarrow(\alpha\cup\alpha',\max\beta\leq\beta'$$

$$(\alpha,\beta)\otimes(\alpha',\beta')\Leftrightarrow(\alpha\cap\alpha',\min\beta\leq\beta'$$

Вся информация (объекты системы) отображается в точки решетки $\{(\alpha,\beta)\}$. Линейный порядок указывает гриф секретности. Точки множества X обычно называются категориями [(6)].

В реальной же ситуации, скорее всего, для крупных организаций, связанных с современными разработками по заданиям директивных органов[2], стратегия защиты информации будет формулироваться на основе обоих этих подходов и физического разделения "открытой" и "закрытой"[3] частей. При этом для первой из них будет делаться приоритет на непрерывности производственного цикла, а для второй - на выполнении некоторой, возможно "тривиальной", политики безопасности. В противном случае затраты на проектирование и эксплуатацию такой "открытой" системы могут оказаться неоправданно высоки.

Заключение

На основе анализа как российских, так и зарубежных источников рассмотрено понятие информационной безопасности, основные принципы и подходы к обеспечению безопасности исходя из формулируемых потребностей. Рассмотрены некоторые модели защиты информации и особенности защиты информации в некотором «виртуальном» медицинском учреждении. Показано, что в силу специфики подавляющего большинства медицинских учреждений процессы работы с медицинской информацией выгоднее разделить, используя в ЛПУ относительно небольшой информационно-вычислительный функционал, где необходимые требования к безопасности можно выполнить на основе относительно простых процедур и правил, не требующих от медицинского персонала существенных знаний в области инфотелекоммуникационных технологий, в то время как основные процессы обработки, анализа хранения и резервирования информации будут выполняться квалифицированным ИТ-персоналом в специализированных центрах обработки данных. Таким образом, существенно легче будет обеспечить все аспекты безопасности, как они

[2] Вполне вероятно,также и для перспективныхмедицинских информационных систем.

[3] Закрытость здесь подразумевается прежде всего в смысле ограничения периметра, а не от отказа следовать общей методике построения открытой системы.

понимаются в современных стандартах, руководящих и иных документах. Последнее также облегчит унификацию политик безопасности, их адаптацию под конкретное медицинское предприятие.

Совершенно очевидно, что проблемы безопасности и приватности в любых информационных системах (и в медицинских, в частности), имеют первоочередное значение и подходы к безопасности должны тщательно продумываться уже на начальных этапах проектирования таких систем. Должны быть сформулированы все основополагающие документы, оценены возможные уязвимости, угрозы, сформулированы матрицы рисков, модели защиты (возможно гибридные). К сожалению, ситуация в области обеспечения безопасности на данный момент усугубляется тем, что к настоящему времени начали широко внедряться принципиально новые архитектуры систем, программных и аппаратных компонентов, быстро прогрессирует развитие различных средств виртуализации и др.

Все это приводит к тому, что спектр специфических проблем безопасности меняется, и к построению систем безопасности необходимо подходить с особым вниманием, стремясь по возможности учесть все проблемы, которые могут возникнуть при расширении и/или модернизации комплексов ИВТ в будущем.

Опыт показывает, что в таких случаях бывает трудно обойтись одной собственной командой разработчиков. Вопросы безопасности слишком важны, поэтому здесь, возможно, потребуются консультации третьей стороны и выбор подходящих решений, уже успевших пройти апробации и имеющих потенциал дальнейшего развития.[4]

Также известно, что ряд разработчиков в области «облачных» технологий уже предлагают свои системы, имеющие необходимые механизмы защиты,

[4] Большинство специалистов по безопасности считает также, что как в документации, так и в программном обеспечении ИБ должны иметься некоторые «черные ящики», что может существенно усилить защиту и безопасность систем. Также известно, что применение исключительно «пассивных» мер в принципе не может обеспечить высоких уровней (комплексной) защиты.

заявленные характеристики которых обладают всеми необходимыми функциями. «Референсная» архитектура безопасности облачных систем представлена одним из последних стандартов NIST Cloud Computing Security Reference Architecture, **NIST Special Publ. 500-299** [15].

Первоначально мы полагали, что защита собственно медицинской информации представляет собой относительно простую задачу; так как хранящиеся в базах «анонимные» данные не представляют для кого-либо большого интереса и их категориальность может быть минимальной. Что конкретно в защите нуждается информация, когда она сопоставлена какому-либо конкретному лицу. Однако некоторые публикации (приводим только одну – [16], стр. 35) несколько изменили нашу точку зрения.

ПРИЛОЖЕНИЕ. МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ (На основе документа FIPS 200)

FIPS Публикации 200 Минимальные Требования к Безопасности федеральной Информации и Информационных Систем [17]

Минимальные требования к безопасности охватывают семнадцать аспектов (требований), связанных с безопасностью в отношении защиты конфиденциальности, целостности и доступности федеральных информационных систем и информации, обрабатываемой, хранимой и передаваемой с помощью этих систем. Безопасность в смежных областях включает: (i) контроль доступа; (ii) обучение и повышение осведомленности; (iii) аудит и отчетность; (iv) аттестация, аккредитация и оценка безопасности; (v) управление конфигурацией; (vi) планирование непредвиденных обстоятельств; (vii) идентификация и аутентификация; (viii) реагирования на происшествия; (ix) техническое обслуживание; (x) защита носителей информации; (xi) физическая защита и защита окружения (environment); (xii) планирование; (xiii) кадровая безопасность; (xiv) оценка рисков; (xv) отслеживание приобретения систем, программных продуктов и услуг (сервисов); (xvi) защита систем и коммуникаций; (xvii) системная и

информационная целостность. Эти семнадцать требований представляют собой основанную на широкой базе и сбалансированную программу обеспечения информационной безопасности, адресуемое к менеджмент-, эксплуатационным и техническим аспектам защиты Федеральной информации и информационных систем.

Политики и процедуры играют важную роль в эффективной реализации корпоративной программы по информационной безопасности в рамках Федерального правительства, обеспечивая успешность мер безопасности, применяемых для защиты федеральной информации и информационных систем. Таким образом, организации должны разработать и обнародовать официальные, документально оформленные политики и процедуры, регулирующие минимальные требования по безопасности, изложенные в настоящем стандарте, и должны обеспечить их эффективное применение.

Технические характеристики Минимальных Требований Безопасности

Контроль доступа: Организации должны предоставлять доступ в систему только зарегистрированным пользователям, процессам, действующим от имени авторизованных пользователей или устройств (в том числе и в другие информационные системы), ограничивая их списком операций и функций, которые авторизованным пользователям разрешено выполнять.

Обучение и повышение осведомленности: Организации должны: (i) убедиться, что менеджеры и пользователи информационных систем в организации должны осознавать риски, связанные с их деятельностью, а также применимыми законами, указами, распоряжениями, правилами, стандартами, инструкциями, правилами или процедурами, относящимися к безопасности организационного информационных систем; и (ii) убедиться, что персонал организации имеет надлежащую подготовку для выполнения возложенных на него и связанных с информационной безопасностью обязанностей с надлежащей ответственностью.

Аудит и отчетность: Организации должны: (i) создавать, защищать и сохранять записи аудита информационной системы настолько, насколько они

необходимы для осуществления мониторинга, анализа, исследования, и отчетности о незаконных, несанкционированных или недопустимых действиях в информационной системе; и (ii) гарантировать, что действия отдельных пользователей системы могут быть однозначно отслежены так, что они могут быть привлечены к ответственности за свои действия.

Сертификация, Аккредитация и Оценка Безопасности: Организации обязаны: (i) проводить периодическую оценку систем контроля безопасности в информационных системах организации для определения их эффективности; (ii) разрабатывать и осуществлять планы действий с целью устранения недостатков, а также уменьшения или устранения уязвимостей в информационных системах организации; (iii) авторизовать подключение информационных систем организации к любой другой информационной системе; и (iv) обеспечить мониторинг систем безопасности и контроля на постоянной основе для уверенности в их надлежащем функционировании.

Управление конфигурацией: Организации должны: (i) устанавливать и поддерживать базовые конфигурации и ресурсы для информационных систем (включая аппаратные средства, программное обеспечение и документацию) в течение всего жизненного цикла системы; и (ii) установить и (по возможности) усилить конфигурационные установки безопасности для продуктов информационных технологий, применяемых в информационных системах организации.

Планирование непредвиденных обстоятельств: Организации должны устанавливать, сохранять и эффективно реализовывать планы аварийного реагирования, операций резервного копирования и восстановления после стихийных бедствий в информационных системах организаций для обеспечения доступности критически важных информационных ресурсов и непрерывности операций в чрезвычайных ситуациях.

Идентификация и Аутентификация: Организации должны идентифицировать пользователей информационной системы, процессы или устройства, действующие от имени пользователей, и аутентифицировать (или

верифицировать[5]) идентичность тех пользователей, процессов или устройств, как необходимое условие для обеспечения доступа к информационным системам организации.

Реагирование на компьютерные инциденты: Организации должны: (i) обеспечить возможности по оперативной обработке инцидентов в информационных системах организации, что включает в себя надлежащую подготовку, обнаружене, анализ, сохранение, восстановление (исходного состояния) и ответные действия действия пользователя; и (ii) отслеживать, документировать и сообщать об инцидентах для принятия соответствующих мер должностным лицам и/или официальным органам.

Техническое обслуживание: Организации должны: (a) выполнять периодическое и своевременное обслуживание информационных систем организации; и (ii) обеспечить эффективный контроль за средствами, методами, механизмами и персоналом, используемыми для проведения обслуживания информационной системы.

Защита носителей: Организации должны: (i) обеспечить сохранность носителей информации, как бумажных, так и цифровых; (ii) ограничить доступ к информации на информационных носителях систем для авторизованных пользователей; и (iii) санировать или уничтожать информацию на носителе, до его списания или высвобождения для повторного использования.

Защита физическая и защита окружения: Организации должны: (i) ограничить физический доступ к информационным системам, оборудованию, а также соответствующему операционному окружению для авторизованных лиц; (ii) обеспечить защиту физических площадей предприятия и поддерживающую инфраструктуру для информационных систем; (iii) обеспечить поддерживающие утилиты для информационных систем; (iv) обеспечить защиту информационных систем от неблагоприятных условий окружающей среды; и (v) обеспечить соответствующий контроль окружения в учреждениях,

[5] Верификация – здесь метод распознавания лжи или подмены, например, путем применения биометрических методов, в отличие от аутентификации, использующей стандартные методы подтверждения, к примеру, на основе сертификатов X.509.

содержащих информационные системы.

Планирование: Организации должны разработать <соответствующую>документацию, периодически обновлять реализации планов охраны организационно-информационных систем, которые описывают действующие и/или планируемые меры безопасности и контроля информационных систем, и правила поведения для лиц, имеющих доступ к информационным системам.

Обеспечение безопасности персонала: Организации должны: (i) удостовериться, что лица, занимающие ответственные должности внутри организации (в том числе сервис-провайдеры третьей стороны) заслуживают доверия и соответствуют установленным критериям безопасности для таких должностей; (ii) убедиться, что информация организации и информационные системы защищены во время и после <критических> действий персонала (например, остановка и перезагрузка информационных комплексов, перенос информации и другие работы с ИТ; и (iii) использовать формальные санкции для персонала, не соблюдающего принятой Подитики и процедур безопасности.

Оценка риска: Организации должны периодически оценивать риски для деятельности организации (включая миссию, функции, имидж или репутацию), а также для организационных активов и физических лиц, как результат функционирования информационных систем организации и связанных с ними переработки, хранения или передачи информации об организации.

Системы и Приобретаемые Услуги: Организации должны: (i) выделить достаточные ресурсы для адекватной защиты информационных систем; (ii) использовать инструменты жизненного цикла системы, включающие в себя соображения информационной безопасности; (iii) при эксплуатации программного обеспечения устанавливать и использовать необходимые ограничения; и (iv) быть уверенными, что провайдеры третьей стороны используют адекватные меры безопасности для защиты информации, приложений и/или сервисов, переданных организацией на аутсорсинг.

Системы и Защита Коммуникаций: Организации должны: (i) осуществлять мониторинг, контроль и защиту коммуникаций (т.е., информации, передаваемой или получаемой с помощью информационных систем организации) на внешних границах и ключевых внутренних границах информационных систем; и (ii) использовать архитектурные проекты, техники разработки программного обеспечения и принципы системного инжиниринга, способствующие продвижению эффективных методов обеспечения информационной безопасности в рамках информационных систем организаций.

Системы и Целостность Информации: Организации должны: (i) определять, документировать и регулярно устранять замеченные недостатки; (ii) обеспечить защиту от вредоносного кода в соответствующих местах внутри информационных систем; и (iii) вести мониторинг событий безопасности в информационных системах и принимать адекватные меры.

ВЫБОР КОНТРОЛЯ БЕЗОПАСНОСТИ

Организации должны удовлетворять минимальным требованиям безопасности настоящего стандарта путем выбора соответствующего контроля (управления) безопасностью и обеспечения требований безопасности, описанных в Специальной Публикации НИСТ 800-53, Рекомендуемые меры контроля в целях безопасности систем Федеральной Информации [18][6] Процесс выбора соответствующего контроля и обеспечения безопасности в требованиях к информационным системам организации для достижения адекватного уровня безопасности[7] является многогранным на основе оценки рисков, управления и деятельности, связанной с оперативным персоналом в организации. **Разбиение информации по категориям,** как того требует FIPS Публикации 199, является

[6] Организации должны использовать самую последнюю версию Публикации НИСТ 800-53, с поправками, для выбора соответствующго управления безопасностью.

[7] бюро Управления и Бюджета (OMB) Циркуляр А-130, приложение III, определяет адекватную безопасность как безопасность, соизмеримую с риском и величиной ущерба от потери вследствие ненадлежащего использования, несанкционированного доступа или изменения информации.

первым шагом в процессе управления рисками[8]. в продолжение процесса классификации информации, организации необходимо выбрать соответствующий набор мер контроля в целях безопасности своих информационных систем, которые удовлетворяют минимальным требованиям безопасности, изложенным в настоящем стандарте. Выбранный набор мер безопасности должен включать одну из трех, соответственно подобранных, исходных линий контроля безопасности, согласно НИСТ Специальной Публикации 800-53, связанных с построенным «импакт-уровнем» информационной системы организации, как было определено в ходе категоризации безопасности.

- для информационных систем с низким импакт-уровнем, как минимум, работает надлежащим образом адаптированный контроль безопасности от низкого исходного уровня мер безопасности, определенные в НИСТ Специальной Публикации 800-53 и необходимо убедиться, что минимальные требования безопасности, связанные с низким базовым уровнем, удовлетворены.

- Для информационных систем со средним импакт-уровнем организации должны, как минимум, внедрять надлежащим образом подобранный[9] контроль безопасности от умеренной базовой линии мер безопасности, определенной в НИСТ Специальной Публикации 800-53 и необходимо убедиться, что минимальные требования безопасности, связанные со средней базовой линией, удовлетворены.

[8] Категоризация безопасности должна быть выполнена в масштабах деятельности всего предприятия с привлечением руководителей высшего уровня организационной должностных лиц, включая, но не ограничиваясь ими, CIO’s (Chief Information Officers), старших сорудников агентства информационной безопасности, санкционирующих чиновников (a.k.a. органов аккредитации), владельцев информационных систем и владельцев информации.

[9] Адаптация руководства по базовым линиям» управления безопасностью, предусмотрены в Специальной Публикации НИСТ 800-53.

- Для информационных систем с высоким импакт-фактором, организации должны, как минимум, применять соответствующим образом подобранную систему управления безопасностью с высокой базовой линией управления безопасностью определенной в НИСТ Специальной Публикации 800-53 и должны при этом убедиться, что минимальные требования безопасности, ассоциированные с высокой базовой линией, удовлетворены.

Организации должны использовать все средства управления безопасностью на соответствующих уровню безопасности базовых линиях, если определенные исключения не допускаются на основе руководства, излагаемого в NIST 800-53.

Для реализация экономически эффективного, риск-ориентированного подхода в обеспечении надлежащего уровня безопасности во всей организации, контроля и безопасности разработанного базового подхода, мероприятия должны быть согласованы и утверждены у соответствующих должностных лиц организации (напр., директор по информационным технологиям, CIO), старших должностных лиц агентства по информационной безопасности, санкционирующих чиновников, и/или должностными лицами, назначенными представителями от соответствующих компетентных организаций. Результирующий набор мер безопасности должен быть задокументирован в план обеспечения безопасности информационной системы.

Литература

1. Дабагов, А. Р. Информатизация здравоохранения и некоторые проблемы построения интегрированных медицинских информационных систем. Журнал Радиоэлектроники, 5, 2011, стр. 1-57.

2. Дабагов, А. Р. и Соколов, С. А. О проблемах безопасности в контексте открытой системной архитектуры. III Всероссийская конференция "Радиолокация и радиосвязь". М. : ИРЭ РАН, 2009. (электронный источник) http://jre.cplire.ru/jre/library/3conference/conf3rd.pdf с.696-702.

3. Бетелин, В. Б., и др. Профили защиты на основе "Общих критериев". Аналитический обзор. Бюллетень Jet Info. 2003, 3. в эл. сб. http://www.jetinfo.ru/2003.

4. Хант, Ч. и Зартарьян, В. Разведка на службе Вашего предприятия. Киев : Укрзакордонсервис, 1992, 159 с.

5. Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach. National Institute of Standards and Technology. Gaithersburg, MD 20899-8930 : Dept.of Commerce, 2010. 93 C.

6. Леманский, Д. А. и Салахова, Ф. Я. Методические подходы к защите информации при введении в гражданско-правовой документооборот результатов интеллектуальной деятельности высокотехнологичных предприятий. М. : ИпРЖР, 2003. с. 51-58.

7. Гутман, Барбара и Бэгвилл, Роберт. Политика безопасности при работе в Интернете - техническое руководство. : National Institute of Standards and Technology (NIST). http://citforum.ru/internet/security_guide/

8. Руководство по проектированию профилей среды открытой системы организации-пользователя; Руководство по проектированию профилей среды открытой системы, Рекомендации Института инженеров по электротехнике и электронике (IEEE). Москва : Янус-К, 2002. стр. 160. , Пер. с англ. под общей редакцией Олейникова А.Я. ISBN5-8037-0085-1.

9. Зегжда, Д. П. и Ивашко, А. М. Основы безопасности информационных систем. М. : Горячая линия-Телеком, 2000. 452 С.

10. Грушо, А.А. и Е.Е.Тимонина. Теоретические основы защиты информации. Москва : Изд. агентства "Яхтсмен", 1996, 188 С.

11. Sandhu, Ravi, и др. Role-Based Access Control Model. : IEEE, 1996 r., IEEE Computer, T. 29, стр. 38-47.

12. Demchenko, Yuri, Gommans, Leon и de Laat, Cees. Extending Role Based Access Control Model for Distributed Multidomain Applications. Amsterdam ,

University of Amsterdam, System and Network Engineering Group, 2006 r. http://www.uazone.org/demch/papers/sec2007-rbac-dm-ext-06.pdf&sa=U&ei=MfgQUvmDGeW44ATv0YD4Dw&ved=0CDMQFjAH&usg=AFQjCNFzblg3s9uyUInEnJ2B__SYiKSEXQ.

13. Bulter, Michael. Extending Role Based Access Control . : A SANS Whitepaper. https://www.sans.org/reading-room/analysts-program/access-control-foxt&sa=U&ei=MfgQUvmDGeW44ATv0YD4Dw&ved=0CCMQFjAB&usg=AFQjCNFVFuwpUN_C6EWKCpe5i063LHmYSQ.

14. Hu, Vincent, и др. Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft). : National Institute of Standards and Technnology, 2013. NIST Special Publication 800-162, 54 C.

15. NIST Cloud Computing Security Reference Architecture. US Dept. of Commerce. 2014.204C.

16. Плэтт, В. Информационная работа стратегической разведки. Под ред. А.Ф.Федорова. Пер. с англ. Е.В.Пескова. М. : ИИЛ, 1958, 341С.

17. FIPS PUB 200. Minimum Security Requirements for Federal Information and Information Systems. National Institute of Standards and Technology, 2006. 17 C.

18. Security and Privacy Controls for Federal Information Systems. : National Institute of Standards and Technology, 2013. NIST Special Publication 800-53 Rev.4, 457 C.