УДК 004.056

Р. С. Койнов, А. С. Добрынин

МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ ТИПОВОЙ БИБЛИОТЕЧНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Предложена модель безопасности для защиты данных в автоматизированных библиотечных информационных системах. Обоснована необходимость создания новой модели управления доступом, отличной от классических, отвечающей современным требованиям по безопасности, гибкости и простоте в настройке прав доступа к защищаемым объектам. Обоснование строится на необходимости защиты большого количества объектов, использования различных вариантов организации доступа к информации, в том числе к полнотекстовым ресурсам (объектам), начиная от открытого доступа и заканчивая строго ограниченной определённой группой пользователей, а также на необходимости быстрого и комфортного доступа читателей к объектам с учётом требований регламента работы библиотеки и законов «Об авторском праве и смежных правах» и «О персональных данных». Модель учитывает все эти требования и ограничения, позволяя использовать различные варианты аутентификации помимо встроенной (в том числе по IP-адресам, Active Directory по LDAP-протоколу, посредством электронной подписи или любую другую внешнюю аутентификацию), учитывает ограничения по времени доступа, по коллекциям объектов, по группам пользователей, с учётом степени конфиденциальности объектов. Описаны основные элементы и операторы предлагаемой модели безопасности. Использование модели в автоматизированных библиотечных информационных системах позволит значительно упростить работу администратора безопасности, а также избежать ошибок назначения прав доступа.

Ключевые слова: модель управления доступом, разграничение доступа, защита данных, модель разграничения доступа, информационные библиотечные системы.

Введение

Существующие классические модели безопасности не обеспечивают должной гибкости при настройке прав доступа к защищаемым объектам в автоматизированных библиотечных информационных системах (АБИС). Это связано прежде всего с тем, что читателю необходимо предоставлять доступ максимально комфортно, быстро и, желательно, без дополнительных шагов по его аутентификации и авторизации, но в то же время необходимо учитывать требования Закона «Об авторском праве и смежных правах», а также регламент работы библиотеки и Закон «О персональных данных». Это подразумевает различные варианты организации доступа к информации, в том числе полнотекстовым ресурсам (объектам), начиная от открытого доступа и заканчивая строго ограниченным определённой группой пользователей. Кроме того, доступ может быть лимитирован по времени; удостоверяться электронной подписью, выданной внутрикорпоративным удостоверяющим центром (например, «VipNet», «Автограф» и т. д.) или сторонним удостоверяющим центром; предоставляться только с определённых IP-адресов (или их диапазонов) сети Интернет, или может быть ограничен ещё какими-либо условиями. Наличие в АБИС пользователей, которые не являются полноценными читателями, но которым необходимо получить единовременный доступ к одному или нескольким объектам (так называемые «внешние временные читатели»), также увеличивает объём работ для администратора безопасности АБИС. Поскольку всё вышеперечисленное в конечном счёте может привести к возникновению ошибок прав доступа, ***целью нашего исследования*** стала разработка новой модели безопасности, учитывающей особенности предоставления доступа к данным в АБИС, а именно различные варианты аутентификации, ограничения по времени доступа, ограничения по группам пользователей, с учётом степени конфиденциальности объектов.

Обзор существующих АБИС

В настоящее время в библиотеках АБИС внедряются повсеместно [1, 2]. Такая система обычно состоит из реляционной базы данных, программного обеспечения, которое взаимодействует с базой данных, и двух графических пользовательских интерфейсов (один для читателей, второй для персонала).

Каждый читатель (посетитель) и объект (книги, журналы, диски и т. д.) имеют уникальный идентификатор в базе данных, который позволяет АБИС отслеживать историю обращений, заказов, загрузок и т. д.

Данный рынок программного обеспечения достаточно инертен и в России представлен в основном либо бесплатными (open-source) системами управления библиографической информацией (Evergreen, CDS Invenio, Koha, NewGenLib, PhpMyBibli, Greenstone, OpenBiblio и др.), либо национальными платными системами (КАБИС, Абсотек Юникод (Absotheque Unicode), МАРК-SQL, Руслан, Либэр, УФД/Библиотека, Senayan, OPAC-Global, Ирбис и др.).

У вышеназванных категорий программного обеспечения есть свои преимущества и недостатки. Так, первые решения (open-source) ориентированы в первую очередь на западный рынок (т. к. разрабатываются и поддерживаются в основном зарубежными программистами для своих потребителей), используют западные стандарты библиографического описания и имеют достаточно ограниченные возможности по настройке прав доступа к объектам хранения. У вторых web-интерфейсы для читателей значительно проигрывают их зарубежным аналогам (даже бесплатным). У тех и других отсутствует также возможность быстрой интеграции АБИС в корпоративную среду организации. Так, например, у большинства систем нет возможности внешней аутентификации читателей (например, Active Directory в локальной или корпоративной сети), нет возможности встроенного разграничения доступа к объектам по IP-адресам (или диапазонам), отсутствуют возможности по созданию ограниченного по времени (и (или) количеству скачиваний) доступа к объекту (группе объектов). Во всех системах в настоящее время отсутствует возможность наиболее безопасной аутентификации электронной подписью, выданной внутрикорпоративным удостоверяющим центром (например, «VipNet», «Автограф» и т. д.) или сторонним удостоверяющим центром. Во многих системах отсутствует также возможность разграничения права доступа по отделам и службам библиотеки при обработке объектов. Информация, обрабатываемая в АБИС, включает в себя персональные данные читателей, следовательно, доступ к такой информации должен быть ограниченным и строго контролируемым [3, 4].

Существующие подходы к защите данных, используемых в АБИС

Наиболее надежным с точки зрения безопасности считается подход, подразумевающий проверку прав доступа пользователей на уровне базы данных. Во многих современных СУБД имеются встроенные средства аутентификации и авторизации пользователей, использующие комбинацию дискреционной и ролевой модели безопасности. В данном случае защитой обеспечиваются «сущности» баз данных, в том числе таблицы, представления и т. д. (они являются объектами безопасности). В качестве субъектов безопасности выступают пользователи (или их группы) АБИС. Для каждого субъекта может быть определено право доступа к объекту (или их группе): например вставка, выборка, редактирование, удаление [5, 6].

Однако такой подход к защите данных не решает всех задач, которые возникают в процессе работы библиотеки и эксплуатации АБИС, и его применение в чистом виде является недостаточным и неудобным.

Прежде всего это связано со спецификой работы библиотек, которые делятся на публичные, вузовские, отраслевые, заводские и т. д. И это определяет степень открытости информации, размещаемой в АБИС, её конфиденциальность, варианты её получения читателем (далее будут рассматриваться, помимо классической книговыдачи, варианты электронной доставки объектов безопасности с использованием web-технологий). К особенностям электронной доставки объектов можно отнести большое количество защищаемых объектов, зависимость прав доступа, обеспечение возможности быстрой аутентификации нестандартным методом (IP-адрес или диапазон, аутентификация через социальные сети с подтверждением профиля читателя, посредством электронной подписи и т. д.), обеспечение возможности для работы внешних читателей с ограничением по списку объектов и по времени с обязательным соблюдением требований Закона «Об авторском праве и смежных правах» и Закона «О персональных данных».

Права доступа зависят от следующих факторов:

– время доступа к данным; по прошествии определенного времени доступ на чтение для субъекта должен быть закрыт, это определяется датой окончания действия читательского билета;

– текущие операции чтения должны быть максимально комфортными для читателей; на время действия читательского билета или на время обучения (например, для случая вузовской библиотеки) читатель должен получать доступ к объектам, согласно его спискам разрешений, максимально быстро (желательно без дополнительных шагов по его аутентификации);

– возможность работы временных внешних читателей с ограничением по спискам объектов и по времени;

– доступ читателя к ограниченным спискам объектов в зависимости от свойств субъекта (читателя); например, в вузовской библиотеке может предоставляться ограниченный доступ к сформированным коллекциям учебно-методических материалов в зависимости от специальности, направления обучения, текущего курса;

– личная информация читателя относится к персональным данным, и, хотя, обычно в электронных библиотечных системах хранятся общедоступные сведения (ФИО и, в худшем случае, электронная почта), доступ к этой информации должен быть ограничен;

– степень конфиденциальности информации; доступ к некоторым объектам должен быть открыт только узкому кругу лиц независимо от других условий.

Наличие большого количества защищаемых объектов предполагает ограничение доступа к защищаемым объектам не только на уровне таблиц, но и на уровне их записей, а также сессий web-сервера.

Таким образом, для обеспечения этого требования с учетом особенностей, указанных выше, достаточно часто приходится переопределять права доступа читателей к АБИС (в вузовских библиотеках как минимум раз в год, в связи со сменой курса обучения читателей).

Учитывая огромное количество в АБИС защищаемых объектов, можно сделать вывод, что обеспечить такой режим работы штатными средствами весьма затруднительно. В любом случае объем работы администратора безопасности существенно увеличится, что неизбежно приведет к ошибкам и несвоевременному переназначению прав доступа.

Таким образом, актуальной является задача модификации стандартного механизма аутентификации и авторизации с целью избавления администратора безопасности от большого объема рутинной работы.

Для достижения поставленной цели прежде всего необходимо разработать модель системы безопасности обобщенной АБИС.

Формальное описание новой модели

С учетом требований к модели разграничения доступа в АБИС была разработана следующая модель.

Основные элементы: S – множество субъектов; G − множество групп субъектов (читателей, пользователей); O – множество объектов (права доступа на некоторые объекты могут быть заданы явно, для остальных объектов права определяются динамически); ACL – множество списков контроля доступа (для явного задания прав); $\{g, o, \{r\}\}$ – список контроля доступа; R − множество прав доступа; $(L, \leq)$ – решетка уровней конфиденциальности; $\{O, t_{\text{СОЗД}}, t_{\text{ПРЕД}}\}$ – метка времени, представляющая собой объект, дату/время его создания, предельную дату/время доступа к нему; I – множество меток времени (определяют предельную дату/время доступа к объекту); $i : O, G \to t_{\text{ПРЕД}}$ – функция, возвращающая значение времени, по истечении которого доступ к объекту для группы прекращается; $\{S, t_{\text{СОЗД}}, t_{\text{ПРЕД}}\}$ – метка времени, представляющая собой субъект, время его создания, предельное время его доступа к АБИС; K – множество меток времени (определяют предельную дату/время доступа субъектов в АБИС); $k : S \to t_{\text{ПРЕД}}$ – функция, возвращающая значение времени, по истечении которого доступ субъекта в АБИС прекращается; $AUTH$ – множество способов аутентификации субъектов; $n : S, AUTH \to s_{AUTH}$ – функция, возвращающая дескриптор безопасности субъекта при выбранном способе аутентификации; IP – множество IP-адресов, которые могут быть привязаны к субъектам для быстрой аутентификации при соответствующем способе аутентификации $m : IP \to AUTH_{IP} \to s_{AUTH}^{IP}$; COL – множество коллекций объектов, которые могут быть доступны субъектам при соответствующих назначенных правах доступа, при этом $COL \subseteq O$; $c : S, O \to R$ – функция, определяющая для каждого субъекта права доступа на определенный объект в зависимости от взаимоотношений между ними; $PG \subseteq G$ – множество привилегированных групп, члены которых имеют полный доступ ко всем объектам; $PA : G, O \to R$ – функция, определяющая множество прав r группы g на объект o; при этом объекты могут быть сгруппированы в коллекции для упроще-

ния назначения прав доступа, поэтому $PA_{COL} : G, COL \to R$ – функция, определяющая множество прав r группы g на коллекцию объектов col; $SA_s \in G$ – множество групп, к которым принадлежит субъект; $group : S \to SA_s$ – функция, определяющая множество групп, к которым принадлежит субъект s; $Avail : S, O, R \to 1,0$ – функция, определяющая доступность права r субъекта s на объект o; $q(S, AUTH, IP, O, COL, G, PG, I, K, L, ACL)$ – состояние системы; Q – множество состояний системы.

В данной модели используются следующие операторы:

– создать объект o' с уровнем конфиденциальности l_o, меткой времени $\{O, t_{\text{СОЗД}}, t_{\text{ПРЕД}}\}$. Условие выполнения: $o' \notin O$, $l_o \in L$. Новое состояние системы: $S' = S$, $O' = O \cup \{o'\}$, $G' = G$, $PG' = PG$, $L' = L$, $I' = I \cup \{i_{oc}\} \cup \{i_{ol}\}$, $AUTH' = AUTH$, $IP' = IP$, $COL' = COL$, $K' = K$, $ACL' = ACL$;

– создать коллекцию col' с уровнем конфиденциальности l_{col}. Условие выполнения: $col' \notin COL$, $l_{col} \in L$. Новое состояние системы: $S' = S$, $O' = O$, $G' = G$, $PG' = PG$, $L' = L$, $I' = I$, $AUTH' = AUTH$, $IP' = IP$, $COL' = COL \cup \{col'\}$, $K' = K$, $ACL' = ACL$;

– включить объект o' в множество коллекций col. Условие выполнения: $o' \in O$, $col' \in COL$, $o' \notin col'$. Новое состояние системы: $s' \in S$, $O' = O$, $G' = G$, $AUTH' = AUTH$, $PG' = PG$, $L' = L$, $I' = I$, $K' = K$, $IP' = IP$, $COL' = COL$, $ACL' = ACL$, $col' = col \cup o'$;

– создать группу g' с уровнем конфиденциальности l_r, множеством прав доступа $\{r\}$ на объекты $\{o'\}$ и их коллекции $\{col'\}$. Условие выполнения: $g \notin G$, $l_r \in L$. Новое состояние системы: $S' = S$, $O' = O$, $G' = G \cup \{g'\}$, $PG' = PG$, $L' = L$, $I' = I$, $K' = K$, $AUTH' = AUTH$, $IP' = IP$, $COL' = COL$, $ACL' = ACL \cup \{g', \{o'\}, \{col'\}, \{r\}\}$;

– добавить право доступа r' группы g' на объект o' или коллекцию col' путем изменения/добавления списка контроля доступа acl'. Условие выполнения: $g' \in G$, $r' \in R$. Новое состояние системы: $S' = S$, $O' = O$, $G' = G$, $PG' = PG$, $L' = L$, $I' = I$, $K' = K$, $AUTH' = AUTH$, $IP' = IP$, $COL' = COL$, $ACL' = ACL \cup \{acl'\}$;

– удалить право доступа r' группы g' на объект o' или коллекцию col' путем изменения/удаления списка контроля доступа acl'. Условие выполнения: $\{g', o', col', r'\} \in ACL$. Новое состояние системы: $S' = S$, $O' = O$, $G' = G$, $PG' = PG$, $L' = L$, $I' = I$, $K' = K$, $AUTH' = AUTH$, $IP' = IP$, $COL' = COL$, $ACL' = ACL / \{acl'\}$;

– создать субъект s', принадлежащий множеству групп g' и использующий множество способов аутентификации $auth'$. Условие выполнения: $g' \in G$, $s' \in S$. Новое состояние системы: $S' = S \cup \{s'\}$, $O' = O$, $G' = G / \{g'\} \cup \{g' \cup s'\}$, $AUTH' = AUTH / \{auth'\} \cup \{auth' \cup s'\}$, $PG' = PG$, $L' = L$, $I' = I$, $K' = K \cup \{k_{sc}\} \cup \{k_{sl}\}$, $IP' = IP$, $COL' = COL$, $ACL' = ACL$;

– включить субъект s' в множество групп g'. Условие выполнения: $g' \in G$, $s' \in S$, $g \notin SA_{s'}$. Новое состояние системы: $s' \in S$, $O' = O$, $G' = G / \{g'\} \cup \{g' \cup s'\}$, $AUTH' = AUTH$, $PG' = PG$, $L' = L$, $I' = I$, $K' = K$, $IP' = IP$, $COL' = COL$, $ACL' = ACL$, $SA'_{s'} = SA'_s / \{g'\}$;

– исключить субъект s из множества групп g'. Условие выполнения: $g' \in SA$, $s' \in S$. Новое состояние системы: $s' \in S$, $O' = O$, $G' = G / \{g'\} \cup \{g' / s'\}$, $AUTH' = AUTH$, $PG' = PG$, $L' = L$, $I' = I$, $K' = K$, $IP' = IP$, $COL' = COL$, $ACL' = ACL$, $SA'_{s'} = SA'_s \setminus \{g'\}$;

– включить группу g' в множество привилегированных. Условие выполнения: $g' \in G$, $g' \notin PG$. Новое состояние системы: $s' \in S$, $O' = O$, $G' = G$, $AUTH' = AUTH$, $PG' = PG \cup \{g'\}$, $L' = L$, $I' = I$, $K' = K$, $IP' = IP$, $COL' = COL$, $ACL' = ACL$;

– исключить объект o' из множества коллекций col. Условие выполнения: $o' \in O$, $col' \in COL$, $o' \in col'$. Новое состояние системы: $s' \in S$, $O' = O$, $G' = G$, $AUTH' = AUTH$, $PG' = PG$, $L' = L$, $I' = I$, $K' = K$, $IP' = IP$, $COL' = COL$, $ACL' = ACL$, $col' = col \setminus o'$;

– исключить группу g' из множества привилегированных. Условие выполнения: $g' \in G$, $g' \in PG$. Новое состояние системы: $s' \in S$, $O' = O$, $G' = G$, $AUTH' = AUTH$, $PG' = PG \setminus \{g'\}$, $L' = L$, $I' = I$, $K' = K$, $IP' = IP$, $COL' = COL$, $ACL' = ACL$;

– уничтожить объект o'. Условие выполнения: $o' \in O$. Новое состояние системы: $s' \in S$, $O' = O \setminus \{o'\}$, $G' = G$, $AUTH' = AUTH$, $PG' = PG$, $L' = L$, $I' = I \setminus \left(\{i_{oc}\} \cup \{i_{ol}\}\right)$, $K' = K$, $IP' = IP$, $COL' = COL$, $ACL' = ACL$;

– уничтожить группу g'. Условие выполнения: $g' \in G$. Новое состояние системы: $s' \in S$, $O' = O$, $G' = G \setminus \{g'\}$, $AUTH' = AUTH$, $PG' = PG$, $L' = L$, $I' = I$, $K' = K$, $IP' = IP$, $COL' = COL$, $ACL' = ACL$;

– уничтожить субъект s'. Условие выполнения: $s' \in S$. Новое состояние системы: $S' = S \setminus \{s'\}$, $O' = O$, $G' = G$, $AUTH' = AUTH$, $PG' = PG$, $L' = L$, $I' = I$, $K' = K \setminus \left(\{k_{sc}\} \cup \{k_{sl}\}\right)$, $IP' = IP$, $COL' = COL$, $ACL' = ACL$;

– определить доступность права r' субъекта s' с уровнем доступа l_s на объект o' с уровнем конфиденциальности $l_{o'}$ или коллекцию col' с уровнем конфиденциальности l_{col}.

Если $\left(SA_{s'} \cap PG\right) \neq \varnothing$, то $Avail = 1$;

Иначе $$Avail = \left[\begin{array}{l} \left(t_{\text{ТЕКУЩ}} < k\left(s'\right)\right) \wedge \left(t_{\text{ТЕКУЩ}} < i\left(o'\right)\right) \wedge \\ \left(\left(\left(r' \in PA\left(SA_{S'}, o'\right)\right) \wedge \left(l_s \geq l_o\right)\right) \vee r' \in c\left(s', o'\right)\right) \vee \\ \left(\left(\left(r' \in PA_{COL}\left(SA_{S'}, col'\right)\right) \wedge \left(l_s \geq l_{col}\right)\right) \vee r' \in c\left(s', col'\right)\right) \end{array}\right].$$

При использовании данной модели процедура определения доступности объекта выглядит следующим образом.

Каждый субъект (пользователь АБИС) использует определённый набор способов аутентификации. Это могут быть: встроенная в АБИС система аутентификации, доменная (LDAP) аутентификация в корпоративной сети организации, аутентификация через социальные сети, упрощенная аутентификация по IP-адресу (или диапазону адресов) субъекта, аутентификация посредством электронной подписи и т. д. Любой из этих способов должен вернуть один и тот же дескриптор безопасности субъекта в АБИС.

Так, например, в корпоративной сети вуза за кафедрой можно закрепить диапазон IP-адресов, и субъекты (читатели), обращающиеся из сети кафедры к АБИС вуза, будут иметь возможность быстрого доступа к учебным материалам (коллекциям объектов), относящимися конкретно к данной кафедре. В этом случае IP-адреса необходимо закрепить за группами (учебными) субъектов.

Каждый субъект входит в определенные группы, имеет временные метки создания и окончания срока действия читательского билета. Если текущее время превышает предельное время активности читательского билета, доступ к АБИС прекращается. Группы могут быть привилегированными и непривилегированными (обычными). Под группой может пониматься и учебная группа (в случае вузовской АБИС). Каждая группа обладает определенным уровнем конфиденциальности. Права доступа субъектов определяются как совокупность прав, явно указанных ему, и прав, указанных для групп. При попытке субъекта совершить определенную операцию над объектом происходит проверка доступности данной операции. Если пользователь входит в одну из привилегированных групп, он имеет полный доступ к любому объекту. Иначе происходит проверка меток времени. Если текущее время превышает предельную дату/время доступа к объекту, субъект не имеет права доступа к нему.

Следующим шагом является проверка явно указанных прав и меток конфиденциальности. Если одна из групп, в которые входит пользователь, обладает правами на данную операцию и уровень доступа субъекта больше либо равен уровню конфиденциальности объекта (коллекции), доступ гарантируется.

Вторым условием гарантии доступа является наличие возможности осуществлять данную операцию исходя из взаимоотношений между объектом (коллекцией) и субъектом непосредственно (при этом не учитываются уровни конфиденциальности). Таким образом, в систему заведомо добавляются необходимые группы со всеми атрибутами и списком прав доступа. Наличие меток конфиденциальности обусловливается обширным списком условий, по которым доступ должен или не должен предоставляться, а также большим количеством объектов. Разделение пользователей на группы необходимо для того, чтобы разграничивать права в зависимости от должности пользователя и места пребывания пациента.

Для реализации представленной модели нами предлагается использовать механизм триггеров, в которых должна быть реализована логика расширенной проверки прав пользователя на выполнение операции в соответствии с разработанной моделью, а также расширить базовый функционал реляционной базы данных возможностями, предлагаемыми web-сервером и языками разработки web-приложений (php, ASP, ASP.NET и т. д.). Блок-схема расширенной проверки прав пользователя на выполнение операции представлена на рис. 1, пример реализации – на рис. 2. В частности, для работы с IP-адресами в PHP можно использовать суперглобальный массив $_SERVER['REMOTE_ADDR'], в ASP – системный объект Request.ServerVariables("remote_addr"). Возможность аутентификации посредством Active Directory по протоколу LDAP или любой другой способ также могут быть реализованы программно.

Рис. 1. Блок-схема расширенной проверки прав пользователя на выполнение операции

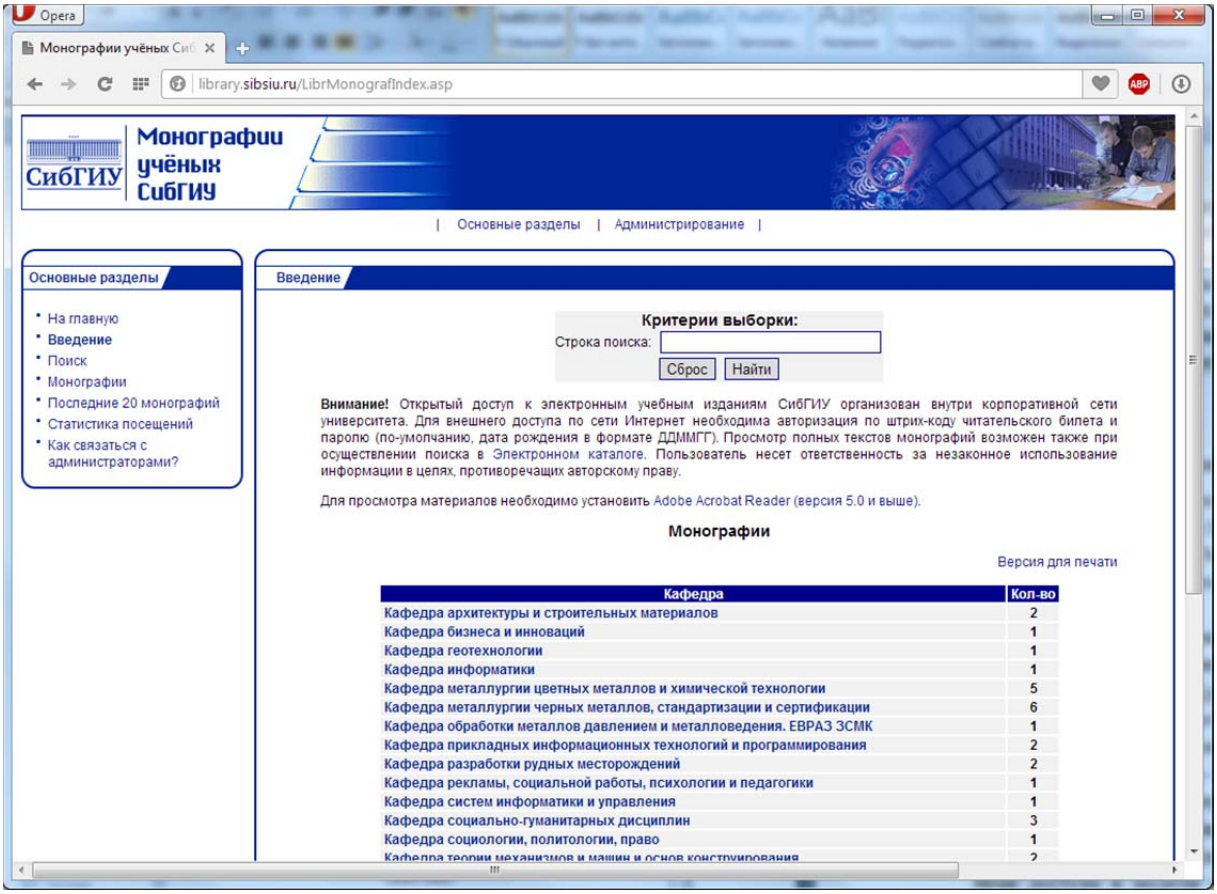

Рис. 2. Пример окна web-приложения, предоставляющего доступ к коллекции и использующего предложенную модель безопасности, в том числе аутентификацию по IP-адресам, штрих-коду и паролю читательского билета, внешнюю аутентификацию (по протоколу LDAP)

В соответствии с представленной моделью безопасности нами для научно-технической библиотеки Сибирского государственного индустриального университета разработано web-приложение, работающее совместно ИБС «Virtua» корпорации «Innovative», которое расширяет базовый функционал системы до необходимого уровня. Пример окна приложения, предоставляющего доступ к одной (монографии учёных СибГИУ) из многих коллекций, представлен на рис. 2. Приложение написано на ASP.NET с использованием C#. Администраторская панель приложения позволяет определять дополнительные параметры безопасности, предусмотренные предлагаемой моделью.

Заключение

Предполагается, что применение предложенной модели управления доступом типовой библиотечной информационной системы позволит существенно снизить вероятность возникновения ошибок настройки прав доступа, а уровень обеспечения безопасности данных системы существенно возрастет. Дальнейшее развитие предложенной модели в перспективе предполагает сокращение объема работы администратора безопасности системы.

СПИСОК ЛИТЕРАТУРЫ

1. *Горбунов-Посадов М. М., Ермаков А. В., Луховицкая Э. С., Скорнякова Р. Ю.* О выборе автоматизированной информационной библиотечной системы для библиотеки ИПМ // Препринты ИПМ им. М. В. Келдыша. 2011. № 2. 32 с. URL: http://library.keldysh.ru/preprint.asp?id=2011-2.

2. *Камалетдинов Р. К.* Автоматизированные библиотечные информационные системы как средство освоения и внедрения информационно-коммуникационных технологий: опыт Республики Татарстан // Вестн. Казан. гос. ун-та культуры и искусств. 2012. № 4. С. 52–60.

3. *Баранова Е.* Защита персональных данных: проблемы и решения // Библиотека. 2011. № 1. С. 32–35.

4. *Бойкова О.* Защита персональных данных // Независимый библиотечный адвокат. 2012. № 1. С. 34–46.

5. *Смольянинов В. Ю.* Анализ условий предоставления и получения прав доступа в модели управления доступом MS SQL Server // Прикладная дискретная математика. 2014. № 2. С. 48–78.

6. *Медведев Н. В., Гришин Г. А.* Модели управления доступом в распределенных информационных системах // Наука и образование. 2011. № 01. С. 1–19. URL: http://technomag.bmstu.ru/doc/164245.html (дата обращения: 02.06.2016).

Статья поступила в редакцию 11.07.2016

ИНФОРМАЦИЯ ОБ АВТОРАХ

Койнов Роман Сергеевич – Россия, 654007, Новокузнецк; Сибирский государственный индустриальный университет; старший преподаватель кафедры автоматизации и информационных систем; koynov_rs@mail.ru.

Добрынин Алексей Сергеевич – Россия, 654007, Новокузнецк; Сибирский государственный индустриальный университет; старший преподаватель кафедры автоматизации и информационных систем; serpentfly@mail.ru.

R. S. Koynov, A. S. Dobrynin

ACCESS CONTROL MODEL OF THE TYPICAL LIBRARY INFORMATION SYSTEM

Abstract. The article describes a model of security to protect data in the automated information library systems (AILS). The necessity of creating a new model of access control that is different from the classic one, meeting the modern requirements for security, flexibility and easiness of setting up the access rights to the protected objects. Justification is based on the need to protect a large number of objects, the use of different options for accessing information, including full-text resources (objects), from open access to severely restricted certain group of users, and also the need for fast and comfortable access of the readers to the sites, taking into account the requirements of the regulations of the library and the Law "On Copyright and Related Rights" and "On Personal data". The developed model takes into account all of these requirements and restrictions, allowing a usage of different options of authentication in addition to the built-in one (including IP-addresses, Active Directory for LDAP-protocol, by electronic signature, or any other external authentication), considers the limitations on access time, on the collection of objects, for groups of users, taking into account the degree of confidentiality of the facilities. The article describes the basic elements and the operators of the proposed security model. Using the proposed model in the AILS would greatly simplify the administrator's job security, as well as eliminate mistakes of access rights.

Key words: information security, access control, data protection, access control model, library information systems.

REFERENCES

1. Gorbunov-Posadov M. M., Ermakov A. V., Lukhovitskaia E. S., Skorniakova R. Iu. *O vybore avtomatizirovannoi informatsionnoi bibliotechnoi sistemy dlia biblioteki IPM* [On the choice of the automated information library system for the library of the Institute of Applied Mathematics]. Preprinty IPM imeni M. V. Keldysha. 2011. № 2. 32 p. Available at: http://library.keldysh.ru/preprint.asp?id=2011-2.

2. Kamaletdinov R. K. Avtomatizirovannye bibliotechnye informatsionnye sistemy kak sredstvo osvoeniia i vnedreniia informatsionno-kommunikatsionnykh tekhnologii: opyt Respubliki Tatarstan [Automated library information systems as a means of mastering and introducing the information-communication technologies: experience of the Republic of Tatarstan]. *Vestnik Kazanskogo gosudarstvennogo universiteta kul'tury i iskusstv*, 2012, no. 4, pp. 52–60.

3. Baranova E. Zashchita personal'nykh dannykh: problemy i resheniia [Personal data protection: problems and solutions]. *Biblioteka*, 2011, no. 1, pp. 32–35.

4. Boikova O. Zashchita personal'nykh dannykh [Personal data protection]. *Nezavisimyi bibliotechnyi advokat*, 2012, no. 1, pp. 34–46.

5. Smol'ianinov V. Iu. Analiz uslovii predostavleniia i polucheniia prav dostupa v modeli upravleniia dostupom MS SQL Server [Analysis of granting and getting access rights in the access control model MS SQL Server]. *Prikladnaia diskretnaia matematika,* 2014, no. 2, pp. 48–78.

6. Medvedev N. V., Grishin G. A. Modeli upravleniia dostupom v raspredelennykh informatsionnykh sistemakh [Access control models in distributed information systems]. Nauka i obrazovanie, 2011, no. 01, pp. 1–19. Available at: http://technomag.bmstu.ru/doc/164245.html (accessed: 02.06.2016).

The article submitted to the editors 11.07.2016

INFORMATION ABOUT THE AUTHORS

Koynov Roman Sergeevich – Russia, 654007, Novokuznetsk; Siberian State Industrial University; Senior Lecturer of the Department of Automation and Information Systems; koynov_rs@mail.ru.

Dobrynin Alexey Sergeevich – Russia, 654007, Novokuznetsk; Siberian State Industrial University; Senior Lecturer of the Department of Automation and Information Systems; serpentfly@mail.ru.