УДК 004.056, 332.871.3

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ УПРАВЛЕНИЯ МНОГОКВАРТИРНЫМИ ДОМАМИ С ИСПОЛЬЗОВАНИЕМ ОБЛАЧНЫХ ИНФОРМАЦИОННЫХ СЕРВИСОВ

Попов А.А.

ФГБОУ ВПО «Российский экономический университет им. Г.В. Плеханова», Москва, e-mail: a1710p@mail.ru

Статья посвящена формированию модели политики информационной безопасности для управления многоквартирными домами с помощью облачных информационных услуг. Были проанализированы проблемы отображения общедоступной информации о деятельности организаций для управления многоквартирными домами. Некоторые сведения, относящиеся к персональным данным и коммерческой тайне, должны быть защищены от несанкционированного доступа. Определены нормативные документы для формирования политики информационной безопасности. Рассмотрено содержание трех уровней политики информационной безопасности. Сформулированы требования к соглашению об уровне услуг (SLA) для организации безопасного информационного обмена между организацией по управлению многоквартирными домами и провайдером облачных сервисов.

Ключевые слова: персональные данные, коммерческая тайна, многоквартирный дом, политика информационной безопасности, информационная система, провайдер, абонент облачного информационного сервиса

DEVELOPMENT OF INFORMATION SECURITY POLICY FOR MANAGEMENT OF APARTMENT BUILDINGS WITH THE USE OF CLOUD INFORMATION SERVICES

Popov A.A.

Plekhanov Russian University of Economics, Moscow, e-mail: a1710p@mail.ru

This article deals with the formation of a model of information security policy for the management of apartment buildings with cloud information services. Were analyzed display issues of publicly available information on the activities of organizations for management of apartment buildings. Some information relating to personal data and commercial secrets must be protected from unauthorized access. Were identified normative documents for the formation of an information security policy. Was considered the content of the three levels of information security policy. Were formulated requirements for Service Level Agreement (SLA) for secure data exchange between the organization for managing apartment buildings and provider of cloud information services.

Keywords: personal information, commercial secret, apartment building, information security policy, information system, provider, the subscriber of cloud information service

Жильцы многоквартирных домов (МКД) используют одну из форм управления МКД, предусмотренную в Жилищном кодексе. Чаще всего для управления МКД выбирается управляющая компания (организация). Управление МКД управляющей компанией (организацией) имеет следующие характерные особенности:

1. Контроль большого объема данных по всем квартирам и собственникам жилья.
2. Выполнение роли посредника при оплате коммунальных услуг между жильцами и непосредственными поставщиками тех или иных услуг.
3. Контроль оплаты расходов.
4. Контроля заявок жильцов на осуществление того или иного вида работ и отслеживание хода их выполнения.
5. Контроля оплаты услуг, не входящих в сумму квартплаты.
6. Контроля расходов в рамках сметы, одобренной жильцами, а также сведений о собранных суммах и о наличии задолженностей.
7. Ведение бухгалтерского учета.

Таким образом, управляющие компании накапливают, обрабатывают, сохраняют и передают информацию в различных формах (электронной, физической, устной) со сведениями о жильцах, а именно: ФИО, адрес проживания, год, месяц и дата рождения, количество проживающих в квартире, семейное, финансовое и социальное положение жильцов, профессия, образование и доходы, другая информация. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» вся вышеупомянутая информация может быть отнесена к персональным данным. Обработка персональных данных в управляющих организациях, как правило, автоматизирована. Поэтому информация, обрабатываемая в организации по управлению МКД, может быть подвержена как преднамеренным, так и случайным угрозам, при этом процессы управления МКД, информационные системы, вычислительные сети, персонал организаций по управлению МКД, жильцы МКД имеют уязвимости. Изменения бизнес-процессов

и систем или другие внешние изменения (такие как новые законы и регламенты) могут создать новые риски для информационной безопасности. Учитывая множество способов, которыми угрозы, используя уязвимости, могут нанести вред организации по управлению МКД, можно сделать вывод, что риски информационной безопасности всегда присутствуют. Грамотно организованная защита информации уменьшает эти риски, страхуя организацию по управлению МКД от угроз и уязвимостей.

Проблемы отображения в открытом доступе информации о деятельности организаций по управлению многоквартирными домами

В Федеральном законе от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [8] определяется информация, относящаяся к коммерческой тайне. В соответствии с Постановлением Правительства РФ от 23 сентября 2010 г. № 731 «Об утверждении стандарта раскрытия информации организациями, осуществляющими деятельность в сфере управления многоквартирными домами» большая часть сведений управляющей компании (ТСЖ) должна быть раскрыта для всеобщего ознакомления в Интернете либо в бумажном виде. Постановление предусматривает, что к информации может обращаться широкий круг лиц, причем, независимо от цели её получения.

Также следует отметить, что с 1 марта 2013 года вступило в действие Постановление Правительства РФ от 28 декабря 2012 г. № 1468. Данное Постановление предусматривает разработку электронных паспортов МКД и жилых домов. В соответствие с данным документом должны быть сформированы электронные паспорта МКД и жилых домов. Часть раскрываемой информации из электронных паспортов (например, размер оплаты за поставленные ресурсы, состояние расчетов с ресурсоснабжающими организациями и т.д.) относится к экономической деятельности организации по управлению МКД. Также в электронных паспортах следует раскрывать сведения о собственниках жилья, а также информацию, непосредственно характеризующую техническое состояние и сведения об инженерной инфраструктуре и конструкции МКД.

Сопоставляя требования приведенных выше нормативных документов, можно сделать вывод, что отображение части информации о деятельности организации по управлению многоквартирными домами в открытом доступе будет производиться с нарушением требований законов №152-ФЗ и №98-ФЗ.

В современных условиях автоматизации ЖКХ могут возникнуть различные проблемы информационной безопасности (сохранность данных, перехват данных злоумышленником, несанкционированный доступ к данным, блокировка доступа к данным). Для того чтобы устранить проблемы информационной безопасности персональных данных жильцов многоквартирных домов, а также информации о деятельности управляющей организации, относящейся к коммерческой тайне, необходимо разработать политику информационной безопасности. При этом политика должна учитывать особенности использования современных информационных систем для управления многоквартирными домами.

Использование облачных информационных сервисов для управления многоквартирными домами

В настоящее время разработано большое количество информационных систем и сервисов для управления ЖКХ и многоквартирными домами [4, 5, 7], которые можно отнести к пяти классам (в соответствии с уровнем готовности организации по управлению многоквартирными домами к информатизации) [4, 7]. В соответствии с [7] четвертый класс информационных систем использует для управления МКД облачные технологии, позволяющие включить собственников жилья в контур управления МКД. Данный класс позволяет в реальном времени отслеживать состояние заявок, оплачивать счета за коммунальные услуги (что уже было реализовано в третьем классе информационных систем [7]), вызывать работников домовых служб (слесарей, сантехников и т.д.). Использование облачных вычислений в сфере управления недвижимостью уже несколько лет практикуется за рубежом. В России же на данный момент времени большинство существующих информационных систем в сфере ЖКХ не используют облачные технологии и обеспечивают включение в контур управления многоквартирными домами, главным образом, технических сотрудников.

Ведется активная разработка государственной информационной системы ЖКХ (ее следует, скорее всего, отнести к информационным системам четвертого класса), которая позволит создать единое информационное пространство ЖКХ. Вследствие этого многие организации по управлению многоквартирными домами будут «вынуждены» либо отказаться от уже эксплуатируемых информационных систем, либо интегрировать используемые информационные

системы в единое информационное пространство.

В случае использования облачных вычислений в управлении многоквартирными домами сразу возникает ряд факторов, обуславливающих проблемы информационной безопасности [6]. Также возникает дополнительная особенность использования облачных информационных сервисов – появление нового действующего лица (провайдера) в контуре управления многоквартирными домами. Поэтому могут возникать следующие дополнительные проблемы:

1. Стоимость подключения к облачным информационным сервисам не соответствует возможностям организации по управлению многоквартирными домами.

2. Нежелание абонентов облачных информационных сервисов (сотрудников организаций по управлению многоквартирными домами и жильцов) устанавливать клиентскую часть программного обеспечения для подключения к облачным сервисам на своих вычислительных устройствах.

3. Недостаточная степень защиты информации, предоставляемой абонентами, в облачных информационных сервисах.

4. Недостаточное доверие абонентов к облачным информационным сервисам. Об этом явлении говорят результаты опроса различных организаций в США. По результатам опроса 2014 года в США лишь 5% опрошенных организаций широко используют облачные информационные сервисы, 55% использует их ограниченно, 23% – в исключительных случаях, 13% – не использует вообще [2]. У возможных абонентов облачных информационных сервисов вызывают вопросы прозрачности, конфиденциальности и контроля. Абонентам облачных информационных сервисов часто не хватает информации о том, как защищаются и обрабатываются перемещаемые в облако данные, и что произойдёт в случае, если они захотят перейти к другому провайдеру или если их провайдер прекратит свою деятельность либо изменит положения своей политики [3].

Формирование политики информационной безопасности при использовании облачных информационных сервисов для управления многоквартирными домами

Политика информационной безопасности организации по управлению многоквартирными домами представляет собой совокупность документов, в которых определены принципы, правила, процедуры и практические приёмы в области информационной безопасности, которые способствуют защите персональных данных и данных, относящихся к коммерческой тайне. Политики информационной безопасности, разрабатываемые для случаев использования информационных систем первого, второго и третьего классов [5, 7] для управления многоквартирными домами, не смогут устранить проблемы использования информационных систем четвертого класса [6].

Основными документами для составления руководящих документов для создания политики информационной безопасности при управлении многоквартирными домами являются российские и иностранные стандарты:

1. Стандарт СТ РК ИСО/МЭК 17799-2006, а также его усовершенствованные варианты ISO/IEC 27002:2005 (ГОСТ Р ИСО/МЭК 27002-2012) и ISO/IEC 27002:2013. В данных стандартах определяются общие положения политики информационной безопасности.

2. Стандарт ISO/IEC 27017:2015 [29] регламентирует управление информационной безопасностью и защиту данных в случае использования облачных технологий и при этом использует положения стандарта ISO/IEC 27002. Планировалось, что данный стандарт будет выпущен вместе со стандартом ISO/IEC 27018, в котором рассматриваются вопросы защиты персональных данных при использовании облачных вычислений.

3. Стандарт ISO/IEC 27018:2014 [1]. Стандарт ISO/IEC 27018 содержит рекомендации для провайдеров облачных информационных сервисов, обрабатывающих персональные данные и предлагает ряд мер контроля и управления, которые провайдерам следует реализовать для смягчения проблем облачных вычислений. Поэтому стандарт предназначен для укрепления доверия к провайдерам облачных информационных сервисов (он содержит рекомендации по защите персональных данных и неприкосновенности частной жизни в публичном облаке).

Организация по управлению МКД может устанавливать свои требования по информационной безопасности. Источником для таких требований являются:

• оценка рисков для организации по управлению МКБ с учетом ее бизнес-стратегии и целей (выявляются угрозы обрабатываемой информации, определяются уязвимости и вероятности их использования, оценивается потенциальное воздействие)

• законодательные, нормативные и контрактные требования, которые организация по управлению МКД и взаимодействующие с ней организации должны выполнить,

а также социокультурная среда, в которой они действуют;

• набор принципов, целей и бизнес-требований, которые организация разработала для управления, обработки, хранения, передачи и архивирования информации.

Политика безопасности организации по управлению МКД составляется после проведения аудита системы внутренними силами организации или при помощи сторонних компаний. На основе «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК от 06.05.2015 и «Методики определения угроз безопасности информации в информационных системах» ФСТЭК от 08.05.2015 [9] составляется модель угроз и модель злоумышленника.

Для составления модели нарушителя используют Методику [9], с помощью которой определяются тип злоумышленника, зависящий от прав доступа, вид злоумышленника, потенциал злоумышленника, способы реализации несанкционированных действий. Модель злоумышленника для организаций по управлению МКД будет зависеть от ее размеров, территориальному расположению обслуживаемых домов, от оборота компании, от используемых программ для обработки информации, от метода сбора и обработки информации и от доступности информации.

При разработке политики информационной безопасности организации по управлению МКД следует выделить три уровня: высший, средний и нижний. Высший уровень политики информационной безопасности предназначен:

• для формулирования руководством организации по управлению МКД отношения к вопросам информационной безопасности и отражения области действия политики информационной безопасности;

• для разработки политик информационной безопасности для более низких уровней, а также правил и инструкций, регулирующих отдельные вопросы информационной безопасности в организации по управлению МКД;

• для использования в качестве средства информирования персонала организации по управлению МКД, жильцов, представителей сторонних организаций об основных задачах и приоритетах в сфере информационной безопасности.

Средний уровень политики информационной безопасности включает в себя отношение организации по управлению МКД (ее руководства) к определенным аспектам функционирования информационной системы (облачных информационных сервисов, реализующих управление МКД):

• перечень информационных потоков, обслуживающих различные бизнес-процессы по управлению МКД, требования к ним (степень важности, конфиденциальности информационных потоков, а также требования к надежности);

• требования к информационным и телекоммуникационным технологиям, методы обработки информации, используемые для управления МКД;

• требования к сотрудникам организации и пользователям облачного информационного сервиса, участвующих в процессах обработки информации по управлению МКД.

На нижнем уровне политика информационной безопасности организации по управлению МКД в соответствии с ISO/IEC 27002:2013 должна раскрываться в политиках по соответствующим направлениям, которые могут реализовываться по следующим целевым областям:

• контроль доступа к данным;

• классификация информации, обрабатываемой в организации по управлению МКД;

• физическая защита и защита от природных факторов;

• целевые области, ориентированные на абонентов, использующих облачные информационные сервисы (надлежащее использование данных, принцип «чистого» стола и «чистого» экрана, передача информации, работа с мобильными устройствами и удаленная работа, ограничения на установку и использование программных приложений);

• резервное копирование;

• передача информации;

• защита от вредоносного кода и управление техническими уязвимостями;

• криптографические методы и безопасность обмена информацией;

• конфиденциальность и защита персональных данных;

• отношения с поставщиками.

Все политики должны быть доведены до сведения сотрудников организации по управлению МКД, жильцов и соответствующих внешних сторон в адекватной, доступной и понятной форме.

Жизненный цикл политики информационной безопасности организации по управлению МКД состоит из ряда основных шагов:

1. Анализ состояния информационной безопасности.

2. Непосредственная разработка политики информационной безопасности.

3. Реализация в деятельности организации разработанных политик безопасности.

4. Анализ соблюдения требований разработанной политики информационной безопасности и формирование направлений ее дальнейшего совершенствования (переход на шаг №1).

Такой цикл может повторяться несколько раз с целью совершенствования политики информационной безопасности и устранения выявляемых проблем в информационной безопасности. Политику информационной безопасности следует анализировать через запланированные промежутки времени или в случае возникновения значительных проблем в информационной безопасности.

Как уже упоминалось выше, использование облачных информационных сервисов добавляет в управление МКД нового участника – провайдера. Поэтому политика информационной безопасности должна быть дополнена соглашением об уровне услуг (Service Level Agreement, SLA) между организацией по управлению МКД и провайдером. В соглашении должны быть указаны следующие вопросы организации безопасной передачи данных между организацией по управлению МКД и провайдером облачного информационного сервиса:

1. Безопасность данных, находящихся на хранении у поставщика облачных сервисов (провайдер обязан шифровать все непубличные, персональные и конфиденциальные данные в процессе их передачи из управляющей организации в облако и из него в течение всего срока действия договора и 90 дней после его прекращения). Для хранения и обработки информации должны использоваться методы и технологии, которые должны свести в минимуму возможность попадания данных в «чужие руки». Абоненты облачных информационных сервисов должны знать, что происходит с их данными (где именно они хранятся и как перемещаются между различными ресурсами).

2. В соответствии со стандартом, клиенты будут защищены от использования их данных в рекламных целях. ISO 27018 требует, чтобы абоненты знали о доступе к их информации на основе законных запросов (если закон не запрещает такое информирование). Также абоненты должны знать о случаях неавторизованного доступа к их информации, потери данных и прочих происшествиях.

3. Данные, передаваемые организацией по управлению МКД провайдеру, должны (в том числе, и в соответствии с изменениями в ФЗ №152 «О персональных данных») храниться на территории РФ. Под это требование подпадают также данные резервного копирования. Организация по управлению МКД вправе запросить конкретное местоположение сервера, на котором будет храниться, а также обрабатываться информация.

4. Защита данных при передаче от организации провайдеру и обратно (данные всегда должны быть зашифрованы, при этом используются проверенные временем протоколы и алгоритмы шифрования, проходят проверку целостности, проверку подлинности и аутентификацию).

5. Подтверждение подлинности клиента (использование токенов и сертификатов, а также стандартов LDAP и SAML для аутентификации абонентов информационных сервисов).

6. Разделение доступа к приложениям между абонентами (использование виртуальных машин и виртуальной сети, основанных на стандартных методах VLAN, VPLS, VPN).

7. Нормативно-правовые стороны взаимодействия (ограничение экспорта данных, особые меры безопасности, аудит информационной безопасности, предоставления доступа к данным сторонних организаций только по запросу).

8. Реакция провайдера на инциденты при эксплуатации облачного сервиса (должен быть разработан и задокументирован соответствующий регламент).

Выводы

1. В случае использования облачных информационных сервисов для управления многоквартирными домами увеличиваются риски несанкционированного доступа к информации, являющейся персональными данными или относящейся к коммерческой тайне.

2. Разработан подход к формированию трехуровневой политики информационной безопасности. При этом вследствие отставания разработки стандартов по информационной безопасности облачных информационных сервисов, для разработки политики информационной безопасности требуется применять требования иностранных стандартов.

3. В дополнение к политике информационной безопасности должно быть разработано соглашение об уровне услуг (Service Level Agreement, SLA) между организацией по управлению МКД и провайдером информационного сервиса. Приводятся требования к содержанию такого соглашения.

Список литературы

1. Колесов А. Microsoft внедряет стандарт ISO 27018 по защите персональных данных. URL: http://www.pcweek.ru/security/article/detail.php?ID=171137 (дата обращения: 22.01.2016).

2. Новости проекта InterPARES Trust. URL: http://rusrim.blogspot.ru/2015/02/interpares-trust_23.html (дата обращения: 23.01.2016).

3. Обзор международного стандарта требований к поставщикам облачных услуг, обрабатывающим персональные данные. URL: http://rusrim.blogspot.co.uk/2015/02/blog-post_1.html (дата обращения: 23.01.2016).

4. Попов А.А. Возможные проблемы управления жкх региона при использовании перспективного единого информационного пространства, сформированного на основе концепции интернета вещей // Вестник научных конференций. – 2015. – №2-5(2). – С.111-114.

5. Попов А.А. Определение направлений, форм и способов перспективного развития инновационной инфраструктуры организаций по управлению многоквартирными домами (товариществ собственников жилья). – М.: Издательство «Ирисбук», 2012. – 213 с.

6. Попов А.А. Проблемы повышения информационной безопасности облачных информационных сервисов при формировании инновационной ИТ-инфраструктуры организации по управлению многоквартирными домами // Современные проблемы науки и образования. – 2013. – № 3; URL: http://www.science-education.ru/ru/article/view?id=9267 (дата обращения: 23.01.2016).

7. Попов А.А. Разработка облачного информационного сервиса для функционирования инновационной ИТ-инфраструктуры организации по управлению многоквартирными домами // Известия Российского экономического университета им. Г.В. Плеханова. – 2013. – №4(14). – С.92-163; URL: http://old.rea.ru/Main.aspx?page=Nomer_4__14_ (дата обращения: 23.01.2016).

8. Федеральный закон от 29 июля 2004 года № 98-ФЗ (ред. от 12.03.2014) «О коммерческой тайне».

9. ФСТЭК России. Методика определения угроз безопасности информации в информационных системах. Проект. Сайт. – URL: http://fstec.ru/component/attachments/download/812 (дата обращения: 23.01.16).

10. ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757 (дата обращения: 23.01.2016).