

**ЗАЩИТА ИНФОРМАЦИИ  
В ГОСУДАРСТВЕННОЙ  
ИНФОРМАЦИОННОЙ СИСТЕМЕ  
ЖИЛИЩНО-КОММУНАЛЬНОГО  
ХОЗЯЙСТВА**

Титов В.А., Замараева О.А., Кузин Д.О.

*ФГБОУ ВПО «Российский экономический  
университет им. Г.В. Плеханова», Москва,  
e-mail: vtitov213@yandex.ru, feya\_fena@mail.ru,  
kuzindmitri@list.ru*

В последнее время в Российской Федерации проводится внедрение информационных систем в различные подразделения государственных и исполнительных органов власти, при этом большое значение уделяется защите информации. В Государственной Думе Российской Федерации был разработан и в настоящее время проходит утверждение закон «О государственной информационной системе жилищно-коммунального хозяйства (ГИС ЖКХ)». С принятием закона правительство получит механизм связи с населением по жилищно-коммунальным вопросам. ГИС ЖКХ сможет облегчить работу с информацией как работникам государственных органов, так и гражданам.

Для обеспечения защиты информации, прежде всего, необходимо определить виды информационных потоков, которые будут храниться

в такой системе: сбор, обработка и хранение информации об объектах жилищного фонда; предоставление коммунальных услуг; ремонт многоквартирных домов; социальные льготы при оплате коммунальных услуг. Таким образом, единая ИС должна обеспечить все информационно-аналитическое обеспечение для управления ЖКХ и прогнозирования его развития.

Далее следует выделить группы пользователей, которые будут применять эту информацию: государственные органы; индивидуальные предприниматели; граждане.

В соответствии с законопроектом информация, содержащаяся в государственной информационной системе жилищно-коммунального хозяйства, подлежит защите в соответствии с законодательством Российской Федерации. Для организации соответствующего уровня защиты информации в системе необходима разработка политики информационной безопасности предприятия, а также составление четких инструкций для руководителей и сотрудников. Поскольку в настоящее время вопросы обеспечения безопасности информации в ЖКХ мало изучены, предлагается на начальном этапе построения защиты определить с наибольшей точностью приоритетную для защиты информацию и, так называемую, модель злоумышленника.