Содержание

Введение

Администрацией города Хабаровска (Далее – Оператор) в лице Управления Приватизации жилья и Жилищного фонда информационная система персональных данных «Приватизация» определило как муниципальную информационную систему (далее – МИС) «Приватизация» согласно Федерального закона от 27.07.2006 N 152-ФЗ, Постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. , приказа ФСТЭК России от 11 февраля 2013 г. N 17.

Одной из центральных проблем разработки и функционирования МИС в любом государственном учреждении является обеспечение безопасности хранения, обработки и передачи информации. Особенно это касается персональных данных субъектов персональных данных, не являющихся сотрудниками, которые обращаются в такие учреждения и работают в них.

Особым образом стоит проблема обеспечения безопасности информации в учреждениях, работающих в сфере жилищного фонда и приватизации жилья. В таких учреждениях необходимо, в первую очередь, обеспечить безопасность персональные данных граждан, обращающихся в такие учреждения, а также персональные данные работников.

Таким образом, целью работы является проектирование профиля системы защиты информации в сегменте администрации г. Хабаровска. Вместе с тем необходимо, чтобы спроектированная система защиты информации соответствовала требованиям действующего законодательства Российской Федерации.

Система защиты информации (далее – СЗИ) представляет собой совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, а также неправомерных действий с ними. Только оптимальное сочетание

организационных, технических и программных мероприятий, а также постоянное внимание и контроль над поддержанием системы защиты в актуальном состоянии позволит с наибольшей эффективностью обеспечить решение постоянной задачи.

Организационные и технические меры по защиты информации, реализуемые в муниципальной информационной системе в рамках ее системы защиты информации, в зависимости от видов и самих угроз безопасности информации, используемых технологий и структурно-функциональных характеристик муниципальной информационной системы должны обеспечивать:

– идентификацию и аутентификацию субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защиту машинных носителей информации;

– регистрацию событий безопасности;

– антивирусную защиту;

– обнаружение (предотвращение) вторжений;

– контроль (анализ) защищенности информации;

– целостность информационной системы и информации;

– доступность информации;

– защиту среды виртуализации;

– защиту технических средств;

– защиту информационной системы, ее средств, систем связи и передачи данных.

Состав мер защиты информации приведены к настоящим требованиям:

– меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого

субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности);

– меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности, установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил;

– меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения;

– меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации;

– меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них;

– меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;

– меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия;

– меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации;

– меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации;

– меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы;

– меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации,

терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям;

– меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей;

– меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

Разработка профиля системы защиты информации в сегменте муниципальной информационной системы администрации города Хабаровска является актуальной задачей в связи с большим объемом обрабатывающихся данных в информационной системе и новым законодательством.

Разработка и реализация организационных и технических мер для создания условий обеспечения безопасности персональных данных, при их обработке в муниципальной информационной системе персональных данных, должны быть в соответствии с требованиями действующих руководящих документов.

Места расположения:

– 680000, г. Хабаровск, ул. Карла Маркса, 66-13 АРМ;

– 680000, г. Хабаровск, ул. Краснореченская, д. 87- 4 АРМ;

– 680000, г. Хабаровск, пер. Ленинградский, д. 13а-3 АРМ;

– 680000, г. Хабаровск, ул. Фрунзе, д. 60, 50-9 АРМ;

– 680000, г. Хабаровск, ул. Руднева, д. 43-4 АРМ.

Назначение объектов – работа с информацией, содержащей персональные данные.

В целях сбора сведений об управлении, выявления вероятных угроз безопасности ПДн, а также определения исходной степени защищенности было проведено обследование данного управления.

Обследование проводилось в соответствии с руководящими документами и законами.

В ходе обследования определялись:

– состав и структура объектов защиты управления;

– конфигурация и структура;

– перечень лиц, участвующих в обработке;

– права доступа лиц, допущенных к обработке;

– существующие меры защиты;

– угрозы безопасности персональных данных управления;

– оценивалась вероятность их реализации, реализуемость, опасность и актуальность.

управления средствами защиты информации из состава СЗПДн и управление серверами, входящими в состав сети с доменной структурой администрации города Хабаровска. Так же администратор предоставляет права доступа к информации, разграничивает права доступа к информации и ресурсам в МИС. Задает порядок изменения паролей пользователей в МИС и в домене.

Перед установкой нового программного обеспечения в МИС администратор безопасности должен провести его антивирусную проверку, а также совместимость работы в терминальном режиме.

Администратор безопасности должен проводить:

– контроль за выполнением требований действующих нормативных и руководящих нормативных и руководящих документов по защите персональных данных, при проведении работ на ПК;

– работу с учетными записями пользователей МИС, их настройка и разграничение прав доступа пользователей к защищенным ресурсам МИС;

– периодическое тестирование и проверку функций СЗПДн при изменении настроек и программной среды в МИС, имитирую попытки НСД;

– регламентированное тестирование реализации политики безопасности: процесса идентификации и аутентификации учетных записей пользователей и администраторов, в том числе администратора СрЗИ, процесса выполнения контроля целостности;

– проверку серверного оборудования, включая сервер терминалов и виртуальные сервера на нем.

Заключение

В ходи разработки дипломного проекта было проведено обследование, анализ состояния информационной безопасности в сегменте муниципальной информационной системы управления приватизации жилья и жилищного фонда администрации города Хабаровска, в соответствии с действующими нормативно-правовыми документами.

В результате обследования на начальном этапе дипломного проектирования были определены существующие программно-технические средства и организационные меры защиты информации. На основе обрабатываемых данных в муниципальной информационной системе и принятых мер по информационной безопасности был определен исходный уровень защищенности муниципальной информационной системы, выявлены актуальные угрозы и сделан анализ вероятности возникновения угроз и определения их опасности. В конце начального этапа было сформулировано аналитическое обоснование необходимости приведения МИС в соответствие с требования нормативно-методических документов.

На следующем этапе дипломного проектирования было разработано техническое задание, которое включает все современные требования к будущей муниципальной информационной системе. Предложено внедрить в действующую сетевую структуру терминальный режим работы для пользователей МИС на основе виртуального сервера терминалов и удаленных рабочих столов. Данная система повысит уровень безопасности и обслуживание парка компьютерной техники. Была предложена структура будущей системы МИС, оценены примерные финансовые затраты на создание данного профиля защиты информации.

Проектирование профиля системы защиты завершилось разработкой технического проекта, включающего описание схемы построения профиля и

системы в МИС, технических средств защиты информации, организационных мер и порядок ввода в эксплуатацию.

На заключительном этапе дипломного проектирования были произведены подсчеты затрат на создания профиля системы защиты, организованы требования к организации рабочих мест при работе с ПК и рассчитана искусственное освещение рабочих мест.

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

Список используемой литературы:

1. http://www.vkaznu.ru – [Электронный ресурс] – Бухгалтерский учет в бюджетных учреждения

2. http://www.grandars.ru – [Электронный ресурс] – Энциклопедия экономиста

3. http://geum.ru – [Электронный ресурс] – Электронное хранилище знаний

4. http://geliomaster.com – [Электронный ресурс] – Светодиодные светильники

5. Рунге В.Ф., Манусевич Ю.П. Эргономика в дизайне среды М.: Архитектура-С, 2005. – 327 с

6. Российская газета http://www.rg.ru

7. http://garant.ru – [Электронный ресурс] –Законодательство РФ

8. Ардован, А. М. Оценка стоимости: учебное пособие/ А. М. Ардован, С. А. Оккель. – Хабаровск.: 2010

9. Валдайцев, В.С. Оценка бизнеса и управление предприятием [Текст]: /В.С. Валдайцев// Оценка бизнеса: учеб. – 3-е изд., перераб. и доп. – М.: ТК Велби, Изд-во Проспект, 2010. – 576 с.

10. Есипов, В.Е. Оценка бизнеса : учеб. пособие [Текст] / В. Е. Есипов, Г.А. Маховикова, В.В. Терехова. – 2-е изд. – СПб. : Питер, 2010. – 464 с.

11. Федотова, М. Оценка бизнеса / под ред. А.Г. Грязновой, М.А. Федотовой. М.: Финансы и статистика, 2014. 736 с.

12. http://www.profiocenka.ru. - [Электронный ресурс] - Портал для специалистов в области оценки

13. http://www.pandia.ru/text/77/201/63253.php . - [Электронный ресурс] – энциклопедия знаний. Подходы к определению стоимости предприятия.

14. Официальный сайт ФСТЭК России [Электронный ресурс]: офиц. сайт – Режим доступа: http://www.fstec.ru/

15. Официальный сайт ФСБ РФ [Электронный ресурс]: офиц. сайт – Режим доступа: http://clsz.fsb.ru.

16. Яскевич, Е.Е. Особенности применения затратного и доходного подходов при оценке рыночной стоимости машин и оборудования [Текст]/ Е.Е. Яскевич // Имущественные отношения в РФ. – 2005. - №10. – С. 89-91.

17. Информационный портал о безопасности [Электронный ресурс]: электрон. информац. ресурс– Режим доступа: http://www.securitylab.ru/

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT