Ф.И. Егоров
Региональный представитель
государственного предприятия «Украинские специальные системы»
Государственной службы специальной связи и защиты информации
Украины в городе Севастополе и Автономной Республике Крым

О ТЕХНИЧЕСКИХ И ТЕХНОЛОГИЧЕСКИХ ОСОБЕННОСТЯХ ЗАЩИТЫ ИНФОРМАЦИИ В СФЕРЕ МЕСТНОГО ЭЛЕКТРОННОГО ПРАВЛЕНИЯ

Разработка со-интегральной системы местного электронного правления вызывает вполне законный интерес к реализации требований защиты информации об абонентах обратной связи и предметной области решаемых задач местного самоуправления ее электронным инструментарием.

Соответственно, требования защиты данных распространяются на сферу:

1. По предметной области обратной связи - в соответствии с формуляром диалоговой информационной системы (ДИС) «Ноосфера»:

- по обращениям за местными административными услугами;
- управлению бюджетной политикой административных единиц;
- поддержке градостроительного кадастра и генерального плана развития;
- контролю проектов застройки и эксплуатации земельных участков,
- учету доходов и расходов целевых средств на развитие территории,
- ведению кадастров потребления ресурсов и паспортизации их циклов;
- другим прикладным аспектам общественных отношений.

2. По абонентам обратной связи – в соответствии с концепцией обеспечения защиты информации от несанкционированного доступа диалоговым программным комплексом «с открытым кодом» ДИС «Ноосфера»:

- головного узла обратной связи Главы государства;
- узлов обратной связи органов государственной власти;
- узлов обратной связи органов местного самоуправления;
- узлов обратной связи неправительственных организаций;
- порталов сайтов предприятий финансовой сферы;
- порталов справочных и поисковых систем;

- информационно-коммуникационных центров (ИКЦ) внутри протокола связи «ДИС «Ноосфера» для нечеткого множества электронных офисов домашних и/или товарных хозяйств участников обратной связи в лице собственников земельных участков (застройщиков в лице граждан и их объединений, коммунальных и государственных учреждений) ;
- компьютерных систем вне протокола связи «ДИС «Ноосфера» для нечеткого множества участников обратной связи в лице граждан и их объединений.

Управление функциями пользования и процессов обработки и обмена данными концентрируется в головном автоматизированном рабочем месте (АРМ) «Гражданский щит Украины» как «местной отрасли гражданского общества», интегрированной в электронное правительство.

Контроль организации защиты информации реализовывался в период создания Программы «Гражданский Щит» на базе пилотного АРМ (99000) «Гражданский Щит города Севастополя» как прототипа головного АРМ «Гражданский Щит Украины» и АРМов административно-территориальных единиц (АТЕ) в его иерархии. В том числе контроль обеспечивался путем:

- лицензирования разработчика Администрацией Государственной службы специальной связи и защиты информации Украины;
- проведения разработчиком установленных ДБН (ГОСТ) и нормами испытаний ДИС «Ноосфера» в предварительном и приемочном режиме;
- указания целевых функций технических и технологических компонентов системы местного электронного правления как предмета их защиты.

Изначально данное требование было реализовано в цели Программы «Гражданский Щит» с раскрытием предмета системы информационно-аналитического обеспечения (СИАО) как целевой функции поддержки:

- организации эффективного и самодостаточного функционирования АТЕ,
- развития административной территории и производственных отношений АТЕ как частей социально-экономического и ландшафтно-экологического базиса национальных реформ и государственного строительства.

Данный подход позволил определить структуру управления и связи:

1) АРМ председателя органа местного самоуправления;

2) АРМы государственных и хозяйственных субъектов рыночной экономики;

3) компьютерная система «Информационно-аналитический центр развития города Севастополя» как ядро СИАО:

а) комплекс стандартных аппаратно-программных средств с КСЗИ;

б) ДИС «Ноосфера» (под КСЗИ от НСД) **со шлюзами портала**:

- **для открытого доступа** из Internet к информационным ресурсам с различной политикой безопасности из незащищенной среды с персональной защитой заказанных (обрабатываемых) данных;
- **для защищенной обратной связи** (по глобальным и локальным сетям).

4) коммутаторы распределенной информационно-аналитической базы СИАО:

а) учреждения центральных и отраслевых органов власти;

б) органы власти местного самоуправления;

в) территориально-хозяйственные комплексы (ТХК);

5) информационно-коммуникационные системы взаимодействия с СИАО:

а) **для неконтролируемых** проектом глобальных сетей (типа Internet) - **защищенные порталы** территориальной размещенной платформы **ДИС «Ноосфера»** в административных единицах;

б) **для контролируемых** проектом глобальных сетей - **защищенный информационный ресурс** национальной системы конфиденциальной связи (НСКС) Государственной службы специальной связи и защиты информации (ГСССЗИ).

Требования работы с разной политикой безопасности регламентированы:

- современной правовой основой защиты информации при обязательности «открытости» государственных и публичных учреждений для населения;
- повышенными требованиями к защите «открытой» информации, принадлежащей государству и/или имеющей статус конфиденциальности;
- обязательностью защиты персональных данных физических лиц, которые, в соответствии с Конституцией Украины, можно собирать «только о себе» с запретом несанкционированного сбора данных о «третьих лицах».

В соответствии со структурой необходимых требований осуществление защиты информации «с открытым доступом» с условием защиты выдаваемых данных организовано по критерию гарантий на уровне Г-2:

- информационный ресурс НСКС до стандартного профиля 3.КЦД.2 = {КА-2, КВ-2, ЦА-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}
- внешний портал ДИС «Ноосфера» не ниже стандартного профиля 3.КЦД.2 = {КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

Данные технические и технологические особенности защиты информации:

- исключают противоречивость ответственности НСКС за передачу защищенным информационным ресурсом незащищенной при обработке информации от угроз ее модификации;
- реализуют Поручение Президента Украины «Об обеспечении внедрения информационно-коммуникационных технологий во всех сферах общественной жизни, реализации в Украине Инициативы «Партнерство« Открытое Правительство» по развитию электронного управления».

Перечень использованной литературы:

1. Прималенный А.А., Егоров Ф.И. Об организации допуска и доступа к информации различных категорий конфиденциальности в АРМ «Гражданский Щит» как автоматизированной системы класса «3» // - Днепропетровск: Научный журнал «Экология и ноосферология», том 19. - 2008. - №№ 3-4. - С. 161-171.

2. Прималенный А.А. Развитие электронного правления в Автономной Республике Крым как зеркало демократии //Досвід впровадження е-демократії та е-урядування в Україні. - К.: Національний центр підтримки електронного урядування, 2010. - С. 66-68.

4. Прималенный А. А. Со-интегральная система местного электронного правления Украины (шифр - «Гражданский Щит») / - Днепропетровск: научный журнал «Экология и ноосферология», Том 23. - 2012. - №№ 1-2. - С. 127 - 139.