G.B. Grigoriev[1], A.N. Vavichkin[2]

[1]AO «NEOLANT», str. Pokrovka 47 A, Moscow, 105062, Russia,
e-mail: ggrigorievrt@gmail.com, ORCID iD 0000-0003-4037-426
[2]National Research Nuclear University MEPHI, Kashirskoe sh., 31, Moscow,
115409, Russia, e-mail: vava70@list.ru, ORCID iD 0000-0001-9755-2167

Safety of the State Information System «Regional Geographic Information System of Territorial Planning of the Republic of Sakha (Yakutia)»

Keywords: state information system, system of protection of personal data, personal data, information security, model of threats and violator.

Information and telecommunication technologies are widely applied by public authorities for improvement of quality of rendering services to the population. According to the legislation of the Russian Federation, the plan of transition to providing the state services and execution of the state functions in electronic form by federal public authorities is approved. The state information systems are created taking into account the requirements provided by the Federal law of July 21, 2005 No. 94-FZ «About placing orders for the supply of goods, works and services for state and municipal needs». The state information systems are created and operated on the basis of the statistical and other documentary information provided by citizens (natural persons), the organizations, public authorities, local governments. In the Federal Law No. 149 need of information security for GIS according to which the owner of information is established of 27.07.06 or the operator of IS is obliged to provide information security from unauthorized access, blocking, destruction, distribution, copying or other actions by means of use of a package of measures for respect for safety of information and restriction of access to public information.

Г.Б. Григорьев[1], А.Н. Вавичкин[2]

[1]АО «НЕОЛАНТ», ул. Покровка, д. 47А, Москва, 105062, Россия,
e-mail: ggrigorievrt@gmail.com, ORCIDiD 0000-0003-4037-426
[2]Национальный исследовательский ядерный университет «МИФИ», Каширское ш, 31,
Москва, 115409, Россия, e-mail: vava70@list.ru, ORCIDiD 0000-0001-9755-2167

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «РЕГИОНАЛЬНАЯ ГЕОИНФОРМАЦИОННАЯ СИСТЕМА ТЕРРИТОРИАЛЬНОГО ПЛАНИРОВАНИЯ РЕСПУБЛИКИ САХА (ЯКУТИЯ)»

Ключевые слова: государственная информационная система, система защиты персональных данных, персональные данные, защита информации, модель угроз и нарушителя.

Информационные и телекоммуникационные технологии широко применяются органами государственной власти в целях повышения качества оказания услуг населению. В соответствии с законодательством РФ утвержден план перехода на предоставление государственных услуг и исполнение государственных функций в электронном виде федеральными органами государственной власти. Государственные информационные системы создаются с учетом требований, предусмотренных Федеральным законом от 21 июля 2005 года № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд». Государственные

информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления. В ФЗ № 149 от 27.07.06 установлена необходимость защиты информации в Государственных информационных системах (ГИС), согласно которой владелец информации или оператор информационной системы (ИС) обязан обеспечить защиту информации от несанкционированного доступа, блокирования, уничтожения, распространения, копирования или других действий с помощью использования комплекса мер по соблюдению сохранности информации и ограничения доступа к общедоступной информации.

Введение

В настоящий момент проблематика защиты информации в ГИС подразумевает наличие разрозненных организационных и нормативно-методических документов. Нет четкой структурированности российского законодательства в области защиты ГИС, к примеру, не все операторы понимают необходимость применения документа утвержденного ФСТЭК России 11 февраля 2014 года «Меры защиты информации в государственных информационных системах» как обязательного к использованию для защиты информации в ГИС. Нормативный документ «Меры защиты информации в государственных информационных системах» содержит указания операторам к усилению режима защиты в существующих ГИС, а также руководство к обеспечению мер защиты информации в ГИС для вновь создаваемых ГИС.

В задачу работы входит систематизация требований регуляторов к защите информации в ГИС (в частности, подготовка единого комплексного документа, регламентирующего меры защиты для каждого класса защищённости ГИС).

Методический документ «Меры защиты информации в государственных информационных системах» предназначен для обладателей информации, заказчиков, операторов информационных систем, лиц, обрабатывающих информацию, являющуюся государственным информационным ресурсом, а также лиц, привлекаемых в соответствии с законодательством Российской Федерации к проведению работ по созданию государственных информационных систем, детализирует организационные и технические меры защиты информации, принимаемые в государственных информационных в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17, а также определяет содержание мер защиты информации и правила их реализации. Документ является дополнением для приказа ФСТЭК России от 11 февраля 2013 г. № 17. Меры защиты информации распределяются на 13 подсистем, определяющих режим комплексной защиты информации в ГИС. Для каждой группы мер приводится детализированное описание и указываются классы ГИС, в которых требуется применение меры.

Однако документ включает в себя относительно сложную структуру и труден к применению операторами, не имеющими в штате технических специалистов с опытом работы по предметной области «защита информации в ГИС» или аналогичной. В связи с этим актуальной является разработка комплексного методического документа, позволяющего наглядно и точно определить набор мер к применению для каждого конкретного класса ГИС.

Подобный документ должен содержать себе переработку таблицы, представленной в приложении № 2 методического документа «Меры защиты информации в государственных информационных системах». Переработанная таблица должна содержать

не только идентификацию меры по условному обозначению и её название, но и описание, представленное в правой части таблицы в виде ссылок на подпункты мер. Такой документ будет обладать следующими преимуществами:

наглядностью содержания меры защиты для каждого класса;

структурированностью мер защиты (на каждый подпункт меры приходится новая строка с описанием подпункта);

шаблонностью документа и возможностью его использования в качестве опросника для проведения обследования ГИС или контрольной карты выполнения мер при проведении аттестационных испытаний.

Такой документ позволил бы, в частности, обосновать заказчику применение той или иной меры защиты в соответствии с требованиями законодательства. К примеру, для демонстрации меры защиты идентификация и аутентификация 1 (ИАФ.1) с использованием приложения, требуется выполнение базовой меры ИАФ.1 приказа № 17, а также пп. 1а, 2а, 3 методического документа «Меры защиты информации в государственных информационных системах». Соответственно, в переработанном документе заказчику демонстрируются не абстрактные пункты меры ИАФ.1, а содержание, при котором:

1) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов): а) с использованием сети связи общего пользования, в том числе сети Интернет;

2) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей): а) с использованием сети связи общего пользования, в том числе сети Интернет;

3) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов);

В результате проведенной работы разработан документ «Модель угроз и нарушителя безопасности ГИС», включающий в себя описание угроз ГИС и вероятного нарушителя режима обеспечения информационной безопасности ГИС.

Модель нарушителя безопасности информации, обрабатываемой в ГИС, предназначена для определения перечня возможных нарушителей, анализа их возможностей, классификации возможных нарушителей в соответствии с руководящими документами ФСТЭК России.

Модель угроз и нарушителя с обоснованием актуальных угроз безопасности ГИС является основой для определения мер защиты информации ГИС (с учетом требований композитного документа «Меры защиты информации ГИС», описанного выше). На основе композитного документа и результатов моделирования угроз, также производится разработка частного технического задания на систему защиты информации ГИС, содержащую описание мер защиты и применения требуемых средств защиты информации ГИС.

Нарушители делятся на две категории:

1) нарушители, которые не имеют легального доступа в ГИС и действуют из-за пределов контролируемой зоны (КЗ);

2) нарушители, у которых имеются легальные права доступа в ГИС угрозы реализуются непосредственно в пределах КЗ.

В данной модели нарушителя предполагается что, что нарушитель может воздействовать на ГИС на любом этапе её существования: от проектирования до вывода из

эксплуатации. В результате определен перечень из 28 актуальных угроз безопасности информации, который можно применить к любой ГИС. Самые распространенные угрозы:

1) злоупотребление правами доступа. Внедрение вредоносных программ администратором безопасности ГИС.

Администратор безопасности ГИС имеет неограниченный доступ к защищаемой информации и имеет возможность скрытия своих действий;

2) восстановление защищаемой информации путем анализа выведенных из эксплуатации для ремонта или утилизации носителей информации.

Передаваемые для ремонта или утилизации носители информации не должны содержать защищаемую информацию;

3) угрозы сканирования, направленные на выявление используемых протоколов, доступных портов и сервисов, версий программного обеспечения (ПО), выявление установленных, но не используемых сетевых служб, с целью определения уязвимых мест ГИС.

Данная угроза не нарушает характеристик безопасности защищаемой информации;

4) угроза выявления аутентифицирующей информации пользователей ГИС.

Получение атрибутов доступа к элементам ГИС или инфраструктуры; реализация других видов угроз при условии получения атрибутов доступа;

5) анализ сетевого трафика с целью извлечения защищаемой информации.

Получение защищаемой информации, предаваемой по каналам связи без использования средств криптографической защиты информации (СКЗИ);

6) угрозы типа «отказ в обслуживании».

Реализация угрозы производится на активном сетевом оборудовании;

7) Проведение сетевых атак на гипервизор.

Разделение сети. Сеть управления, сеть доступа, служебная сеть. Применение средств обнаружения вторжений;

8) угрозы внедрения по сети вредоносных программ;

реализация угрозы может быть преднамеренной или случайной;

9) угрозы удаленного запуска приложений.

Доступность специализированного ПО упрощает реализацию данной угрозы.

В результате моделирования и с учётом выявленных требований композитного документа «Меры защиты информации ГИС» был произведен выбор средств защиты информации, актуальных организационно-технических и организационных мер защиты.

Заключение

Разработанные документы апробированы на практике при проведении аттестационных испытаний ГИС, а также при разработке ГИС «с нуля». Так, использование контрольных карт мер защиты информации позволило продемонстрировать заказчику обоснованный выбор подсистем защиты информации и необходимых средств защиты информации исходя их требуемых мер защиты. Представленный композитный документ по выполнению каждого требования адаптированного набора мер защиты для конкретной ГИС позволил в кратчайшие сроки сформировать исходный комплект документов для проведения аттестационных испытаний, включающих корректировку существующих мер защиты. Специалистам заказчика была продемонстрирована недостаточность имеющихся мер и осуществлена поддержка в устранении замечаний. Результатом работы на практике явилась выдача положительного заключения аттестационной

комиссии и, как следствие, аттестата соответствия ГИС требованиям по информационной безопасности. Практическая значимость представляется в виде разработанного комплекса шаблонов документов, которые после адаптации, можно применить для защиты информации в любой ГИС.

СПИСОК ЛИТЕРАТУРЫ:

1. Приказ ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
2. Методический документ ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».
3. Руководящий документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный 15.02.2008.
4. Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный 14.02.2008.
5. Курносов К.В. Обеспечение безопасности виртуальной инфраструктуры в государственных информационных системах (ГИС) / В сборнике: Информационно-телекоммуникационные системы и технологии. Материалы Всероссийской научно-практической конференции. 2014. С. 92–93.
6. Громыко И.А., Оспищев Е.Я., Кильмаев С.Ю. Будущее за упреждающими системами защиты // Вопросы защиты информации. 2007. № 2. С.11–14.
7. Шивдяков Л.А. Проблемы обеспечения информационной безопасности в ключевых системах информационной инфраструктуры органов государственного управления. Модель угроз информационной безопасности информации в КСИИ // Безопасность информационных технологий. 2009. № 2. С. 108–116.
8. Съемщиков Д.Л. Обеспечение информационной безопасности государственных информационных систем // В сборнике: Наследие нобелевских лауреатов по экономике. Сборник статей III Всероссийской научно-практической конференции молодых ученых. 2016. С. 216–218.

REFERENCES:

1. Prikaz FSTEK Rossii № 17 ot 11 fevralya 2013 g. «Ob utverzhdenii trebovaniy o zaschite informatsii, ne sostavlyayuschey gosudarstvennuyu taynu, soderzhascheysya v gosudarstvennyih informatsionnyih sistemah».
2. Metodicheskiy dokument FSTEK Rossii ot 11 fevralya 2014 g. «Meryi zaschityi informatsii v gosudarstvennyih informatsionnyih sistemah».
3. Rukovodyaschiy dokument FSTEK Rossii «Bazovaya model ugroz bezopasnosti personalnyih dannyih pri ih obrabotke v informatsionnyih sistemah personalnyih dannyih», utverzhdennyiy 15.02.2008.
4. Rukovodyaschiy dokument FSTEK Rossii «Metodika opredeleniya aktualnyih ugroz bezopasnosti personalnyih dannyih pri ih obrabotke v informatsionnyih sistemah personalnyih dannyih», utverzhdennyiy 14.02.2008.
5. Kurnosov K.V. Obespechenie bezopasnosti virtualnoy infrastrukturyi v gosudarstvennyih informatsionnyih sistemah (GIS) / V sbornike: Informatsionno-telekommunikatsionnyie sistemyi i tehnologii. Materialyi Vserossiyskoy nauchno-prakticheskoy konferentsii. 2014. S. 92–93;
6. Gromyiko I.A., Ospischev E.Ya., Kilmaev S.Yu. Buduschee za uprezhdayuschimi sistemami zaschityi // Voprosyi zaschity iinformatsii. 2007. № 2. S. 11–14.
7. Shivdyakov L.A. Problemyi obespecheniya informatsionnoy bezopasnosti v klyuchevyih sistemah informatsionnoy infrastrukturyi organov gosudarstvennogo upravleniya. Model ugroz informatsionnoy bezopasnosti informatsii v KSII // Bezopasnost informatsionnyih tehnologiy. 2009. № 2. S. 108–116.
8. S'emschikov D.L. Obespechenie informatsionnoy bezopasnosti gosudarstvennyih informatsionnyih sistem / V sbornike: Nasledie nobelevskih laureatov po ekonomike. Sbornik statey III Vserossiyskoy nauchno-prakticheskoy konferentsii molodyih uchenyih. 2016. S. 216–218.