**УДК 004.056.53, 004.056.52**

# ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ К ВЗЛОМУ ИНФОРМАЦИОННЫХ СИСТЕМ РАЗГРАНИЧЕНИЯ ДОСТУПА К ДАННЫМ НА ОСНОВЕ ГЕОПРОСТРАНСТВЕННОГО ПОЛОЖЕНИЯ ПОЛЬЗОВАТЕЛЯ

**Хусаинова Р. Ф., Максимов В. И.**

*ГОУ ВПО «Московский государственный университет геодезии и картографии (МИИГАиК)», Москва, Россия (105064, Москва, Гороховский пер., 4)*

**Проведен анализ особенностей «технологии разграничения доступа к данным на основе геопространственных характеристик пользователя» на предмет выявления перечня потенциальных угроз информационной безопасности информационных систем, работающих на базе указанной технологии. Выявлен перечень уязвимостей информационной безопасности указанных информационных систем, через которые возможна реализация угроз. Произведена оценка критичности выявленных угроз, описаны возможные сценарии осуществления атак с использованием обнаруженных уязвимостей. Сформированы технологические решения и рекомендации по ликвидации угроз и предотвращения потенциальных атак. Указанные решения опираются на специфику целевых информационных систем, в частности, предложены оригинальные частные решения применения координатной информации пользователей в методах шифрования сетевого трафика, проверки подлинности компонентов программного обеспечения и алгоритмах идентификации, аутентификации и авторизации.**

Ключевые слова: разграничение доступа, геопространственные характеристики, координаты, конфиденциальность и целостность данных, модели разграничения, авторизация, аутентификация, шифрование.

# ENSURING THE STABILITY TO CRACKING OF INFORMATION SYSTEMS OF DATA ACCESS CONTROL ON THE BASIS OF USER'S LOCATION

**Khusainova R. F., Maksimov V. I.**

*Moscow State University of Geodesy and Cartography, Moscow, Russia (105064, Moscow, Gorohovsky lane, 4)*

**The analysis of the special features of the "Technology of data access control on the basis of the user's geospatial position" for detection of information security potential threats of information systems' that operate according to this technology is conducted. The list of information security vulnerabilities of target information systems, through which the threats realization is possible, is formed. The estimation of the identified threats' criticality is produced; the possible scenarios of attacks using detected vulnerabilities are described. Technological solutions and recommendations for the threats elimination and potential attacks prevention are formed. Stated solutions rely on the objective target information systems specificity, particularly innovative special solutions of the application of the users' coordinate information in the network traffic encryption methods, software elements verification and identification, authentication and authorization algorithms.**

Keywords: access control, geospatial characteristics, location, data confidentiality and integrity, delimitation models, authorization, authentication, encryption.

## Введение

Увеличение рыночного сегмента мобильных и компьютерных устройств, снабженных модулями приема и обработки сигналов глобальных навигационных спутниковых систем (ГНСС), далее именуемые «целевыми устройствами», увеличение рыночного спроса на них открывает перспективы для разработки новых технологий, в том числе и по направлению «информационная безопасность». Авторами была предложена концепция[1] разграничения

[1] Впервые концепция публично освещена на 67-й «Научно-технической конференции студентов, аспирантов и молодых ученых МИИГАиК» (2012 г.) в докладе Хусаиновой Рены Фаридовны «Пространственное позиционирование в качестве средства разграничения доступа к информации».

доступа к данным на основе геопространственного положения пользовательского устройства (далее «геопространственные характеристики пользователя», «координатные данные»). Концепция предполагает разработку информационных систем хранения и защиты данных, в которых доступ к защищаемым данным предоставляется только в том случае, если субъект доступа находится в одной из зон геопространства, сопоставленной с запрашиваемым объектом доступа (далее «разрешающая зона»). На основе концепции авторами проводится разработка технологии разграничения доступа к данным на основе геопространственного положения пользователей (далее «целевая технология»). Технология предполагает разработку инструментальных программных средств (далее «ИС-геоРД» или «целевые системы»), осуществляющих хранение и защиту данных, а также предоставляющих избирательный доступ к этим данным на основе настраиваемых политик доступа, в зависимости от координат субъектов, запрашивающих данные.

В процессе разработки целевой технологии была поставлена задача обеспечения устойчивости целевых систем к взлому с целью предотвращения несанкционированного доступа к защищаемым посредством технологии данным. Под «взломом» в работе понимается осуществление злонамеренного субъективного (антропогенного) воздействия на целевые системы, приводящее к реализации угроз их информационной безопасности. Для разрешения проблемы защиты от взлома поставлены задачи:

- провести анализ целевой технологии с целью выявления и оценки потенциальных угроз информационной безопасности информационных систем класса ИС-геоРД;
- выявить уязвимости, через которые возможна реализация потенциальных угроз, оценить их критичность;
- сформировать технологические решения по устранению выявленных уязвимостей.

Потенциальные угрозы информационной безопасности «систем разграничения доступа к данным на основе геопространственных характеристик пользователя»

При проведении анализа целевой технологии на предмет выявления потенциальных угроз информационной безопасности особое внимание уделено рассмотрению преднамеренных *субъективных внешних угроз*, так как решения по защите от объективных и *внутренних* субъективных угроз не представляют особой специфики – они идентичны угрозам безопасности всего класса «информационные системы».

Целевые ИС функционируют по принципу «клиент-сервер», предполагают централизованное, удаленное хранение данных, доступ к которым осуществляется

посредством обращения к серверному модулю ИС-геоРД с мобильных устройств пользователей посредством клиентских программных модулей (рис. 1):

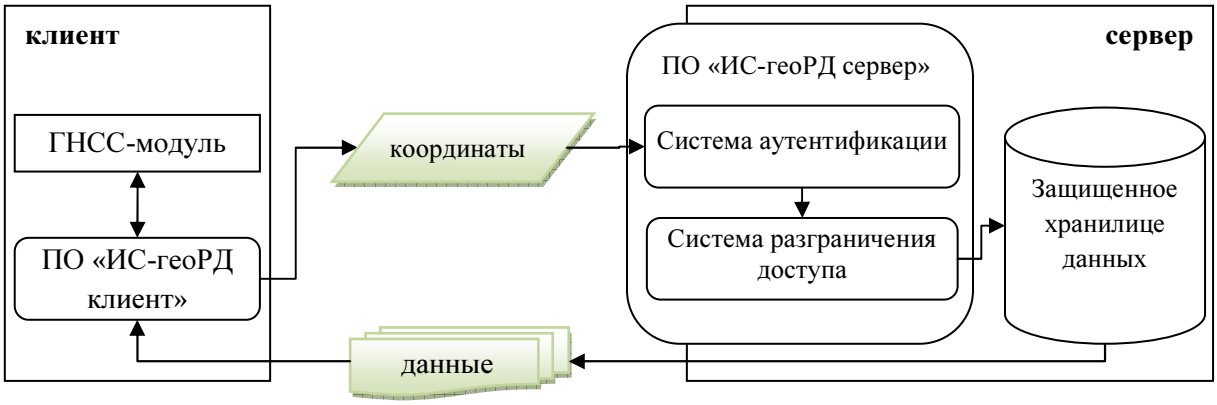


Рис.1. Обобщенная схема функционирования информационных систем разграничения доступа на основе геопространственного положения пользователей

По результатам анализа архитектуры целевых систем с учетом их функционала (хранение и предоставление доступа к данным), а также специфики работы с данными (удаленное хранение и передача), выявлен ряд субъективных внешних угроз:

- угроза нарушения конфиденциальности информации (а именно несанкционированный доступ к защищаемым данным, Т 1 – здесь и далее код угрозы, Т – от англ. threat, угроза);
- угрозы нарушения целостности информации, включая:
  - искажение хранимых на серверной стороне данных (Т 2);
  - подмена передаваемых клиенту данных на участке сервер-клиент (Т 3);
- угроза нарушения доступности (угроза отказа удаленного сервиса, Т 4).

Потенциальные уязвимости «информационных систем разграничения доступа к данным на основе геопространственных характеристик пользователя»

Для выявления уязвимостей составлена функциональная схема взаимодействия основных компонентов целевых систем. На схеме (рис. 2) отмечены участки, потенциально имеющие уязвимости, через которые возможна реализация атак, с целью осуществления каждой из угроз (участки обозначены узлами с нумерацией римскими цифрами, коды уязвимостей далее – через латинскую «V» – от англ. vulnerability).

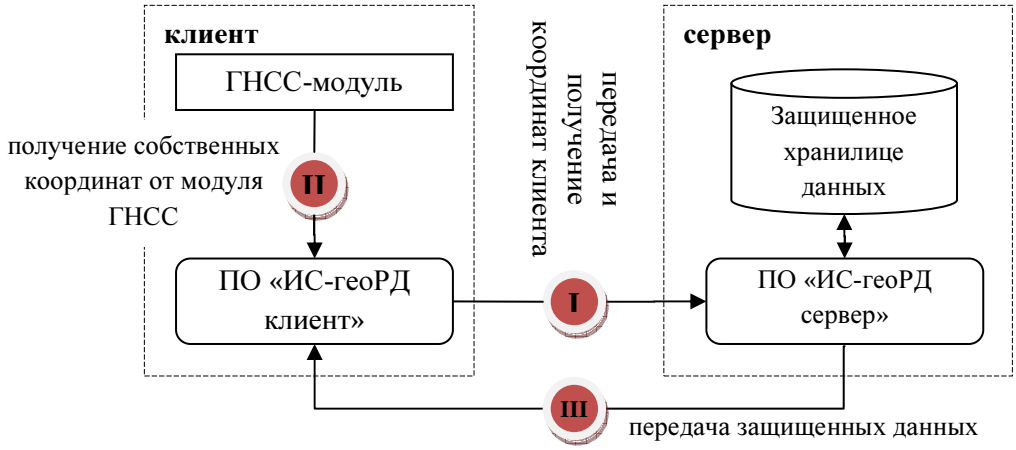


Рис. 2. Уязвимости целевых информационных систем

Через уязвимость V1 возможна атака подменой координат клиента (A1, здесь и далее – код атаки). Атакующий, находящийся вне «разрешающей зоны», может осуществить попытку перехвата сообщения от клиентского ПО и подменить истинные координаты на координаты одной из «разрешающей зон». Второй вариант атаки (A2) – фальсификация сообщения клиентского ПО (то есть осуществление запроса к серверной стороне без использования ПО «ИС-геоРД клиент», с эмуляцией формата и протокола его взаимодействия с серверной стороной). В случае успешно осуществленной атаки злоумышленник может получить права доступа, позволяющие осуществить чтение защищаемых данных (тем самым нарушив принцип конфиденциальности), или изменить защищаемые данные на серверной стороне (нарушая их целостность). Процесс авторизации через подмену истинных координат назовем «компрометацией разрешающей зоны». Так же, в случае несанкционированного делегирования прав злоумышленником может быть проведена атака типа «отказ в обслуживании» (As1, от англ. secondary attack, вторичная атака) путем осуществления множественных параллельных запросов значительных объемов данных, что может повлечь за собой перегрузку и нарушение работоспособности серверной стороны, что нарушает принцип доступности данных.

Через уязвимость V2 возможна подмена собственных координат пользовательского устройства, получаемых клиентским ПО системы разграничения доступа от встроенного модуля ГНСС (атака A3). В таком случае атакующий может попытаться фальсифицировать передаваемые от ГНСС модуля координатные данные и, как и в случае атак A1 и A2, заменить их на координаты одной из «разрешающих зон». Указанная атака аналогично атакам A1 и A2 ставит под угрозу конфиденциальность и целостность защищаемых данных.

Через уязвимость V3 возможен перехват третьей стороной передаваемых авторизованному клиенту данных, подлежащих защите (атака A4). Перехват может быть осуществлен

различными способами, зависящими от используемой транспортной среды передачи данных. В случае простого перехвата передаваемых данных произойдет нарушение конфиденциальности данных, в случае перехвата с подменой (искажением) – нарушение конфиденциальности и целостности.

При подведении итогов анализа потенциальных угроз информационной безопасности целевых систем произведена оценка критичности выявленных уязвимостей. Уязвимостям присвоены оценки по трехбалльной шкале (оценка «3» – высокая критичность, «2» – средняя, «1» – низкая). В качестве основного критерия, определяющего степень критичности, использован показатель объема данных, для которых нарушается конфиденциальность, целостность или доступность при реализации соответствующих угроз через соответствующие уязвимости (таб. 1):

Таблица 1

Оценка критичности уязвимостей информационной безопасности целевых систем

| Уязвимости | Атаки | Реализуемые угрозы | Критичность уязвимостей |
|---|---|---|---|
| V1 | A1 | T1, T2 | 3 |
| | A2 | T1, T2 | |
| | As1 | T4 | |
| V2 | A3 | T1, T2 | 2 |
| V3 | A4 | T1, T3 | 1 |

Устранение потенциальных уязвимостей «систем разграничения доступа к данным на основе геопространственного положения пользователя»

Как было указано выше, атаки A1 и A2 производятся путем фальсификации запроса клиентского ПО целевых систем, при этом в рамках A1 происходит искажение сообщения (запроса) клиентского ПО (с подменой координат), в рамках A2 – самостоятельное формирование всего сообщения третьими инструментальными средствами, без использования клиентского ПО. Для ликвидации такой возможности предложено двухступенчатое решение, предусматривающее:

- контроль подлинности клиентского ПО;
- защиту сетевого трафика между клиентским и серверным ПО целевых систем.

Под контролем подлинности подразумевается: во-первых, проверка самого факта использования клиентского ПО (с целью исключения атаки A2), во-вторых, проверка целостности последнего, то есть отсутствия изменений программного кода, произведенных злоумышленником. Данная задача может быть решена с помощью подписания программных компонентов клиентского ПО электронной цифровой подписью, с возможностью ее проверки на серверной стороне. Защита сетевого трафика подразумевает передачу

служебных запросов между клиентским и серверным ПО через шифруемое сетевое соединение, например, с использованием протокола SSL (англ. Secure Sockets Layer – «уровень защищённых сокетов»).

Как отмечалось выше, проведение атаки As1 возможно лишь при условии предварительного выполнения атаки A1 или A2, соответственно с введением методов защиты от последних, возможность проведения первой исключается. Функциональная схема решения по защите от проведения атак A1, A2, As1 и ликвидации уязвимости V1 приведена на схеме (рис.3):

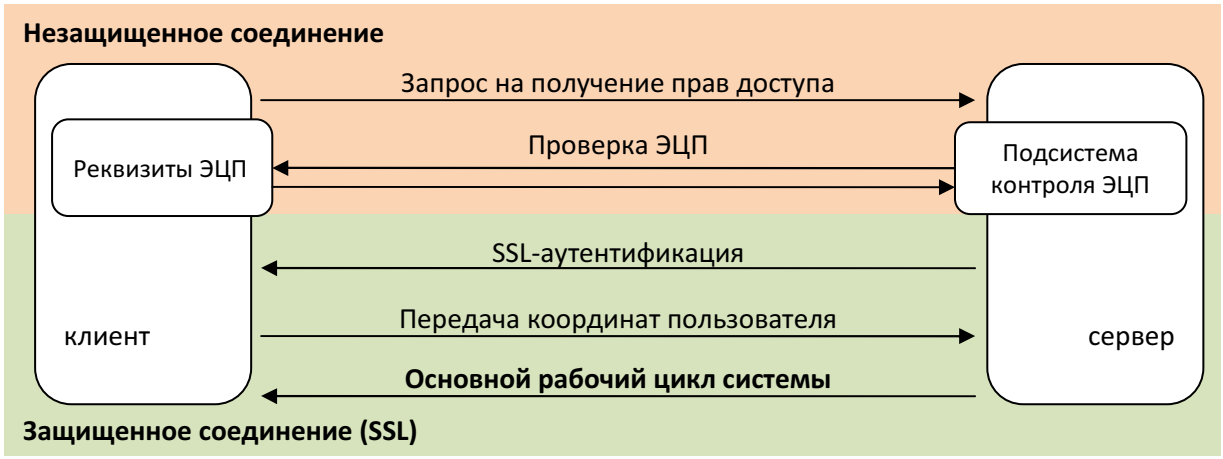


Рис. 3. Функциональная схема технического решения ликвидации уязвимости V1

Согласно описанию атаки A3, выполняющейся через уязвимость V2, злоумышленник может провести подмену собственных координат на этапе передачи от встроенного модуля ГНСС к клиентскому ПО целевых систем. Реализация такой атаки сильно коррелирует с конечной аппаратно-программной платформой, на которой функционируют компоненты клиентского ПО. Для современных платформ целевых устройств, рассматриваемых в данной работе, существует два варианта взаимодействия со встроенными модулями ГНСС:

- через API операционной системы (англ., application programming interface - интерфейс программирования приложений) для семейств Android и iOS;
- путем обращения непосредственно к драйверу модуля для семейств Symbian и WindowsMobile.

Соответственно, в зависимости от особенностей платформы, злоумышленник может произвести подмену (модификацию) драйвера устройства (с целью управления и искажения его вывода) или осуществить модификацию программного кода компонентов операционной системы (с целью перехвата функций API). Для решения данной проблемы предложено использовать механизм так называемой «двухфакторной авторизации». Суть двухфакторной авторизации заключается в использовании нескольких независимых механизмов аутентификации, при этом один из них является главным, а второй – подтверждающим.

Подключение целевых устройств к сети Интернет осуществляется посредством услуг «мобильного доступа в сеть» на основе ряда технологий беспроводного доступа операторов сотовой связи (таких как GPRS, EDGE, CDMA), а также с помощью технологии WiFi. Операторы сотовой связи постоянно располагает достоверной информацией о местоположении своих пользователей с точностью разрешения не менее одной ячейки зоны покрытия (соты). Таким образом, возможна реализация целевой системы с использованием подтверждения положения пользователя от независимой стороны – поставщика услуги мобильного доступа в сеть интернет. Алгоритм взаимодействия клиентского и серверного ПО дополняется шагом – запросом от серверного компонента целевой системы к поставщику мобильного доступа в сеть, которым пользуется клиент. Необходимым условием предоставления прав доступа является совпадение координат, полученных от пользователя, и координат, полученных от поставщика мобильного доступа в сеть (с допуском на погрешности определения координат системами ГНСС и средствами операторов сотовой связи).

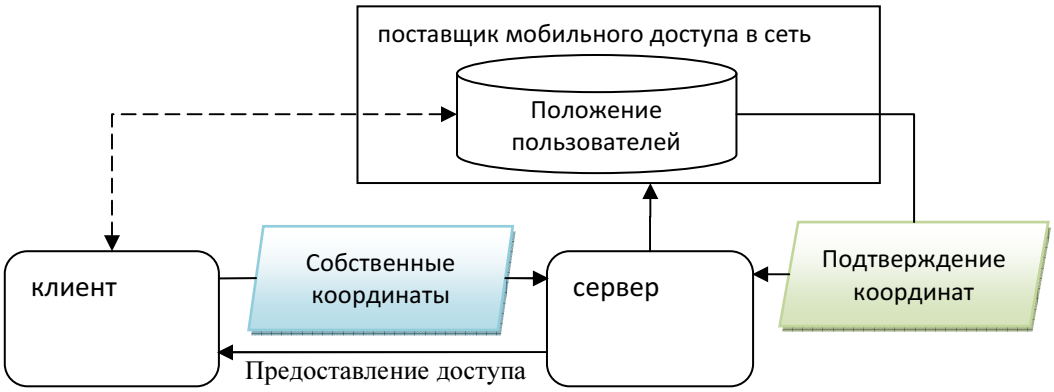


Рис. 4. Функциональная схема технического решения ликвидации уязвимости V2

Рассматривая потенциальный сценарий использования уязвимости V3 через осуществление атаки A4, следует отметить, что защищаемые данные могут быть перехвачены двумя способами – на уровне сетевого взаимодействия (путем «прослушивания» сетевого трафика между сервером и клиентом) и непосредственно на оборудовании клиента (как специализированными программами-анализаторами сетевого трафика, так и вирусным ПО). Решение, сформированное для ликвидации уязвимости V1 и предполагающее организацию защищенного сетевого соединения, автоматически закрывает уязвимость V3, так как в случае перехвата трафика злоумышленник получит зашифрованные данные. В связи с этим, а также с низкой критичностью рассматриваемой уязвимости (см. табл.1), специальное решение не предлагается. Однако стоит отметить, что потенциал целевой технологии позволяет осуществлять шифрование передаваемых данных на серверной стороне, с использованием координатной информации пользователя в качестве криптографического

ключа, с последующей ее дешифровкой на стороне клиента. Такой подход позволяет использовать произвольные алгоритмы шифрования требуемой стойкости и не ограничиваться алгоритмом шифрования, заложенным в избранную технологию организации защищенных сетевых соединений (например, SSL).

Выводы

Анализ особенностей технологии разграничения доступа на основе геопространственного положения пользователей позволил определить перечень угроз безопасности информационных систем, работающих под управлением указанной технологии. Выявлены потенциальные уязвимости указанных информационных систем, оценена их критичность. Сформирован ряд технологических решений, ликвидирующих данные уязвимости. В целом можно утверждать, что комплекс предложенных мер обеспечивает должную защиту целевых информационных систем от угроз, специфичных для данного класса информационных систем.

**Список литературы**

1. Бабенко Л. К., Макаревич О. Б., Журкин И. Г., Басан А. С. Защита данных геоинформационных систем. – М.: Гелиос АРВ, 2010. – 336 с.

2. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – 400 с.

3. Смит Р. Э. Аутентификация: от паролей до открытых ключей. – М.: Вильямс, 2002. – 432 с.

4. Семенов Ю. А. Протоколы и ресурсы Internet. – М.: Радио и связь, 1996. – 320 с.

5. Фергюсон Н., Шнайдер Б. Практическая криптография. – М.: Диалектика, 2004. – 432 с.

6. A Guide to Understanding Identification and Authentication in Trusted Systems. [Электронный ресурс]. URL: http://www.fas.org/irp/nsa/rainbow/tg017.htm (дата обращения: 15.06.2012).

**Рецензенты:**

Малинников Василий Александрович, д.т.н., профессор, первый проректор, проректор по УР, МИИГАиК, г. Москва.

Журкин Игорь Георгиевич, д.т.н., профессор, зав. кафедрой вычислительной техники и автоматизированной обработки аэрокосмической информации, МИИГАиК, г. Москва.