ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.93
DOI: 10.22213/2410-9304-2019-3-4-33-40

МЕТОД ЗАЩИТЫ ДОСТУПА К ИНФОРМАЦИОННОМУ РЕСУРСУ МОБИЛЬНОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ НА ОСНОВЕ НАВИГАЦИОННОГО КЛЮЧА

Т. З. Аралбаев, доктор технических наук, профессор, Оренбургский государственный университет, Оренбург, Россия
Р. Р. Галимов, кандидат технических наук, доцент, Оренбургский государственный университет, Оренбург, Россия
Е. В. Каменева, старший преподаватель, Оренбургский государственный университет, Оренбург, Россия
А. Ш. Идрисов, магистр, Оренбургский государственный университет, Оренбург, Россия
А. С. Солдатов, магистр, Оренбургский государственный университет, Оренбург, Россия

Актуальность темы определяется широким развитием и применением мобильных вычислительных средств, использующихся для хранения и обработки конфиденциальных информационных ресурсов. Данная работа посвящена вопросам защиты информационных ресурсов в бортовой системе транспортных средств от несанкционированного доступа. Выявлены недостатки существующих подходов защиты подобных систем вследствие широких возможностей злоумышленников вне контролируемых зон воздействия как на средства защиты, так и на пользователей системы. В связи с этим предложен подход защиты информационных ресурсов мобильных вычислительных средств, позволяющий получить доступ только в защищенных зонах. В статье разработана структурная модель многоуровневой системы защиты доступа к информационному ресурсу, включающая следующие уровни: физическую защиту, систему аутентификации, криптографическую и стеганографическую системы. Особенность данного метода заключается в том, что предлагается дополнить правила доступа к ресурсу данных подсистем контролем местоположения мобильного объекта информатизации. Это достигается за счет формирования ключей криптографической и стеганографической систем с учетом данных о географических координатах мобильного объекта. На основе данной модели разработано программное средство для защиты доступа к информационному ресурсу с учетом навигационного ключа, позволяющее повысить уровень защищенности мобильных объектов информатизации.

Ключевые слова: защита доступа к информационному ресурсу, навигационный ключ, стеганография, криптография, многоуровневая система защиты, мобильный объект информатизации.

Введение

Современный этап информатизации характеризуется стремительным ростом числа мобильных устройств, в связи с этим возникают специфические угрозы для объектов информатизации, связанные с их мобильностью, что приводит к размытию периметра защиты информационной системы [1]. Среди подобных угроз можно выделить такие угрозы, как нарушение доступности информации вследствие недостаточного заряда батарей и несанкционированного доступа к информации в результате кражи мобильных устройств [2, 3]. С точки зрения обеспечения конфиденциальности информации наиболее актуальной задачей является защита информационного ресурса (ИР) от несанкционированного доступа вне контролируемых зон. При этом злоумышленники часто обладают широкими возможностями для преодоления стандартных методов защиты информации. Кроме того, необходимо отметить, что большинство мобильных вычислительных устройств содержат следующие специализированные подсистемы: навигации, видео- и фотосъемки. Если подсистемы видео- и фотосъемки обычно используются в целях аутентификации, то подсистема навигации в данных целях применяется крайне редко [4]. В связи с этим существует необходимость в разработке методов и средств обеспечения конфиденциальности информации на мобильных объектах информатизации вне контролируемых зон.

Задачам разработки и исследования систем и способов защиты доступа к информации уделено большое внимание в современной литературе и сети Интернет. Среди работ по защите доступа на основе определения навигационного местоположения пользователей следует отметить следующие разработки. В частности, система и способ С. А. Васильева и В. В. Яблокова позволяет организовать защиту доступа к данным, сохраненным на мобильном устройстве, с помощью пароля, которым могут являться, по меньшей мере, географические координаты, последовательность изменений координат расположения мобильного устройства в пространстве,

голосовая команда, название Wi-Fi-сети или Bluetooth-устройства [5]. Способ и устройство авторов ЧА Инхиок, ШАХ Йоджендра К. и Е. Чуньсюань обеспечивает привязывание информации о местоположении и верификации метрик доверия внешнего объекта перед предоставлением доступа к информации о местоположении [6]. Система автоматической разблокировки мобильного устройства «Smart Lock» для операционных систем «Android» позволяет выбирать местоположение (например, дом или работу), в которых устройство будет автоматически снимать блокировку.

Несмотря на достоинства данных работ, необходимо отметить, что в них не учитывается погрешность получаемых навигационных данных, отсутствует непосредственный запрет доступа к информации и ее защита посредством стеганографических либо криптографических методов. В связи с этим существует необходимость в разработке метода защиты доступа к информационным ресурсам, позволяющего обеспечить возможность защиты информационных ресурсов от несанкционированного доступа (НСД) вне контролируемых зон на основе навигационного ключа.

Целью работы является снижение риска от несанкционированного доступа к информационному ресурсу на основе многоуровневой системы защиты, учитывающей местоположение мобильного объекта информатизации посредством навигационного ключа.

Для достижения поставленной цели необходимо решить следующие задачи:

– определить целевую функцию метода защиты доступа к информационному ресурсу на основе навигационного ключа;

– разработать структурную схему системы защиты доступа к информационному ресурсу на основе навигационного ключа;

– разработать алгоритм для программного средства защиты доступа к информационному ресурсу на основе навигационного ключа;

– разработать программное средство для защиты доступа к информационному ресурсу на основе навигационного ключа.

Целевая функция метода защиты доступа к информационному ресурсу на основе навигационного ключа определяется как минимизация риска R НСД к информационным ресурсам:

$$R = \sum_{i=0}^{n} P_i \cdot U_i, i = \overline{1,n}, R \to \min, \qquad (1)$$

где P – вероятность реализации атаки НСД; U – материальный ущерб в результате разовой атаки НСД; n – количество угроз несанкционированного доступа к информационному ресурсу.

Структурная схема системы защиты доступа на основе навигационного ключа

Разрабатываемый метод предполагает наличие на автомобильном транспортном средстве (АТС) бортовой информационной системы, которая хранит в своей памяти ИР. Под информационным ресурсом в данной работе понимается электронный документ, содержащий сведения конфиденциального характера. Навигационный ключ – это пароль, сформированный на основе географических координат местонахождения МОИ, необходимый для получения доступа к информационному ресурсу с защищаемой информацией. В качестве способа защиты информации от НСД в методе предлагается применение многоуровневой системы, включающей следующие уровни:

– физическая защита доступа к МОИ, реализованной в виде охранной системы;

– система разграничения доступа к бортовой информационной системе АТС, например, на базе парольной подсистемы аутентификации;

– криптографическая подсистема шифрования конфиденциальной информации;

– стеганографическая подсистема сокрытия зашифрованной информации.

В отличие от подобных решений эшелонированной защиты в данной работе предлагается дополнить правила доступа к ресурсу данных подсистем контролем местоположения МОИ. Фактически, ключи доступа к каждой подсистеме формируются на основе навигационного ключа и пароля соответствующего уровня.

Примерами физической защиты АТС являются металлические ключи, иммобилайзеры [7]. Для металлических ключей есть высокая степень риска изготовления дубликатов или преодоления при помощи слесарных инструментов. Недостатком применения иммобилайзера является использование общего ключа с охранной системой автомобиля, что определяет высокую вероятность возможности создания дубликата [8]. Последнее время набирает популярность, особенно для автомобилей премиум-класса, использование пассивных или удаленных бесконтактных систем доступа. Данные системы используют схему аутентификации типа запрос-ответ, при котором обмениваются случайным числом, зашифрованным ассиметричным алгоритмом. Актуальными угрозами для подобных систем защиты доступа являются атаки ретрансляции сигнала от бесконтактного ключа до АТС или попытка определить алгоритм фор-

мирования случайного числа (часто в роли случайного числа используются данные счетчика, увеличивающегося после каждого цикла аутентификации). Включение в состав запроса при аутентификации данных о местоположении автомобиля и водителя в одной зоне позволяет снизить вышеуказанные риски. При этом данные о координатах не передаются между охранной системой АТС и аппаратным ключом аутентификации, а независимо определяются при помощи своего навигационного оборудования и сравниваются в цикле подтверждения подлинности. Это позволяет проверить фактическое нахождение водителя вблизи АТС.

Применение стандартных решений для защиты от несанкционированного доступа к бортовой информационной системе (БИС) автомобильного транспортного средства на втором уровне, таких как парольный и двухфакторный методы аутентификации, имеет ряд недостатков: возможность перебора пароля, применение средств социальной инженерии для получения информации о пароле или PIN-коде [9]. Для предотвращения подобных атак в данной работе предлагается, чтобы ключ к системе состоял из двух частей: пароля пользователя и навигационных координат. Для повышения защищенности бортовой информационной системы необходимо, чтобы при аутентификации данные о местоположении определялись самой БИС или аппаратным ключом без участия человека.

Основной вид угроз – это физический перехват мобильного объекта во время остановки, стоянки или движения вне контролируемых зон. При этом атаки, направленные непосредственно на навигационную подсистему транспортного средства, являются труднореализуемыми и требуют значительного времени на исполнение. Нарушители делятся на два основных класса в зависимости от наличия информации об эталонном навигационном ключе: внутренние и внешние. При отсутствии информации о навигационном ключе сложность получения доступа к информационному ресурсу определяется временем, которое необходимо затратить нарушителю на перебор координат. Если же навигационный ключ известен нарушителю, то для получения доступа к информационному ресурсу последний может попытаться переместить АТС как можно ближе к контролируемой зоне, учитывая погрешность GPS/ГЛОНАСС-оборудования.

Задача защиты доступа к ИР заключается в предоставлении возможности считывания информации только в пределах контролируемых зон. На рис. 1 представлена структурная схема защиты доступа к информационному ресурсу, расположенному на АТС, и реализующая два нижних уровня защиты с использованием навигационного ключа.

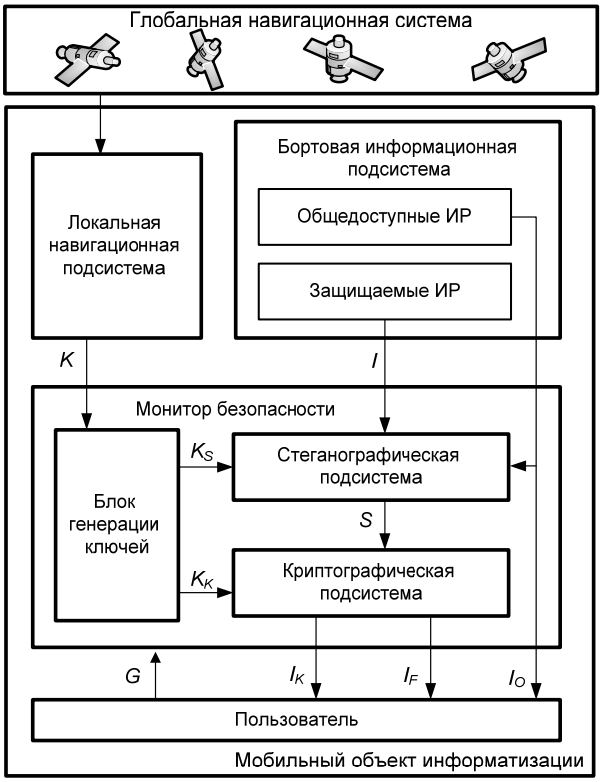

Рис. 1. Структурная схема системы защиты доступа к информационному ресурсу с использованием навигационного ключа: K_G – данные глобальной навигационной системы; K – географические координаты, рассчитанные GPS/ГЛОНАСС-модулем; K_S – ключ для стеганографической системы; K_K – ключ для криптографической системы; S – стеганографический контейнер с защищаемым ИР; I_K – зашифрованный ИР; I – защищаемый ИР; I_O – общедоступный ИР; I_F – отказ в доступе; G – запрос пользователя на получение доступа к ИР

Для уменьшения вероятности перебора ключей подсистем эшелонированной защиты к ним дополнительно добавляется навигационный ключ, определяющий область контролируемой зоны. Чтобы предотвратить возможность перехвата и извлечения навигационного ключа, используется операция хеширования. Так как данные о местоположении K МОИ определяются с погрешностью, то при формировании ключей используется его округленное значение $K_{\text{окр}}$. Обобщенная формула генерации ключей имеет следующий вид:

$$K_S = HASH\left(floor\left(K\right) + S_S\right), \qquad (2)$$

$$K_K = HASH\left(floor\left(K\right) + S_K\right), \qquad (3)$$

где S_S и S_K – это заданные пользователем ключи стеганографической и криптографической систем соответственно; *floor* – функция округления; *HASH* – функция хэширования; + – операция слияния ключей.

Параметры округления определяют диапазон действия навигационного ключа, который представляет собой множество географических координат, которые в результате округления совпадают с эталонным значением.

Выбор диапазона действия навигационного ключа во многом определяется размерами контролируемой зоны. Область действия навигационного ключа должна находиться внутри контролируемой зоны с учетом интервала погрешности определения местоположения мобильного объекта информатизации. В целях корректного задания диапазона действия навигационного ключа был проведен эксперимент по замеру координат в статическом состоянии антенны GPS-трекера в режиме теплого старта, длительностью в 30 минут [10]. В соответствии с данными проведенного эксперимента, погрешность координат в результате долговременного (продолжительного) эксперимента не превышает 2,5 метров и определяет минимальную величину контролируемой зоны l [11]. Схема диапазона действия навигационного ключа представлена на рис. 2.

Разработка программного средства защиты доступа на основе навигационного ключа

С учетом разработанной структурной схемы системы защиты доступа к ИР мобильного объекта разработан алгоритм программного средства защиты доступа на основе навигационного ключа, схема которого представлена на рис. 3. Данный алгоритм определяет функционирование в двух режимах:

– установка защиты на ИР;

– запрос доступа к информационному ресурсу.

При установке защиты на информационный ресурс выполняются следующие действия:

1) генерация ключей для стеганографического скрытия K_S и криптографического шифрования K_K информационного ресурса на основе координат контролируемой зоны и ключей пользователя S_S и S_K;

2) шифрование информационного ресурса I сформированным ключом K_K;

3) стеганографическое сокрытие зашифрованного ресурса I_K ключом K_S.

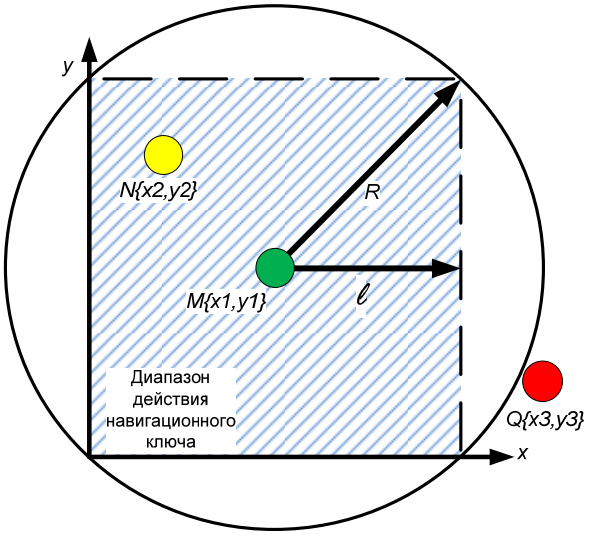

Рис. 2. Графическая схема диапазона действия навигационного ключа: $M\{x1,y1\}$ – координата местонахождения МОИ, $N\{x2,y2\}$ – координата назначения, в которой откроется ресурс, $Q\{x3,y3\}$ – любая другая координата, не попадающая в зону действия навигационного ключа, R – радиус окружности, описывающей пограничные точки контролируемой зоны

Во втором режиме работы программы ключи $K_{S.m}$ и $K_{K.m}$ для извлечения из стегоконтейнера S_I и дешифрования информационного ресурса, соответственно, формируются на основе текущих координат АТС и ключей пользователя S_S и S_K. Несовпадение текущих ключей и используемых при установке защиты приводит фактически к отказу доступа к информации.

На основе вышепредставленного алгоритма разработана прикладная программа «Защита доступа к информационному ресурсу на основе навигационного ключа» (рис. 4) [12].

Программа позволяет осуществить разграничение доступа к информационному ресурсу на основе географических координат по представленному ранее алгоритму. Исходными данными для работы программы являются стеганографический контейнер, представляющий собой rtf-файл, защищаемый информационный ресурс, и навигационные координаты местоположения, представленные в формате NMEA-протокола. Для определения географических координат к программе подключается GPS/ГЛОНАСС-трекер с поддержкой NMEA-протокола по интерфейсу COM-порт.

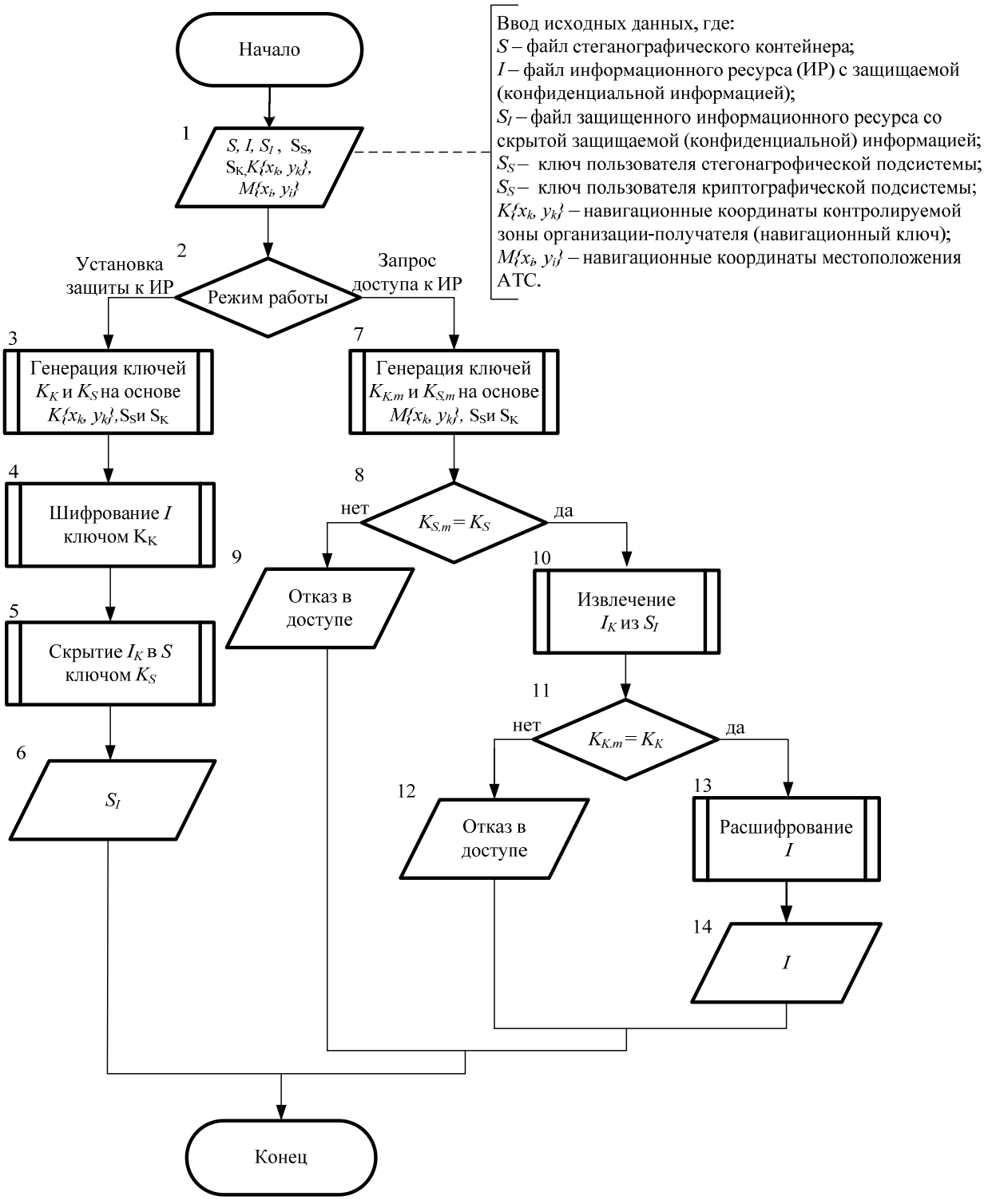

Рис. 3. Схема алгоритма программного средства защиты доступа к информационному ресурсу на основе навигационного ключа

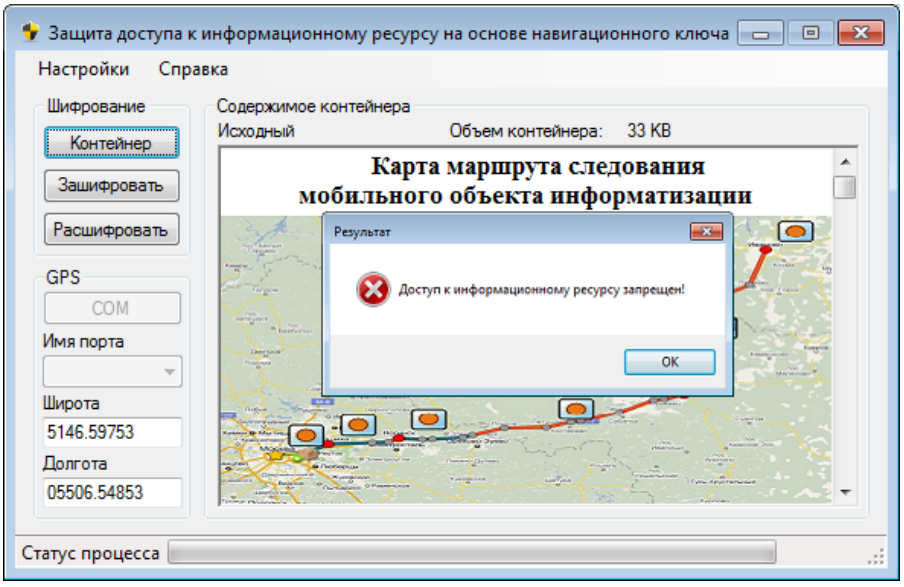

Рис. 4. Экранная форма прикладной программы «Защита доступа к информационному ресурсу на основе навигационного ключа»

Результатом выполнения программы является стеговложение формата rtf, в которое произведено скрытие зашифрованного файла с защищаемой информацией.

Выводы

С учетом того что злоумышленнику для доступа к информационному ресурсу необходимо преодолеть несколько уровней защиты, каждый из которых имеет собственную вероятность взлома, то риск НСД к информации системы будет определяться:

$$R = U \cdot P_1 \cdot P_2 \cdot P_3 \cdot P_4, \qquad (5)$$

где U – оценка ущерба от несанкционированного доступа к ИР; P_1 – вероятность преодоления уровня охранной системы АТС; P_2 – вероятность преодоления системы разграничения доступа бортовой системы АТС; P_3 – вероятность преодоления подсистемы стеганографического сокрытия ИР; P_4 – вероятность преодоления криптографической подсистемы.

В связи с тем что навигационные координаты используются как составная часть ключей 4 подсистем, то для реализации атаки злоумышленник должен преодолеть все уровни защиты. Причем использование навигационного ключа выполняет сразу две функции:

– увеличивает время перебора ключей всех 4 уровней;

– обеспечивается выполнение защищенных операций только в заданных областях, определяющихся навигационными координатами и являющихся составной частью правил доступа.

Таким образом, разработанный метод позволяет реализовать многоуровневую систему защиты доступа к информационным ресурсам, которая в качестве дополнительного правила разграничения доступа использует местоположение субъекта на основе навигационного ключа. Достоинством данного подхода является снижение вероятности угрозы физического или психологического воздействие на владельца ИР, чтобы он сам предоставил доступ злоумышленнику к информационному ресурсу вне контролируемой зоны. Это обусловлено тем, что определение навигационных координат осуществляется автоматически системой защиты без участия субъекта доступа к ИР. Кроме того, представленный подход осуществляет интеграцию данных о расположении субъекта в безопасной зоне в стандартные средства защиты информации, что дополняет их и позволяет значительно снизить риск НСД. Одним из аспектов усовершенствования рассмотренного метода является повышение точности определения координат объекта защиты на основе аппаратно-программных средств спутниковой навигации и использования базовых станций [13].

Библиографические ссылки

1. Безопасность мобильных технологий в корпоративном секторе, общие рекомендации. Москва, 2015. [Электронный ресурс]. URL: http://aciso.ru/upload/docs/MobileSecurity_ACISO_brochure_v.1.0.pdf (дата обращения 05.08.2019).

2. *G. Delac, M. Silic and J. Krolo.* (2011) Emerging security threats for mobile platforms, Proceedings of the 34th International Convention MIPRO, Opatija, 2011, pp. 1468-1473.

3. Muthuswamy, Sujithra & Ganapathi, Padmavathi. (2012). Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism. International Journal of Computer Applications. 56. pp. 24-29.

4. Shafique, Usman & Khan, Hikmat & Waqar, Sabah-Ud-Din & Sher, Asma & Zeb, Adnan & Shafi, Uferah & , Ullah & Bashir, Faisal & Munam, Ali. (2017). Modern Authentication Techniques in Smart Phones: Security and Usability Perspective. International Journal of Advanced Computer Science and Applications. 8. pp. 331–340.

5. *Яблоков В. В., Васильев С. А.* Система и способ для защиты доступа к данным, сохраненным на мобильном устройстве, с помощью пароля. Патент РФ № 2488879/C1, 2013.

6. *Чуньсюань Е., ШАХ Йоджендра К., ЧА Инхиок.* Способ и устройство для организации защиты информации о местоположении и управления доступом с использованием информации о местоположении. Патент РФ № 2428808/C2, 2011.

7. *Garcia F., Oswald D., Kasper T., Pavlides P.* Lock It and Still Lose It: On the (In)Security of Automotive Remote Keyless Entry Systems . In Proceedings of the 25th USENIX Security Symposium. USENIX Association. 2016. p. 929-944.

8. *Francillon A., Danev B., Čapkun S.* Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. [Электронный ресурс]. URL: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/franc2.pdf (дата обращения – 03.06.2018).

9. *Евсеев С. П., Абдуллаев В. Г., Агазаде Ж. Ф., Аббасова В. С.* Усовершенствование метода двухфакторной аутентификации на основе использования модифицированных крипто-кодовых схем // Системы обработки информации. 2016. № 9 (146). – С. 132–145.

10. *Аралбаев Т. З., Галимов Р. Р., Каменева Е. В., Идрисов А. Ш., Солдатов А. С.* Исследование погрешностей в системе мониторинга мобильных объектов на основе навигационного ключа // сборник статей «Прогрессивные технологии в транспортных системах», XIII международная научно-практическая конференция – Оренбург: Оренбургский государственный университет, 2017. – С. 9–12.

11. Там же.

12. *Аралбаев Т. З., Галимов Р. Р., Каменева Е. В., Идрисов А. Ш., Солдатов А. С.* Защита доступа к информационному ресурсу на основе навигационного ключа: прикладная программа. – Оренбург : ОГУ. – 2017. [Электронный ресурс]. URL: http://ufer.osu.ru/index.php?option=com_uferdbsearch&view= uferdbsearch&action =details&ufer_id=1353 (дата обращения 09.10.2017).

13. *Идрисов А.Ш., Солдатов А.С.* Исследование погрешности определения местоположения мобильных объектов информатизации с применением корректирующей навигационной аппаратуры // Дневник науки. 2019. № 4 [Электронный ресурс]. URL: http://www.dnevniknauki.ru/images/publications/2019/4/technics/Idrisov_Soldatov.pdf (дата обращения 05.05.2019).

References

1. *Bezopasnost' mobil'nykh tekhnologii v korporativnom sektore obshchie rekomendatsii* [Mobile technology security in the corporate sector general recommendations. Moscow, 2015] (in Russ.). Available at: http://aciso.ru/upload/docs/MobileSecurity_ACISO_brochure_v.1.0.pdf (accessed 08.08.2019).

2. G. Delac, M. Silicon and J. Krolo. (2011) Emerging security threats for mobile platforms, Proceedings of the 34th International Convention MIPRO, Opatija, 2011, pp. 1468-1473.

3. Muthuswamy, Sujithra & Ganapathi, Padmavathi. (2012). Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism. International Journal of Computer Applications. 56. pp 24-29.

4. Shafique, Usman & Khan, Hikmat & Waqar, Sabah-Ud-Din & Sher, Asma & Zeb, Adnan & Shafi, Uferah &, Ullah & Bashir, Faisal & Munam, Ali. (2017). Modern Authentication Techniques in Smart Phones: Security and Usability Perspective. International Journal of Advanced Computer Science and Applications. 8. pp 331-340.

5. Yablokov V.V., Vasiliev S.A. *Sistema i sposob dlya zashchity dostupa k dannym, sokhranennym na mobil'nom ustroistve, s pomoshch'yu parolya* [System and method for protecting access to data stored on a mobile device with a password]. Patent RF, no. 2488879 / C1, 2013.

6. Chunsuan E., SHA Yojendra K., CH Inhiok. *Sposob i ustroistvo dlya organizatsii zashchity informatsii o mestopolozhenii i upravleniya dostupom s ispol'zovaniem informatsii o mestopolozhenii* [Method and device for organizing the protection of location information and access control using location information] Patent RF, no. 2428808 / C2, 2011.

7. Garcia F, Oswald D, Kasper T, Pavlides P. (2016) Lock It and Still Lose It: On the (In) Security of Automotive Remote Keyless Entry Systems. In Proceedings of the 25th USENIX Security Symposium. USENIX Association. pp. 929-944.

8. Francillon A., Danev B., Иарkun S. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. Available at: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/franc2.pdf (accessed June 3, 2018).

9. Evseev, S.P., Abdullaev V.G., Agazade J.F., Abbasova V.S. (2016) *Usovershenstvovanie metoda dvukhfaktornoi autentifikatsii na osnove ispol'zovaniya modifitsirovannykh kripto-kodovykh skhem* [Improving the method of two-factor authentication based on the use of modified crypto-code schemes]. *Sistemy obrabotki informatsii* [Information Processing Systems]. N 9 (146), pp. 132-145.

10. Aralbaev T.Z., Galimov R.R., Kameneva E.V., Idrisov A.Sh., Soldatov A.S. (2017) Issledovanie pogreshnostei v sisteme monitoringa mobil'nykh ob"ektov na osnove navigatsionnogo klyucha [The study

of errors in the monitoring system of mobile objects based on the navigation key]. In collection of articles "Progressivnye tekhnologii v transportnykh sistemakh" ["Progressive technologies in transport systems"], XIII international scientific-practical conference - Orenburg: Orenburg State University, 2017. - P. 9-12.

11. Ibid.

12. Aralbaev T.Z., Galimov R.R., Kameneva E.V., Idrisov A.Sh., Soldatov A.S. (2017) *Zashchita dostupa k informatsionnomu resursu na osnove navigatsionnogo klyucha* [Securing access to an information resource based on a navigation key]: application program. - Orenburg: OSU. - 2017. Available at: http://ufer.osu.ru/index.php?option=com_uferdbsearch&view= uferdbsearch & action = details & ufer_id = 1353 (accessed 09.10.2017).

13. Idrisov A.Sh., Soldatov A.S. (2019) *Issledovanie pogreshnosti opredeleniya mestopolozheniya mobil'nykh ob"ektov informatizatsii s primeneniem korrektiruyushchei navigatsionnoi apparatury* [Investigation of the error in determining the location of mobile informatization objects using corrective navigation equipment] Dnevnik nauki [Science Diary]. 2019. No. 4. Available at: http://www.dnevniknauki.ru/images/publications/2019/4/technics/Idrisov_Soldatov.pdf (accessed 05.05.2019).

* * *

Method of Protecting Access to the Information Resource of a Mobile Object of Informatization Based on Navigation Key

T. Z. Aralbaev, DSc in Engineering, Professor, Orenburg State University
R. R. Galimov, PhD in Engineering, Associate Professor, Orenburg State University
E. V. Kameneva, Senior Lecturer, Orenburg State University
A. Sh. Idrisov, Master's Degree Student, Orenburg State University
A. S. Soldatov, Master's Degree Student, Orenburg State University

The relevance of the topic is determined by the broad development and use of mobile computing facilities used to store and process confidential information resources. This work is devoted to the protection of information resources in the on-board system of vehicles from unauthorized access. The shortcomings of the existing approaches to protecting such systems due to the wide possibilities of attackers outside the controlled areas impacts, both on the means of protection and on users of the system, were identified. In this regard, an approach to the protection of information resources of mobile computing facilities has been proposed, which allows access only in protected areas. In the work, a structural model of a multilevel system for protecting access to an information resource is developed, which includes the following levels: physical protection, authentication system, cryptographic and steganographic systems. A feature of the proposed method is that it is proposed to supplement the rules for accessing the subsystems data resource by controlling the location of the mobile computerization object. This is achieved by generating keys of cryptographic and steganographic systems taking into account data on the geographical coordinates of the mobile object. Based on this model, a software tool has been developed to protect access to an information resource, taking into account the navigation access key, which allows to increase the level of security of mobile informatization objects.

Keywords: protection of access to the information resource, navigation key, steganography, cryptography, multi-level security system, mobile object of informatization.

Получено: 26.08.19