Научная статья
УДК 004.457
DOI:10.31854/1813-324X-2023-9-4-86-96

Метод повышения защищенности информационно-телекоммуникационной сети с учетом использования средств определения геолокации нарушителя

Валерий Алексеевич Липатников✉, lipatnikovanl@mail.ru
Вадим Александрович Задбоев, zadboev89@mail.ru
Кирилл Витальевич Мелехов, kirill_melehov@bk.ru
Александр Александрович Шевченко, alex_pavel1991@mail.ru

Военная академия связи им. С.М. Буденного,
Санкт-Петербург, 194064, Российская Федерация

Аннотация: *Известные методы обеспечения информационной безопасности информационно-телекоммуникационных сетей с применением анализа их внутреннего трафика в современных условиях недостаточно эффективны, так как используют не все средства обнаружения внешних угроз. В данной статье авторами затрагивается вопрос возможности применения процедуры определения IP-геолокации в рамках обеспечения информационной безопасности сети.* ***Цель:*** *обеспечение уровня защищенности информационно-телекоммуникационной сети выше требуемого значения путем эффективности обнаружения внешних нарушителей за счет использования средств определения геолокации нарушителя в процессе обеспечения информационной безопасности.* ***Результат:*** *предложен метод повышения защищенности информационно-телекоммуникационной сети за счет внедрения программного обеспечения для определения геолокации нарушителя после обнаружения вторжений.*

Ключевые слова: *информационная безопасность, информационно-телекоммуникационная сеть, IP-геолокация, внешние угрозы, сканирование сети.*

Ссылка для цитирования: Липатников В.А., Задбоев В.А., Мелехов К.В., Шевченко А.А. Метод повышения защищенности информационно-телекоммуникационной сети с учетом использования средств определения геолокации нарушителя // Труды учебных заведений связи. 2023. Т. 9. № 4. С. 86–96. DOI:10.31854/1813-324X-2023-9-4-86-96

A Method of Improving the Security of Information and Telecommunications Network Using the Means of Determining Intruder's Geolocation

Valery Lipatnikov✉, lipatnikovanl@mail.ru
Vadim Zadboev, zadboev89@mail.ru
Kirill Melekhov, kirill_melehov@bk.ru
Aleksandr Shevchenko, alex_pavel1991@mail.ru

Military Academy of Communications,
St. Petersburg, 194064, Russian Federation

Abstract: *Known methods of ensuring information security of information and telecommunication networks with the use in modern conditions are not effective enough, since not all means of detecting external threats are used. In this article, the authors raise the issue of the possibility of using the procedure for determining IP geolocation in the*

framework of ensuring the information security of the network. Purpose: to ensure the level of security of the information and telecommunications network above the required value by effectively detecting external intruders through the use of tools for determining the geolocation of the intruder in the process of ensuring information security. Result: a method is proposed for improving the security of an information and telecommunication network, taking into account the introduction of software for determining the geolocation of an intruder after intrusion detection.

Keywords: *information security, information and telecommunications network, IP geolocation, external threats, network scanning.*

For citation: Lipatnikov V., Zadboev V., Melekhov K., Shevchenko A. A method of Improving the Security of Information and Telecommunications Network Using the Means of Determining Intruder's Geolocation. *Proceedings of Telecommun. Univ.* 2023;9(4):86–96. DOI:10.31854/1813-324X-2023-9-4-86-96

Введение

В наше время, когда сеть Интернет стала неотъемлемой частью жизни большинства людей и бизнес-процессов, вопрос безопасности критической информации, находящейся во внутренней сети, становится все более актуальным. Одним из процессов, позволяющим обеспечить защищенность информационно-телекоммуникационной сети (ИТКС), является определение геолокации по заданному IP-адресу, который может быть полезным инструментом для расследования инцидентов информационной безопасности (ИБ), выявления нарушителей и предотвращения различных видов мошенничества, хакерских атак, кибершпионажа и других преступлений в сети.

Анализ результатов исследований в области обеспечения информационной безопасности (ИБ) ИТКС показал недостаточную проработку вопросов по определению геолокации нарушителя для повышения защищенности сетей. Так в [1] рассмотрены основные категории IP-адресов и угрозы использования действительных IP-адресов в сети Интернет. Также представлен фрагмент работы программы, позволяющей по IP-адресу пользователя определять его местоположение и некоторые персональные данные.

В статье [2] предложен метод повышения точности определения IP-геолокации, заключающийся в использовании метода простого большинства и вычисления координат с учетом уровня доверия к IP-геосервисам. Авторы предлагают устанавливать уровень доверия за счет сравнительного анализа IP-геосервисов по точности. Отмечая их значительный вклад в обоснование необходимости определения IP-геолокации нарушителя и развитие методов повышения его точности, следует отметить, что авторы не предлагают конкретных решений по внедрению процесса определения геолокации нарушителя в процесс обеспечения защищенности ИТКС и способов отслеживания нарушителей, находящихся вне сети.

В связи с этим **целью исследования** является обеспечение уровня защищенности ИТКС выше требуемого значения за счет разработки метода его повышения с использованием средств определения геолокации нарушителя.

1. Алгоритм сканирования ИТКС для выявления подозрительных действий внутри сети и алгоритм определения геолокации нарушителя

Основой метода являются алгоритм сканирования ИТКС для выявления подозрительных действий внутри сети (рисунок 1) и алгоритм определения геолокации нарушителя (рисунок 2).

Алгоритм сканирования ИТКС поясняется следующим образом:

1) постоянно сканируется сетевой трафик внутренней сети на предмет подозрительных действий пользователя;

2) поочередно выбирается каждый адрес для проверки на наличие в списке доверенных IP-адресов;

3) в случае обнаружения несоответствия со списком доверенных IP-адресов, при несоответствии данному адресу, блокируется доступ к ИТКС, регистрируется инцидент и определяется географическое местоположение данного IP-адреса;

4) по окончанию данных мероприятий выводится сформированный отчет о проделанной работе и полученных данных;

5) при условии, что полученный IP-адрес находится в списке доверенных, ему предоставляется доступ к ИТКС, однако продолжается постоянное наблюдение за ним на выявление подозрительных действий;

6) при обнаружении таких действий для него также доступ блокируется, регистрируется инцидент и определяется географическое местоположение по данному IP-адресу. По окончанию данных мероприятий выводится сформированный отчет о проделанной работе и полученных данных [3, 4].

Система определения геолокации осуществляет выявление местоположения по известному IP-адресу нарушителя. Процесс работы программы происходит следующим образом [5, 6]: IP-адрес для повторной отправки запроса, полученные данные записываются во внутреннюю базу данных (БД) и обрабатываются.

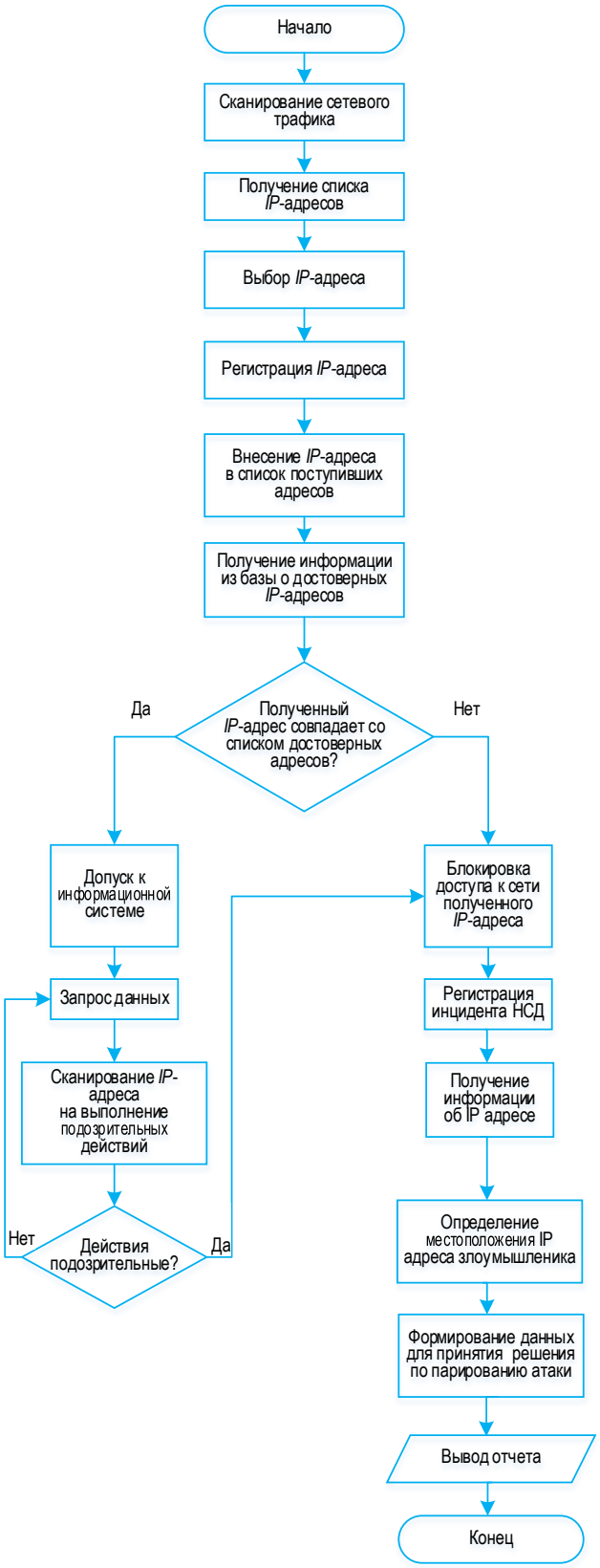


Рис. 1. Алгоритм сканирования ИТКС для выявления подозрительных действий внутри сети

Fig. 1. Enterprise ITCS Algorithm for Suspicious Activities within the Network

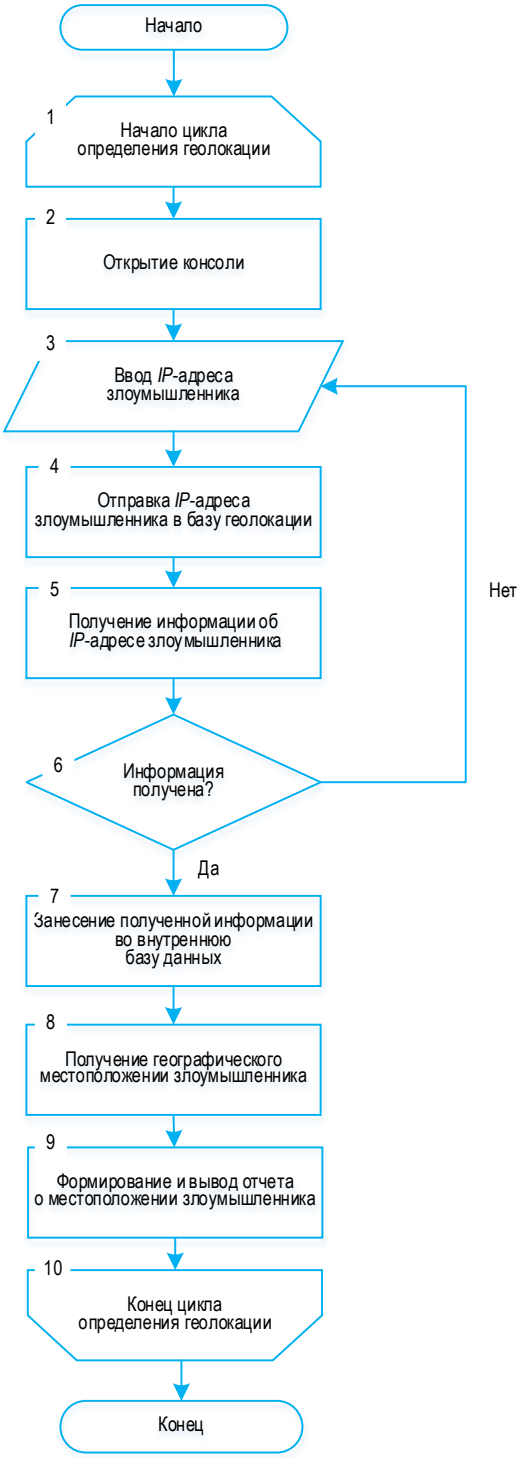


Рис. 2. Алгоритм определения геолокации нарушителя

Fig. 2. Algorithm for Determining the Geolocation of the Intrude

Первоначально открывается консоль программы и в активном окне вводится IP-адрес нарушителя, полученный адрес отправляется в базу IP–геолокации, из которой получают информацию об IP-адресе нарушителя, а в случае, если данные не были получены, программа снова потребует ввести.

По итогу из обработанных данных получают данные о географическом местоположении, а именно: наименование страны, региона, города, координаты, временная зона, наименование провайдера и почтовый код-нарушителя, которому принадлежит адрес. По этим данным формируется и выводится отчет о результатах работы программы [7, 8]

2. Моделирование процесса определения геолокации нарушителя

С целью формирования требований к процессу определения геолокации нарушителя, как к подпроцессу процесса обеспечения ИБ ИТКС было проведено моделирование данного процесса.

В процессе моделирования введен показатель – вероятность успешного определения геолокации нарушителя ($Рм$) и параметры: $\lambda_О$ – интенсивность поступления задач на определение геолокации нарушителя: $\lambda_О = \frac{1}{\overline{t}_О}$, где $\overline{t}_О$ – среднее время поступления задач на определение геолокации нарушителя; $\lambda_{ОК}$ – интенсивность открытия консоли программы: $\lambda_{ОК} = \frac{1}{\overline{t}_{ОК}}$, где $\overline{t}_{ОК}$ – среднее время открытия консоли программы; $\lambda_{ВА}$ – интенсивность ввода IP-адреса: $\lambda_{ВА} = \frac{1}{\overline{t}_{ВА}}$, где $\overline{t}_{ВА}$ – среднее время ввода IP-адреса; $\lambda_{ОА}$ – интенсивность отправки IP-адреса: $\lambda_{ОА} = \frac{1}{\overline{t}_{ОА}}$, где $\overline{t}_{ОА}$ – среднее время отправки IP-адреса; $\lambda_{ПИ}$ – интенсивность получения информации: $\lambda_{ПИ} = \frac{1}{\overline{t}_{ПИ}}$, где $\overline{t}_{ПИ}$ – среднее время получения информации; $\lambda_{ЗПИ}$ – интенсивность занесения полученной информации во временную БД: $\lambda_{ЗПИ} = \frac{1}{\overline{t}_{ЗПИ}}$, где $\overline{t}_{ЗПИ}$ – среднее время занесения полученной информации во временную БД; $\lambda_{ПГМ}$ – интенсивность получения геолокации: $\lambda_{ПГМ} = \frac{1}{\overline{t}_{ПГМ}}$, где $\overline{t}_{ПГМ}$ – среднее время получения геолокации; λ_{42} – интенсивность перехода к повторному запросу IP-адреса: $\lambda_{42} = \frac{1}{\overline{t}_{42}}$, где $\overline{t}_{42}$ – среднее время перехода к повторному запросу IP-адреса [9, 10].

На рисунке 3 представлен граф возможных состояний системы ИБ в процессе определения геолокации нарушителя в информационной сети [11].

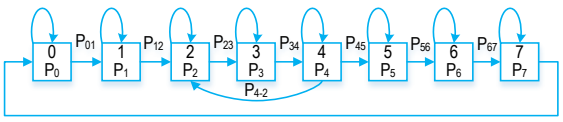


Рис. 3. Граф состояний системы ИБ в процессе определения геолокации нарушителя

Fig. 3. State Graph of the IS System in the Process of Determining the Geolocation of the Intruder

На рисунке 3 представлены следующие состояния системы ИБ.

Состояние «0» соответствует состоянию, когда система ИБ ожидает получение IP-адреса. Вероятность того, что система ИБ находится в этом состоянии, обозначим через P_0. Система ИБ переходит в состояние «1» с вероятностью P_{01} за время $t_{ОК}$.

Состояние «1» соответствует состоянию, когда администратор ИБ, получив задачу по определению геолокации нарушителя, открывает консоль. Вероятность того, что система ИБ находится в этом состоянии, обозначим через P_1. Система ИБ переходит в состояние «2» с вероятностью P_{12} за время $t_{ОК}$.

Состояние «2» соответствует состоянию, когда вводится IP-адрес нарушителя. Вероятность того, что система ИБ находится в этом состоянии, обозначим через P_2. Система ИБ переходит в состояние «3» с вероятностью P_{23} за время $t_{ВА}$.

Состояние «3» соответствует состоянию, когда введенный IP-адрес отправляется в базу геолокации. Вероятность того, что система ИБ находится в этом состоянии, обозначим через P_3. По окончанию данного процесса система переходит в состояние «4» с вероятностью P_{34} за время $t_{ОА}$.

Состояние «4» соответствует состоянию, когда введенный IP-адрес проверяется на получение данных. Вероятность того, что система ИБ находится в этом состоянии, обозначим через P_4. Если данные не были получены, то система переходит в состояние «2» с вероятностью P_{42} за время t_{42}. Если данные получены, то система переходит в состояние «5» с вероятностью P_{45} за время $t_{ПИ}$.

Состояние «5» соответствует состоянию, когда полученная информация заносится во внутреннюю БД. Вероятность того, что система ИБ находится в этом состоянии, обозначим через P_5. По окончанию данного процесса система переходит в состояние «6» с вероятностью P_{56} за время $t_{ЗПИ}$.

Состояние «6» соответствует состоянию, когда из полученной информации добывается геолокация нарушителя. Вероятность того, что система ИБ находится в этом состоянии, обозначим через P_6. По окончанию данного процесса система переходит в состояние «7» с вероятностью P_{67} за время $t_{ПГМ}$.

Состояние «7» соответствует состоянию, когда на основе полученной информации о геолокации формируется отчет, который затем передается администратору ИБ. Вероятность того, что система ИБ находится в этом состоянии, обозначим через P_7. По окончании данного процесса система переходит в состояние «0» с вероятностью P_{70} за время $t_{ФВО}$.

В процессе моделирования были введены следующие допущения:

1) потоки задач на определение геолокации нарушителя и на формирование отчета о ней являются простейшими потоками;

2) поток задач на определение геолокации нарушителя является «редким»;

3) время распределено по показательному закону;

4) для каждого момента времени вероятность любого состояния системы в будущем зависит только от ее состояния в настоящий момент и не зависит от того, каким образом система пришла в это состояние.

Исходя из принятых допущений для построения модели процесса определения геолокации нарушителя можно воспользоваться аппаратом Марковских случайных процессов [12], то есть с помощью дифференциальных уравнений, в которых неизвестными функциями являются вероятности нахождения системы ИБ в различных состояниях с P_0 до P_7. В результате была составлена система дифференциальных уравнений (1), которая преобразована в система алгебраических уравнений (2) ввиду того, что при достижении стационарного состояния, то есть при $t \to \infty$ вероятности $P_i(t)$ будут стремиться к постоянным пределам, а и их производные – к нулю.

$$\begin{cases} \frac{dP_0(t)}{dt} = \mu_0 P_0(t) - \lambda_0 P_0(t), \\ \frac{dP_1(t)}{dt} = \lambda_0 P_0(t) - \lambda_{12} P_1(t), \\ \frac{dP_2(t)}{dt} = \lambda_{12} P_1(t) + \alpha P_4(t) - \lambda_{23} P_2(t), \\ \frac{dP_3(t)}{dt} = \lambda_{23} P_2(t) - \lambda_{34} P_3(t), \\ \frac{dP_4(t)}{dt} = \lambda_{34} P_3(t) - \alpha P_4(t) - \beta P_4(t), \\ \frac{dP_5(t)}{dt} = \beta P_4(t) - \lambda_{56} P_5(t), \\ \frac{dP_6(t)}{dt} = \lambda_{56} P_5(t) - \lambda_{67} P_6(t), \\ \frac{dP_7(t)}{dt} = \lambda_{67} P_0(t) - \mu_0 P_7(t), \end{cases} \quad (1)$$

где P_x – возможные состояния графа; λ_x – плотность потока формирования модели перехода из одного состояния в другое; α, β – плотность потока перехода состояний при разных соблюдениях условий алгоритма; ϕ_0 – начальное состояние графа.

$$\begin{cases} \mu_0 P_0(t) - \lambda_0 P_0(t) = 0, \\ \lambda_0 P_0(t) - \lambda_{12} P_1(t) = 0, \\ \lambda_{12} P_1(t) + \alpha P_4(t) - \lambda_{23} P_2(t) = 0, \\ \lambda_{23} P_2(t) - \lambda_{34} P_3(t) = 0, \\ \lambda_{34} P_3(t) - \alpha P_4(t) - \beta P_4(t) = 0, \\ \beta P_4(t) - \lambda_{56} P_5(t) = 0, \\ \lambda_{56} P_5(t) - \lambda_{67} P_6(t) = 0, \\ \lambda_{67} P_0(t) - \mu_0 P_7(t) = 0. \end{cases} \quad (2)$$

Решив систему (2) с учетом условия нормировки $\sum_{k=0}^{m} P_k = 1$, получаем решения (3).

В качестве вероятности успешного определения геолокации нарушителя можно использовать вероятность нахождения системы ИБ в состоянии, когда последняя реализует конечное формирование и вывод отчета по результатам работы (P_7) [13, 14]. Вероятность P_7 можно принять за вероятность успешного определения геолокации нарушителя, если считать, что после определения геолокации нарушителя по одному IP-адресу система ИБ сразу же приступает к определению геолокации нарушителя по следующему IP-адресу, то есть система ИБ должна эффективно работать и в состоянии штатной работы (P_0) [15, 16]. Таким образом, вероятность успешного выполнения $P_M = P_0 + P_7$, а с учетом (3) P_M принимает вид (4).

После чего проводится верификация разработанной модели; для этого были взяты исходные данные, представленные в таблице 1 [15].

ТАБЛИЦА 1. Исходные данные верификация модели процесса определения геолокации нарушителя

TABLE 1. Initial Data Verification of the Process Model for Determining the Geolocation of the Intruder

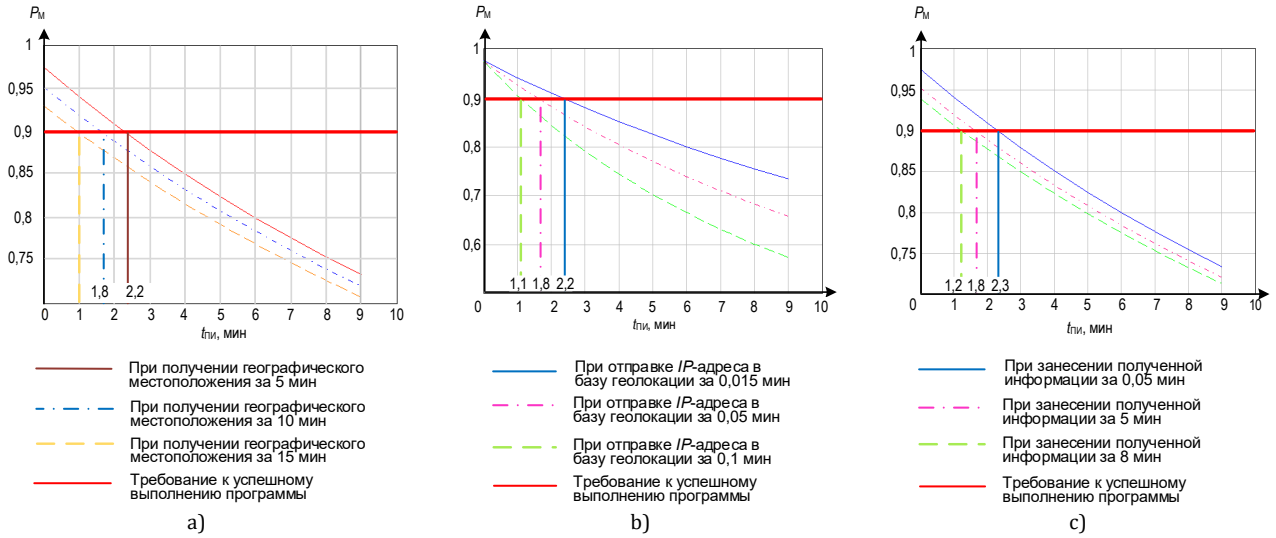
№ п/п	Состояние системы	Параметр	Значение, мин
1.	Ожидание начала работы (О)	$t_О$	0,01
2.	Открытие консоли (ОК)	$t_{ОК}$	0,03
3.	Ввод IP-адреса (ВА) нарушителя	$t_{ВА}$	0,05
4.	Отправка IP-адреса (ОА) нарушителя в базу геолокации	$t_{ОА}$	0,015 0,05 0,1
5.	Получение информации (ПИ) об IP-адресе нарушителя	$t_{ПИ}$	10
6.	Занесение полученной (ЗПИ) информации во временную БД	$t_{ЗПИ}$	0,05 5 8
7.	Получение геолокации (ПГМ) нарушителя	$t_{ПГМ}$	5 10 15
8.	Формирование и вывод отчета (ФВО) о геолокации нарушителя	$t_{ФВО}$	0,005

Подставляя вышеперечисленные исходные данные в выражение (4), получаем зависимости вероятности успешного определения геолокации нарушителя (P_M) от времени получения информации об IP-адресе ($t_{ПИ}$) при различном времени получения геолокации нарушителя ($t_{ПГМ}$) [17, 18], представленные на рисунке 4a. Из рисунка следует, что при увеличении времени получения геолокации нарушителя ($t_{ПГМ}$), P_M будет опускаться ниже требуемого уровня 0,9. Так, например, при реализации получении геолокации за 5 минут $t_{ПИ}$ должно быть больше 2,2 минут, при реализации получении геолокации за 10 минут $t_{ПИ}$ должно быть больше 1,8 минут, а при реализации получении геолокации за 15 минут $t_{ПИ}$ должно быть больше 1 минуты [19].

Далее получаем зависимости вероятности успешного определения геолокации нарушителя (P_M) от времени получения информации об IP-адресе ($t_{ПИ}$) при различном времени отправки IP-адреса в базу геолокации ($t_{ОА}$), представленные на рисунке 4b.

$$\begin{cases} P_0 = \dfrac{1}{1+\frac{\lambda_0}{\lambda_{12}}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{23}\beta}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{34}\beta}+\frac{\lambda_0}{\beta}+\frac{\lambda_0}{\lambda_{56}}+\frac{\lambda_0}{\lambda_{67}}+\frac{\lambda_0}{\mu_0}}, \\ P_1 = \dfrac{\lambda_0}{\lambda_{12}} \bullet \left(\dfrac{1}{1+\frac{\lambda_0}{\lambda_{12}}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{23}\beta}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{34}\beta}+\frac{\lambda_0}{\beta}+\frac{\lambda_0}{\lambda_{56}}+\frac{\lambda_0}{\lambda_{67}}+\frac{\lambda_0}{\mu_0}} \right), \\ P_2 = \dfrac{\lambda_0(\lambda+\beta)}{\lambda_{23}\beta} \bullet \left(\dfrac{1}{1+\frac{\lambda_0}{\lambda_{12}}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{23}\beta}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{34}\beta}+\frac{\lambda_0}{\beta}+\frac{\lambda_0}{\lambda_{56}}+\frac{\lambda_0}{\lambda_{67}}+\frac{\lambda_0}{\mu_0}} \right), \\ P_3 = \dfrac{\lambda_0(\lambda+\beta)}{\lambda_{34}\beta} \bullet \left(\dfrac{1}{1+\frac{\lambda_0}{\lambda_{12}}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{23}\beta}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{34}\beta}+\frac{\lambda_0}{\beta}+\frac{\lambda_0}{\lambda_{56}}+\frac{\lambda_0}{\lambda_{67}}+\frac{\lambda_0}{\mu_0}} \right), \\ P_4 = \dfrac{\lambda_0}{\beta} \bullet \left(\dfrac{1}{1+\frac{\lambda_0}{\lambda_{12}}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{23}\beta}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{34}\beta}+\frac{\lambda_0}{\beta}+\frac{\lambda_0}{\lambda_{56}}+\frac{\lambda_0}{\lambda_{67}}+\frac{\lambda_0}{\mu_0}} \right), \\ P_5 = \dfrac{\lambda_0}{\lambda_{56}} \bullet \left(\dfrac{1}{1+\frac{\lambda_0}{\lambda_{12}}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{23}\beta}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{34}\beta}+\frac{\lambda_0}{\beta}+\frac{\lambda_0}{\lambda_{56}}+\frac{\lambda_0}{\lambda_{67}}+\frac{\lambda_0}{\mu_0}} \right), \\ P_6 = \dfrac{\lambda_0}{\lambda_{67}} \bullet \left(\dfrac{1}{1+\frac{\lambda_0}{\lambda_{12}}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{23}\beta}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{34}\beta}+\frac{\lambda_0}{\beta}+\frac{\lambda_0}{\lambda_{56}}+\frac{\lambda_0}{\lambda_{67}}+\frac{\lambda_0}{\mu_0}} \right), \\ P_7 = \dfrac{\lambda_0}{\mu_0} \bullet \left(\dfrac{1}{1+\frac{\lambda_0}{\lambda_{12}}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{23}\beta}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{34}\beta}+\frac{\lambda_0}{\beta}+\frac{\lambda_0}{\lambda_{56}}+\frac{\lambda_0}{\lambda_{67}}+\frac{\lambda_0}{\mu_0}} \right). \end{cases} \quad (3)$$

$$P_{\text{M}} = \frac{\lambda_0 + \mu_0}{\mu_0 \cdot \left(1+\frac{\lambda_0}{\lambda_{12}}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{23}\beta}+\frac{\lambda_0(\alpha+\beta)}{\lambda_{34}\beta}+\frac{\lambda_0}{\beta}+\frac{\lambda_0}{\lambda_{56}}+\frac{\lambda_0}{\lambda_{67}}+\frac{\lambda_0}{\mu_0}\right)}. \quad (4)$$



a) b) c)

Рис. 4. Зависимости вероятности $P_м$ от времени получения информации об IP-адресе при различном времени: а) получения геолокации нарушителя ($t_{ПГМ}$); b) отправки IP-адреса в базу данных ($t_{ОА}$); с) занесения полученной информации в базу данных ($t_{ЗПИ}$)

Fig. 4. Dependences of the Probability $P_м$ on the Time of Receiving Information about the IP Address at Different Times: a) Obtaining the Geolocation of the Intruder ($t_{ПГМ}$); b) Sending the IP Address to the Database ($t_{ОА}$); c) Entering the Received Information into the Database ($t_{ЗПИ}$

Из рисунка 4b следует, что при увеличении времени отправки IP-адреса в базу геолокации ($t_{ОА}$) вероятности успешного определения геолокации нарушителя ($P_М$) будет опускаться ниже требуемого уровня 0,9. Так, например, при реализации отправки IP-адреса в базу геолокации за 0,015 минут $t_{ПИ}$ должно быть больше 2,2 минут, при реализации отправки IP-адреса в базу геолокации за 0,05 минут $t_{ПИ}$ должно быть больше 1,8 минут, а при реализации отправки IP-адреса в базу геолокации за 0,1 минут $t_{ПИ}$ должно быть больше 1,1 минуты [20].

Следующим этапом было проведено исследование зависимостей вероятности успешного определения геолокации нарушителя ($P_М$) от времени получения информации об IP-адресе ($t_{ПИ}$) при различном времени занесения полученной информации в БД ($t_{ЗПИ}$), представленные на рисунке 4c. Из рисунка следует, что при увеличении времени занесения полученной информации в БД ($t_{ЗПИ}$) вероятность успешного определения геолокации нарушителя ($P_М$) будет уменьшается ниже требуемого уровня 0,9.

Так, например, при реализации занесения полученной информации в БД за 0,05 минут $t_{ПИ}$ должно быть больше 2,3 минут, при реализации занесения полученной информации в БД за 5 минут $t_{ПИ}$ должно быть больше 1,8 минут, а при реализации занесения полученной информации в БД за 8 минут $t_{ПИ}$ должно быть больше 1,2 минуты [21].

Исходя из всего вышеизложенного следует, что администратору ИБ необходимо своевременно реагировать на действия нарушителя в ИТКС. Для этого необходимо разработать средство, позволяющее сократить временные параметры, описанные выше [22, 23].

3. Программное обеспечение определения геолокации нарушителя

Для практической реализации предлагаемого метода повышения защищенности ИТКС принято решение разработать программное обеспечение (ПО) определения геолокации нарушителя с целью повышения оперативности реагирования на внешних нарушителей сети.

Для разрабатываемого ПО предъявляются следующие требования.

1) Завершенность – это насколько полно программа выполняет все заявленные функции и задачи, для которых она была разработана. Если программа имеет высокую завершенность, это означает, что она содержит все функции и возможности, которые были обещаны ее разработчиками.

2) Актуальность – это насколько программа соответствует требованиям и ожиданиям пользователей, а также насколько она удовлетворяет текущим требованиям рынка. Если программа актуальна, она отвечает потребностям пользователей и предоставляет им актуальные функции и возможности.

3) Исполнимость – это насколько эффективно программа выполняет свои функции и задачи. Если программа имеет высокую исполнимость, это означает, что она работает быстро и без ошибок, используя минимальное количество ресурсов компьютера [24, 25].

Важно, чтобы ПО было достаточно завершенным, актуальным и исполнимым, удовлетворяло потребности пользователей и оставалось конкурентоспособным на рынке. Кроме того, эти качественные характеристики помогают удовлетворять требованиям безопасности и надежности ПО.

Для разработки ПО в качестве языка программирования выбран язык – Python [26], преимуществами которого являются:

– простой и понятный синтаксис;

– совместимость с различными операционными системами: Windows, macOS, Linux;

– широкое применение;

– высокая скорость разработки.

В качестве среды программирования выбран Microsoft Visual Code [27], которому свойственна:

1) работа со множеством языков программирования, включая Python, JavaScript, C++, C#;

2) встроенная поддержка системы контроля версий, таких как Git.

3) возможность запускать и отлаживать приложения прямо из редактора, что упрощает процесс разработки.

Алгоритм работы ПО [28] представлен ниже:

1) после запуска программы вводится обнаруженный IP-адрес;

2) отправляется запрос на службы геолокации, с помощью которых определяется местоположение;

3) представляется вывод полученных данных геолокации по заданному IP-адресу в окне программы (рисунок 7).

```
Please enter IP: 15.65.128.255
[IP] : 15.65.128.255
[Int prov] : HP Inc.
[Org] : HP Inc
[Country] : Hesse
[City] : Frankfurt am Main
[ZIP] : 60313
[Lat] : 50.1109
[Lon] : 8.68213
```

Рис. 7. Пример работы программного обеспечения определения IP-геолокации

Fig. 7. An Example of How IP Geolocation Software Works

Вывод программы содержит следующие данные по порядку: введенный IP-адрес, название провайдера, предоставляющего услуги сети Интернет-пользователю, название организации, которой принадлежит IP-адрес, страну, город, почтовый индекс, а также примерную широту и долготу IP-адреса, что позволит оперативно начать расследование по данному факту несанкционированного воздействия на ИТКС предприятия [29, 30].

Заключение

В настоящее время обеспечение ИБ ИТКС основано на реализации реактивных способов защиты, которые не позволяют оперативно получать точную информацию о нахождении нарушителя и не учитывают динамику и стохастическую неопределенность основных процессов защиты информации. Также построенные системы обеспечения ИБ ИТКС на основе известных способов защиты информации не удовлетворяют требованиям нормативно-правовых документов. Поэтому предложен метод повышения защищенности ИТКС с использованием средств определения геолокации нарушителя. В его основе лежит описание способа сканирования сети предприятия, а также разработанные алгоритмы действий в случае обнаружения подозрительных активностей в сети и алгоритм определения геолокации нарушителя. Эти инновации в области кибербезопасности вносят дополнительный уровень защиты, обеспечивая более надежное и усовершенствованное реагирование на потенциальные угрозы в сети ИТКС.

Сравнительный анализ достоинств и недостатков методов моделирования сложнодинамических информационных систем позволяет сделать вывод о том, что процесс определения геолокации нарушителя, с учетом введенных ограничений и допущений, наиболее адекватно моделируется аналитическим методом с использованием основных положений теории принятия статистических решений, теории вероятности, математической статистики, теории Марковских цепей и дифференциального исчисления.

За счет моделирования процесса определения геолокации нарушителя установлены необходимые требования по вероятностно-временны́м характеристикам данного процесса, выполнение которых позволит оптимизировать выполнение процесса и обеспечить точность и своевременность в выявлении нарушителей. Эти требования при использовании предлагаемого метода способствуют достижению заданного уровня защищенности ИТКС и обеспечивают более надежную защиту от потенциальных угроз.

Разработанный метод повышения защищенности ИТКС с использованием средств определения геолокации нарушителя позволяет:

1) быстро и эффективно определить геолокацию нарушителя, так как использованы различные способы определения местоположения на основе IP-адреса, что повышает точность и достоверность полученных данных;

2) оптимизировать процесс обеспечения ИБ ИТКС за счет эффективной и быстрой обработки данных о геолокации нарушителя, что позволяет ускорить расследование инцидентов ИБ.

На основе предложенного метода разработано ПО «Средство определения в сети передачи данных цепочки маршрутов до географического местоположения нарушителя» [31], которое получило государственную регистрацию. Разработанное средство позволяет повысить безопасность ИТКС предприятия путем повышения оперативности реагирования на внешние угрозы.

В дальнейшем будут исследоваться возможности по реализации данного метода с точки зрения автоматизации процесса, что позволит полностью на программном уровне принимать самостоятельные решения по реагированию на подозрительные действия в сети для защиты от нарушителя. Развитие метода будет включать в себя анализ эффективности и масштабируемости автоматизированных решений, оптимизацию процесса для более эффективной защиты ИТКС. Этот шаг позволит более эффективно противодействовать потенциальным угрозам и обеспечивать непрерывную защиту информационных систем.

Список источников:

1. Морковкин Е.А., Новичихина А.А., Замулин И.С. IP-адресация и информационная безопасность // Вестник Хакасского государственного университета им. Н.Ф. Катанова. 2022. № 1(39). С. 9–12.

2. Иванов М.В., Полунин А.А. Повышение точности IP-геолокации на основе данных, предоставляемых открытыми IP-геосервисами // Информатика и автоматизация. 2022. Т. 21. № 4. С. 758–785. DOI:10.15622/ia.21.4.5

3. Липатников В.А., Шевченко А.А., Мелехов К.В., Задбоев В.А. Способ обнаружения географического местоположения нарушителя безопасности информации в сети передачи данных // II Всероссийская научно-техническая конференция «Состояние и перспективы развития современной науки по направлению "ИТ-технологии"» (Анапа, Россия, 23–24 марта 2023). Анапа: Федеральное государственное автономное учреждение «Военный инновационный технополис «ЭРА», 2023. Т. 2. С. 178–183.

4. Aljumaily M. Content Delivery Networks Architecture, Features, and Benefits. 2016. DOI:10.13140/RG.2.1. 1762.0722

5. Arif M.J., Karunasekera S., Kulkarni S., Gunatilaka A., Ristic B. Internet Host Geolocation Using Maximum Likelihood Estimation Technique // Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (Perth, Australia, 20–23 April 2010). IEEE, 2010. PP. 422–429. DOI:10.1109/AINA.2010.139

6. Липатников В.А., Шевченко А.А. Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2016. № 2(94). С. 128–140.

7. Williams J. Identification of IP address using fraudulent geolocation data. 2020. URL: https://www.imperial.ac.uk/media/imperial-college/faculty-of-engineering/computing/public/1920-ug-projects/Williams,-James-%28jw1317%29.pdf (дата обращения 13.09.2023)

8. Wang Z., Li H., Li Q., Li W., Zhu H., Sun L. Towards IP geolocation with intermediate routers based on topology discovery // Cybersecurity. 2019. Vol. 2. Article ID 13. DOI:10.1186/s42400-019-0030-2

9. Hufaker B., Fomenkov M., Claffy K. Geocompare: a comparison of public and commercial geolocation databases. 2011. URL: https://api.semanticscholar.org/CorpusID:13521646 (дата обращения 13.09.2023)

10. Pratap U., Canudas-de-Wit C., Garin F. Average state estimation in presence of outliers // Proceedings of the 59th IEEE Conference on Decision and Control (CDC, Jeju, South Korea, 14–18 December 2020). IEEE, 2020. PP. 6058–6063. DOI:10.1109/CDC42340.2020.9303809

11. Шевченко А.А. Математическая модель информационного противоборства двух систем в информационно-телекоммуникационном пространстве // Труды всеармейской научно-практической конференции: Инновационная деятельность в Вооруженных Силах Российской Федерации (Санкт-Петербург, России, 14–15 октября 2020). СПб.: Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации, 2020. С. 237–241.

12. Zhao F., Luo X., Gan Y., Zu S., Cheng Q., Liu F. IP Geolocation based on identification routers and local delay distribution similarity // Concurrency and Computation: Practice and Experience. 2018. Vol. 31. Iss. 22. DOI:10.1002/cpe.4722

13. Липатников В.А, Шевченко А.А., Яцкин А.Д., Семенова Е.Г. Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией // Информационно-управляющие системы. 2017. № 4. С. 67–76. DOI:10.15217/issn1684-8853.2017.4.67

14. Top 10 Best IP Geolocation APIs (in 2022). URL: https://rapidapi.com/blog/ip-geolocation-api (дата обращения 21.02.2022)

15. Semiu O.A. Migration of IPv4 to IPv6; Translation Method. 2018. URL: https://www.researchgate.net/publication/345727747_Migration_of_IPv4_to_IPv6_Translation_Method (дата обращения 21.02.2022)

16. Taylor J., Devlin J., Curran K. Bringing location to IP Addresses with IP Geolocation // Journal of Emerging Technologies in Web Intelligence. 2012. Vol. 4. Iss. 3. PP. 273–277.

17. Липатников В.А., Чепелев К.В., Шевченко А.А. Способ защиты информационно-вычислительной сети от вторжений. Патент RU 2705773 C1 от 09.01.2019. Опубл. 11.11.2019.

18. Padmanabhan V.N., Subramanian L. An investigation of geographic mapping techniques for internet hosts // Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM, San Diego, USA, 24–26 October 2023). PP. 173–185. New York: ACM, 2001. DOI:10.1145/383059.383073

19. Luckie M., Dhamdhere A., Huffaker B., Clark D., claffy kc. bdrmap: Inference of Borders Between IP Networks // Proceedings of the Internet Measurement Conference (IMC '16, Santa Monica, USA, 14–16 November 2016). New York: ACM, 2016. PP. 381–396. DOI:10.1145/2987443.2987467

20. Липатников В.А., Мелехов К.В., Задбоев В.А. Способ определения локации злоумышленника в сети передачи данных сетевой инфраструктуры // Международная научно-практическая конференция «Транспорт России: проблемы и перспективы» (Санкт-Петербург, Россия, 09–10 ноября 2022). Санкт-Петербург: Институт проблем транспорта им. Н.С. Соломенко РАН, 2022. Т. 2. С. 215–220.

21. Кунашев Д.А., Алакулов А.А., Рахаев А.Х. Адресное пространство IPV4 – IP-геолокация // Международная научная конференция студентов, аспирантов и молодых ученых «Перспектива–2021» (Эльбрус, Россия, 23–30 апреля 2021). Эльбрус, 2021. Т. III. С. 295–297.

22. Hufaker B., Fomenkov M., claffy kc. Geocompare: a comparison of public and commercial geolocation databases. 2011. URL: https://www.caida.org/catalog/papers/2011_geocompare_tr/geocompare-tr.pdf (дата обращения 13.09.2023)

23. Лизнева Ю.С., Кокорева Е.В., Костюкович А.Е. Прогнозирование местоположения мобильного абонента в сети // Вестник СибГУТИ. 2022. № 3(59). С. 101–111. DOI:10.55648/1998-6920-2022-16-3-101-111

24. Gouel M., Vermeulen K., Fourmaux O., Friedman T., Beverly R. IP Geolocation Database Stability and Implications for Network Research. 2021. URL: https://hal.science/hal-03419874 (дата обращения 13.09.2023)

25. iPapi AP. URL: https://ipapi.com (дата обращения 12.04.2023)

26. Сорокин М.А., Курило А.А., Кузин П.И. Модель процесса анализа служебного трафика при управлении безопасностью информационной сети // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2021. № 1–2(151–152). С. 67–73.

27. Медведев Ю.С., Терехов В.В. Особенности построения распределенной корпоративной сети предприятия для обеспечения информационными и вычислительными ресурсами // XII Международная научно-практическая конференция «Научные чтения имени профессора Н.Е. Жуковского» (Краснодар, Россия, 22–23 декабря 2021) Краснодар: Общество с ограниченной ответственностью "Издательский Дом – Юг", 2022. С. 258–260.

28. Measures of distance between samples: Euclidean. URL: http://www.econ.upf.edu/~michael/stanford/maeb4.pdf (дата обращения 20.05.2023)

29. Li Z. Levin D., Spring N., Bhattacharjee B. Internet anycast: performance, problems, & potential // Proceedings of the Conference of the ACM Special Interest Group on Data Communication (SIGCOMM '18, Budapest, Hungary, 20–25 August 2018). New York: ACM, 2018. PP. 59–73. DOI:10.1145/3230543.3230547

30. Шевченко А.А. Модель процесса защиты информационно-телекоммуникационной сети от несанкционированного воздействия // Всеармейская научно-практическая конференция «Инновационная деятельность в Вооруженных Силах Российской Федерации» (Санкт-Петербург, Россия, 10–11 октября 2019). СПб.: Военная академия связи имени Маршала Советского Союза С.М. Буденного МО РФ, 2019. С. 166–173.

31. Задбоев В.А., Мелехов К.В., Петренко М.И., Комов А.А., Липатников В.А., Парфиров В.А. Средство определения в сети передачи данных цепочки маршрутов до географического местоположения нарушителя. Свидетельство о регистрации программы для ЭВМ № RU 2023614977 от 01.03.2023. Опубл. 09.03.2023.

References*:*

1. Morkovkin Ye.A., Novichikhina A.A., Zamulin I.S. IP-addressing and information security. *Bulletin of the Khakass State University. N.F. Katanov*. 2022;1(39):9–12.
2. Ivanov M., Polunin A. Improving the accuracy of IP geolocation based on public ip geoservices data. *Informatics and Automation*. 2022;21(4):758–785. DOI:10.15622/ia.21.4.5
3. Lipatnikov V.A., Shevchenko A.A., Melekhov K.V., Zadboev V.A. Method of detecting the geographical location of the information security intruder in the data network. *Proceedings of the IInd All-Russian Scientific and Technical Conference on State and Prospects of Development of Modern Science in the Direction of "IT-Technologies", 23–24 March 2023, Anapa, Russia, vol.2*. Anapa: Military Innovation Technopolis "ERA" Publ.; 2023. PP. 178–183.
4. Aljumaily M. *Content Delivery Networks Architecture, Features, and Benefits*. 2016. DOI:10.13140/RG.2.1.1762. 0722
5. Arif M.J., Karunasekera S., Kulkarni S., Gunatilaka A., Ristic B. Internet Host Geolocation Using Maximum Likelihood Estimation Technique. *Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, 20–23 April 2010, Perth, Australia*. IEEE; 2010. p.422–429. DOI:10.1109/AINA.2010.139
6. Lipatnikov V.A., Shevchenko A.A. The Vulnerability Control Method Applying While Automated Integrated Structure Organization Management System Scaling. *Information Systems and Technologies*. 2016;2(94):128–140.
7. Williams J. *Identification of IP address using fraudulent geolocation data*. 2020. URL: https://www.imperial.ac.uk/media/imperial-college/faculty-of-engineering/computing/public/1920-ug-projects/Williams,-James-%28jw1317%29.pdf [Accessed 13.09.2023]
8. Wang Z., Li H., Li Q., Li W., Zhu H., Sun L. Towards IP geolocation with intermediate routers based on topology discovery. *Cybersecurity*. 2019;2:13. DOI:10.1186/s42400-019-0030-2
9. Hufaker B., Fomenkov M., Claffy K. *Geocompare: a comparison of public and commercial geolocation databases*. 2011. URL: https://api.semanticscholar.org/CorpusID:13521646 [Accessed 13.09.2023]
10. Pratap U., Canudas-de-Wit C., Garin F. Average state estimation in presence of outliers. *Proceedings of the 59th IEEE Conference on Decision and Control, CDC, 14–18 December 2020, Jeju, South Korea*. IEEE; 2020. p.6058–6063. DOI:10.1109/CDC42340.2020.9303809
11. Shevchenko A.A. Mathematical model of information confrontation of two systems in information and telecommunication space. *Proceedings of the All-Army Scientific and Practical Conference on Innovative Activity in the Armed Forces of the Russian Federation, 14–15 October 2020, St. Petersburg, Russia*. St. Petersburg: Military Academy of Communications Publ.; 2020. p.237–241.
12. Zhao F., Luo X., Gan Y., Zu S., Cheng Q., Liu F. IP Geolocation based on identification routers and local delay distribution similarity. *Concurrency and Computation: Practice and Experience*. 2018;31(22). DOI:10.1002/cpe.4722
13. Lipatnikov V.A., Shevchenko A.A., Yatskin A.D., Semenova E.G. Information Security Management of Integrated Structure Organization Based on a Dedicated Server with Container Virtualization. *Information and Control Systems.* 2017;4:67–76. DOI:10.15217/issn1684-8853.2017.4.67
14. *Top 10 Best IP Geolocation APIs (in 2022).* URL: https://rapidapi.com/blog/ip-geolocation-api [Accessed 13.09.2023]
15. Semiu O.A. *Migration of IPv4 to IPv6; Translation Method.* 2018. URL: https://www.researchgate.net/publication/345727747_Migration_of_IPv4_to_IPv6_Translation_Method [Accessed 13.09.2023]
16. Taylor J., Devlin J., Curran K. Bringing location to IP Addresses with IP Geolocation. *Journal of Emerging Technologies in Web Intelligence*. 2012;4(3):273–277.
17. Lipatnikov V.A., Chepelev K.V., Shevchenko A.A. *Method of Protecting an Information Network from Intrusions*. Patent RF. 2705773 C1, 11.11.2019.
18. Padmanabhan V.N., Subramanian L. An investigation of geographic mapping techniques for internet hosts. *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM, 24–26 October 2023, San Diego, USA*. p.173–185. New York: ACM; 2001. DOI:10.1145/383059.383073
19. Luckie M., Dhamdhere A., Huffaker B., Clark D., claffy kc. bdrmap: Inference of Borders between IP Networks. *Proceedings of the 2016 Internet Measurement Conference, IMC '16, 14–16 November 2016, Santa Monica, USA*. New York: ACM; 2016. PP. 381–396. DOI:10.1145/2987443.2987467
20. Lipatnikov V.A., Melekhov K.V., Zadboev V.A. A Method of Detection of an Intruder's Location in the Data Network of the Network Infrastructure. *Proceedings of the International Scientific and Practical Conference on Transport of Russia: Problems and Prospects, 09–10 November 2022, St. Petersburg, Russia, vol.2*. St. Petersburg: N.S. Solomenko Institute of Transport Problems RAS; 2022. p.215–220.
21. Kunashev D.A., Alakulov A.A., Rakhaev A.Kh. Address space IPV4 – IP-geolocation. *Proceedings of the International Scientific Conference of Students, Graduate Students and Young Scientists «Perspektiva–2021», 23–30 April 2021, Elbrus, Russia*. Elbrus, 2021. vol.III. p.295–297.
22. Hufaker B., Fomenkov M., claffy kc. *Geocompare: a comparison of public and commercial geolocation databases*. 2011. URL: https://www.caida.org/catalog/papers/2011_geocompare_tr/geocompare-tr.pdf [Accessed 13.09.2023]
23. Lizneva Ju. S., Kokoreva E.V., Kostyukovich A.E. Predicting the location of a mobile subscriber in the network. *The Herald of the Siberian State University of Telecommunications and Information Science*. 2022;3(59):101–111. DOI:10.55648/1998-6920-2022-16-3-101-111
24. Gouel M., Vermeulen K., Fourmaux O., Friedman T., Beverly R. *IP Geolocation Database Stability and Implications for Network Research*. 2021. URL: https://hal.science/hal-03419874 [Accessed 13.09.2023]
25. iPapi AP. URL: https://ipapi.com [Accessed 12.04.2023]
26. Sorokin M.A., Kurilo A.A., Kuzin P.I. Service Traffic Analysis Process Model for Information Network Security Management. Military Energy. *Scientific and Technical Journal. Counter-terrorism technical devices.Issue 16***.** 2021;1-2(151-152):67–73.

27. Medvedev Yu.S., Terekhov V.V. Features of building a distributed corporate network of an enterprise to provide information and computing resources. *Proceedings of the XII International Scientific and Practical Conference "Scientific readings named after Professor N.E. Zhukovsky", 22–23 December 2021, Krasnodar, Russia*. Krasnodar: Publishing House – South, 2022. p.258–260.

28. Measures of distance between samples: Euclidean. URL: http://www.econ.upf.edu/~michael/stanford/maeb4.pdf [Accessed 20.05.2023]

29. Li Z., Levin D., Spring N., Bhattacharjee B. Internet anycast: performance, problems, & potential. *Proceedings of the Conference of the ACM Special Interest Group on Data Communication, SIGCOMM '18, 20–25 August 2018, Budapest, Hungary*. New York: ACM; 2018. p.59–73. DOI:10.1145/3230543.3230547

30. Shevchenko A.A. A model of the process of protecting an information and telecommunications network from unauthorized influence. *Proceedings of the All-Army Scientific and Practical Conference on Innovative Activity in the Armed Forces of the Russian Federation, 10–11 October 2019, St. Petersburg, Russia*. St. Petersburg: Military Academy of Communications Publ.; 2019. p.166–173.

31. Zadboev V.A., Melekhov K.V., Petrenko M.I., Komov A.A., Lipatnikov V.A., Parfirov V.A., et al. *Means of Determining the Chain of Routes in the Data Transmission Network to the Geographical Location of the Offender*. Patent RF, no 2023614029, 01.03.2023.

Статья поступила в редакцию 14.06.2023; одобрена после рецензирования 18.07.2023; принята к публикации 25.07.2023.
The article was submitted 14.06.2023; approved after reviewing 18.07.2023; accepted for publication 25.07.2023.

Информация об авторах:

ЛИПАТНИКОВ Валерий Алексеевич
доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С.М. Буденного
https://orcid.org/0000-0002-3736-4743

ЗАДБОЕВ Вадим Александрович
оператор роты (научной) научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С.М. Буденного
https://orcid.org/0009-0003-9362-1307

МЕЛЕХОВ Кирилл Витальевич
адъюнкт научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С.М. Буденного
https://orcid.org/0009-0007-3474-412X

ШЕВЧЕНКО Александр Александрович
кандидат технических наук, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С.М. Буденного
https://orcid.org/0000-0001-9113-1089