DOI 10.36622/VSTU.2023.26.1.013
УДК 004.056

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ НАРУШЕНИЯ ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ ИНФОРМАЦИИ В БЕСПРОВОДНОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СВЯЗИ С УЧЕТОМ КООРДИНАТ, РАССТОЯНИЯ МЕЖДУ ЕЁ АБОНЕНТАМИ И ИХ ВЛИЯНИЯ ДРУГ НА ДРУГА

А.В. Гречишкин, Е.А. Гулидова, В.А. Краснопольская, Ю.В. Завгородняя, Е.А. Москалева

В данной статье предлагается методика количественной оценки и регулирования рисков нарушения целостности и доступности информации, циркулирующей в беспроводной телекоммуникационной сети связи. Данная методика основана на применении теории сложных сетей для определения ключевых узлов сети и на применении модели дерева атак для оценки вероятности атаки. Разработаны алгоритмы для количественной оценки и регулирования рисков в момент возможной реализации атаки. Регулирование рисков происходит путем регулирования частот работы приемников и передатчиков абонентов сети с учетом координат, расстояний между абонентами и их влияния друг на друга. Представлен программно-технический комплекс, позволяющий путем статистических экспериментов сравнивать конфигурации сети и выбирать квазиоптимальные значения относительно риска с точки зрения риска успешной реализации атаки на целостность и доступность в беспроводной сети связи.

Ключевые слова: программно-технический комплекс, беспроводная телекоммуникационная сеть связи, риск, оценка, регулирование, защищенность, целостность, доступность.

Введение

В условиях информатизации и сетевых операций беспроводные телекоммуникационные сети связи сталкиваются с серьезными угрозами. Любое устройство в рамках беспроводной сети должно получать информацию в режиме реального времени и обмениваться ею. В свою очередь, активное развитие полупроводниковых технологий и технологии интернета вещей приводит к росту количества радиосредств в эфире [1]. Увеличение количества радиосредств приводит к неконтролируемому влиянию их друг на друга и загруженности эфира связи. В этом процессе проблема информационной безопасности беспроводной сети связи особенно важна; обеспечение целостности и доступности передаваемой информации может в значительной степени гарантировать бесперебойное выполнение задачи. В данном вопросе обеспечение конфиденциальности не является главной целью, так как в отличие от двух других критериев защиты информации, затраты на нарушение конфиденциальности выше и требования к осуществлению атак на нее серьезнее.

В настоящее время существует множество работ, связанных с исследованием информационной безопасности беспроводных телекоммуникационных сетей, например, [2,3]. Традиционная оценка рисков информационной безопасности в основном включает в себя качественный и количественный анализ. Однако исследования существующих методов традиционной оценки рисков [4-7] в качественных и количественных методиках не подходят для всех беспроводных телекоммуникационных сетей связи из-за ограниченности открытой и доступной информации о них. Введя в исследование новые факторы, такие как координаты абонентов, максимально возможные расстояния между абонентами и влияние продуктов интермодуляции в сети, а также, назначив частоты для передатчиков и приемников, можно более детально провести анализ рисков и в последующем регулировать их.

Луо и другие в своей методике [8] предлагают использовать теорию сложных сетей и модель дерева атаки для количественной оценки рисков.

В исследовании используют определение ключевых узлов в сложных сетях. По причине существования множества объектов и способов связи для беспроводной телекоммуникационной сети, в них легко создавать помехи и уничтожать информацию. Более того, поскольку передаваемая информация может проходить через множество блоков и этапов, помехи между объектами сети могут иметь несколько уровней каскадного сбоя. Определение ключевых узлов направлено на более детальное изучение сложных сетей и помогает повысить надежность и неуязвимость всей сети.

Недостатком данной методики является то, что она рассматривает только угрозы и атаки, исходящие от преднамеренного злоумышленника, не затрагивая угрозы и атаки, возникающие непреднамеренно.

Несмотря на новый подход к исследованию рисков, в ней не учитывается влияние частот между приемниками и передатчиками абонентов сети. В настоящей статье предлагается выбирать частоты, опираясь на особенности распространения радиоволн в ограниченном диапазоне. Это позволит минимизировать риски нарушения целостности и доступности информации в рассматриваемой беспроводной телекоммуникационной сети связи.

Недостатком данной методики является то, что она рассматривает только угрозы и атаки, исходящие от злоумышленника, не затрагивая угрозы и атаки, возникающие непреднамеренно.

Целью данной статьи, с учетом описанной выше ситуации, является предложение новой методики оценки и регулирования рисков, основанной на количественном анализе и оценке ключевых узлов сложных сетей в сочетании с моделью дерева атак в беспроводных телекоммуникационных сетях связи.

Для этого требуется выполнить следующее: построение расширенного дерева атак, содержащее в себе ветви, отображающие путь атаки для преднамеренного и непреднамеренного злоумышленников; рассмотрение сценариев атаки для непреднамеренного злоумышленника:

- обеспечение связи там, где её не должно быть;
- отсутствие связи там, где она должна быть.

Для достижения цели необходимо решить задачи:

- разработать методическое и алгоритмическое обеспечение оценки рисков нарушения целостности и доступности информации, передаваемой по беспроводным телекоммуникационным сетям, в зависимости от координат абонентов;
- разработать методическое и алгоритмическое обеспечение регулирования рисков нарушения целостности и доступности информации, передаваемой по беспроводным телекоммуникационным сетям, в зависимости от координат абонентов.

Методика оценки и регулирования рисков в беспроводной сети связи

Наиболее значимой частью регулирования рисков является оценка рисков информационной безопасности. Величина риска R используется для количественной оценки риска опасности события:

$$R(U) = U \times P(U),$$

где U – значение ущерба;

$P(U)$ – вероятность наступления атаки;

Для беспроводной телекоммуникационной сети связи риск информационной безопасности в процессе связи определяется двумя факторами, а именно значением вероятности атаки P в процессе связи и степенью важности узла, осуществляющего связь с устройством сети. Чем выше вероятность быть подвергнутым атаке в процессе связи, тем выше будут риски информационной безопасности. Аналогично, чем выше степень важности узла в сети, тем выше влияние на всю сеть после прекращения связи с узлом и тем выше значение риска.

Для вычисления воздействия ущерба U предлагается использовать теорию сложных сетей.

В первую очередь необходимо рассчитать значение ущерба U, используя построенную модель связи между абонентами, чтобы определить все ключевые узлы и построить матрицу связности для абонентов.

Матрица связности определяется следующим образом:

$$\delta_{\text{идеал}} = \begin{matrix} \\ \nu_1 \\ \nu_2 \\ \cdots \\ \nu_n \end{matrix} \begin{matrix} \begin{matrix} \nu_1 & \nu_2 & \dots & \nu_n \end{matrix} \\ \begin{bmatrix} 0 & \delta_{12} & \vdots & \delta_{1n} \\ \delta_{21} & 0 & \vdots & \delta_{2n} \\ \cdots & \cdots & \ddots & \cdots \\ \delta_{n1} & \delta_{n2} & \dots & 0 \end{bmatrix} \end{matrix},$$

где n – количество узлов в сети,

ν_i– узлы сети, $i = 1 \dots n$,

δ_{ij} – соединение между узлами i и j,

$$\delta_{ij} = \begin{cases} 1, \text{если узел } i \text{ напрямую подключен к узлу } j, \\ 0, \text{если узел } i \text{ напрямую не подключен к узлу } j. \end{cases}$$

Благодаря построенной матрице связности можно определить эффективность узла. Эффективность узла представляет собой уровень сложности узла для других узлов, а значение эффективности узла тем больше, чем более важное положение узла в процессе передачи сетевой информации.

Вычисляется эффективность узла I_i следующим образом:

$$I_i = \frac{1}{n-1} \sum_{i=0, i \neq j}^{n-1} \frac{1}{d_{ij}},$$

где n – количество узлов в сети;

d_{ij} – расстояние между узлами i и j.

Степень узла D_i представляет собой количество связанных с выбранным узлом остальных узлов. Чем больше значение степени, тем больше количество узлов, непосредственно связанных с рассматриваемым узлом, и тем больше значение соответствующего узла.

D_i и I_i используются для построения матрицы важности узлов H, где H структурирована следующим образом:

$$H = \begin{matrix} \\ \nu_1 \\ \nu_2 \\ \cdots \\ \nu_n \end{matrix} \begin{matrix} \begin{matrix} \nu_1 & \nu_2 & \cdots & \nu_n \end{matrix} \\ \begin{bmatrix} I_1 & \delta_{12} D_2 I_2 / k & \vdots & \delta_{1n} D_n I_n / k \\ \delta_{21} D_1 I_1 / k & I_2 & \vdots & \delta_{2n} D_n I_n / k \\ \cdots & \cdots & \ddots & \cdots \\ \delta_{n1} D_1 I_1 / k & \delta_{n2} D_2 I_2 / k & \dots & I_n \end{bmatrix} \end{matrix},$$

где $\nu_1, \nu_2, \dots, \nu_n$ – узлы сети;

$D_1, D_2, \dots, D_n$ – степени узлов,

$I_1, I_2, \dots, I$ – эффективности узлов,

δ_{ij} – соединение между узлами i и j,

k – среднее значение всех степеней узла в сети.

Тогда ущерб от атаки U на узел сети может быть определен так:

$$U = I_i \times \frac{t_{\text{оо}}}{t_{\text{р}}} \times \sum_{j-1, i \neq j}^{n} \frac{\delta_{ij} D_j I_j}{k},$$

где $t_{\text{оо}}$ – время, когда абонент находится в состоянии отказа в обслуживании,

$t_{\text{р}}$ – общее время работы абонента.

В статье рассматривается момент, когда система находится в отказе, таким образом

$$t_{\text{оо}}/t_{\text{р}} = 1.$$

Каждое сообщение, передаваемое в исследуемой беспроводной телекоммуникационной сети связи насколько важно, что даже незначительное его повреждение злоумышленниками приводит к реализации атаки на целостность.

Для определения вероятности атаки P используется модель дерева атак. Каждая ветвь в таком дереве представляет собой путь атаки, а вероятность возникновения корневого узла определяется вероятностью возникновения события конечного узла и путем атаки.

Общая модель дерева атаки на i-го абонента представлена на рис. 1.

В дереве рассматривается атака типа «отказ в обслуживании» на i-го абонента сети. Ветвь, отвечающая за вероятность возникновения атаки нарушения конфиденциальности также представлена в дереве и принимается за нуль:

$$P_{\text{да}} = const = 0.$$

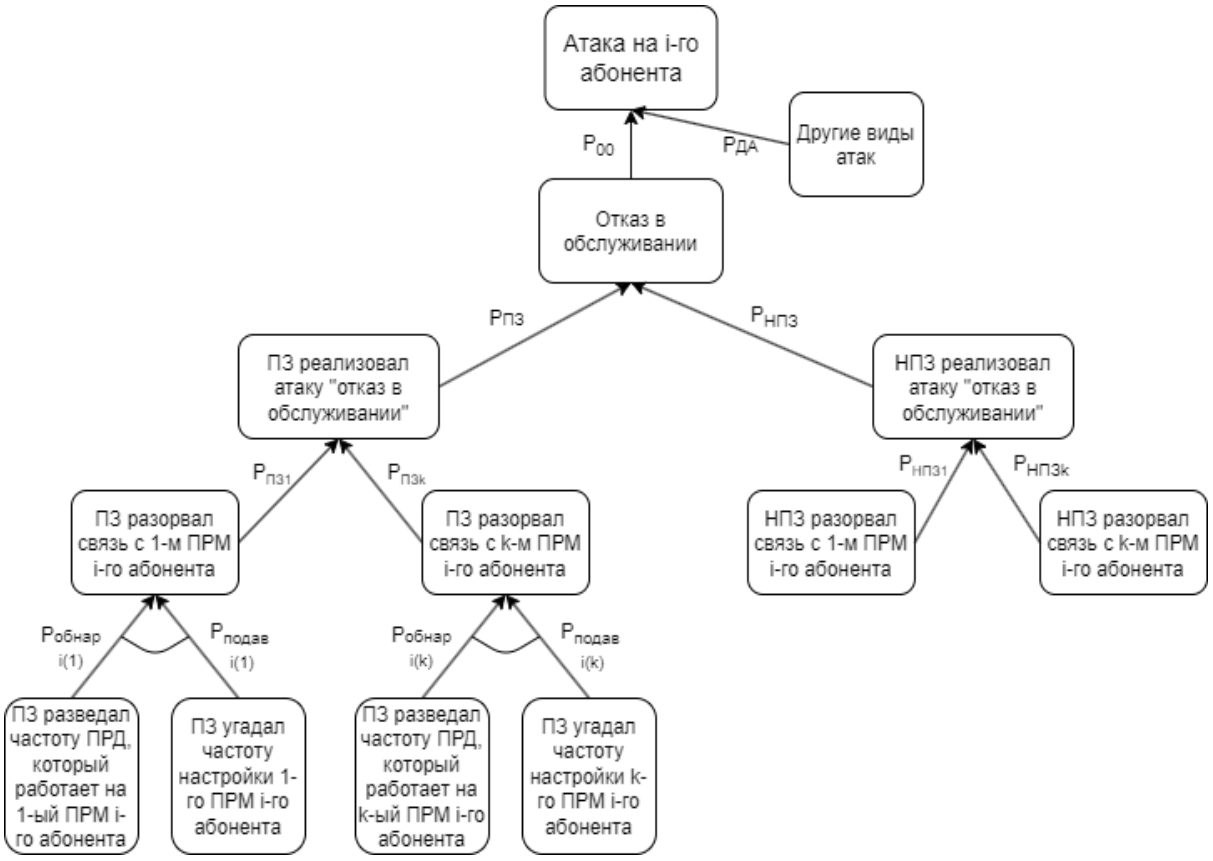

Рис. 1. Модель дерева атак на i-го абонента беспроводной телекоммуникационной сети

Злоумышленник (преднамеренное воздействие) может действовать по следующим сценариям:

- разведать частоту передатчика, который работает на приемник абонента в беспроводной сети связи;
- угадать частоту настройки приемника абонента в беспроводной сети связи.

Вероятность того, что злоумышленник выполнит свою задачу (определит частоту приемника), определяется следующим образом:

$$P_{\text{пз}} = \frac{S_{\text{прд}}^{j-i(k)}}{S_{\text{рр}}},$$

где $P_{\text{пз}}$ – вероятность того, что злоумышленник определит частоту приемника,

$S_{\text{прд}}^{j-i(k)}$ – площадь покрытия передатчика j-го абонента, который организовывает связь с k-ым приемником i-го абонента;

$S_{\text{рр}}$ – общая площадь района размещения абонентов сети.

В ином случае, если частота была угадана, вероятность совершения атаки будет рассчитываться так:

$$P_{\text{подавл}}^{i(k)} = P_{\text{подавл}} = \frac{1}{N_{f\text{прд}} - 1},$$

где $P_{\text{подавл}}^{i(k)} = P_{\text{подавл}}$ – вероятность совершения атаки злоумышленником, т. е. вероятность подавления узла связи,

$N_{f\text{прд}}$ – общее количество частот передатчиков, требуемое для организации сети с заданной связностью.

Существует ряд допущений, относящихся к атакам злоумышленника.

1. Количество злоумышленников не ограничено, вследствие чего рядом с каждым передатчиком сети может размещаться злоумышленник, который с определенной вероятностью $P_{\text{пз}}$ имеет возможность разведать частоту работы передатчика. Рядом с приемником также может находиться злоумышленник, который с вероятностью $P_{\text{подавл}}$ может его уничтожить.

2. Все злоумышленники связаны друг с другом и могут передавать информацию о разведанных частотах передатчиков сети друг другу.

3. Время реакции злоумышленника представлено в идеальном варианте: $t_p = 0$, значит, он разведывает частоты передатчика, обменивается информацией и воздействует на приемник объектов сети мгновенно.

Однако злоумышленники имеют доступ не ко всей информации в сети связи:

1. Злоумышленники не обладают доступом к информации о местоположении размещения абонентов сети.

2. Несмотря на то, что количество злоумышленников не ограничено, они не имеют информации о частотах настройки приемника абонентов сети, но существует отличная от нуля вероятность того, что злоумышленник вычислит частоту настройки приемника и уничтожит его.

Чтобы детально рассмотреть вероятность совершения атак злоумышленника на узды сети связи, стоит расширить дерево атак и подробнее описать ветвь, отвечающую за разрыв связи с k-м приемником i-го абонента. Ветвь дерева атак представлена на рис. 2.

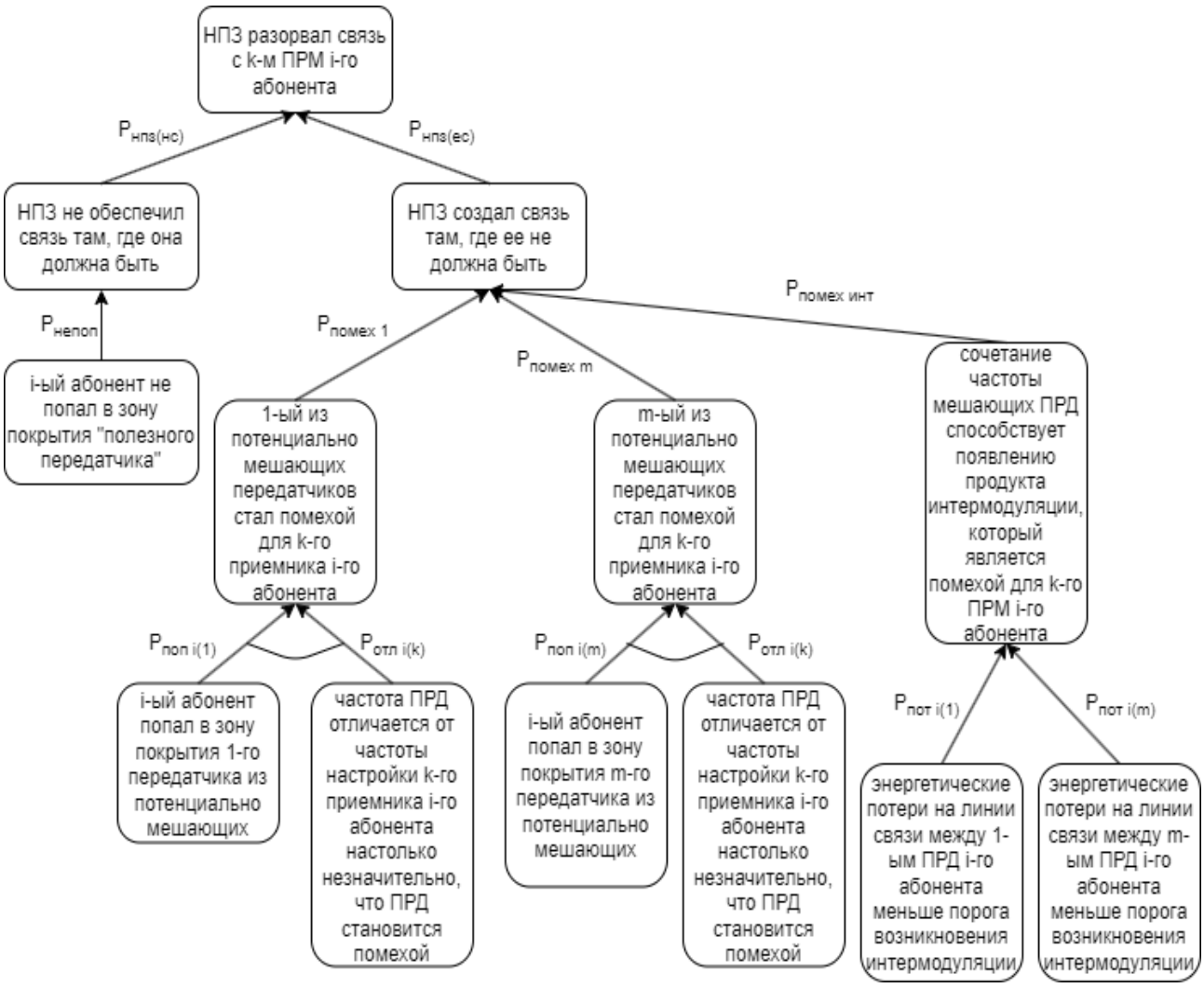

Рис. 2. Ветвь непреднамеренного злоумышленника в модели дерева атак на *i*-го абонента сети

Непреднамеренное воздействие может происходить по следующим сценариям:

- не обеспечивается связь там, где она должна быть: выбраны частоты приемника и передатчика, затухание при распространении радиоволн на которых превышает минимально необходимое;
- есть связь там, где ее не должно быть: частоты приемника и передатчика выбраны так, что до несвязных напрямую абонентов доходит мощность нежелательных передатчиков, вызывающая риск возникновения интермодуляции.

Вероятность того, что непреднамеренное воздействие (перегрузку абонента сети) проведет не связанный напрямую с абонентом сети приемник абонента, рассчитывается так:

$$P_{\text{нпз}} = P_{\text{связь}}\left(L_{\text{абон}}^{\text{НПЗ}}\left(f_{\text{ПРД}}^{\text{НПЗ}}, d_{\text{абон}}^{\text{НПЗ}}\right), L_{\text{порог}}\right) \times \frac{\frac{\Delta F}{2}}{\frac{\Delta F}{2} + \left|f_{\text{ПРМ}}^{\text{абон}} - f_{\text{ПРД}}^{\text{НПЗ}}\right|},$$

где $P_{\text{связь}}(L_{\text{абон}}^{\text{НПЗ}}(f_{\text{ПРД}}^{\text{НПЗ}}, d_{\text{абон}}^{\text{НПЗ}}), L_{\text{порог}})$ – функция вероятности того, что связь между i-ым абонентом и воздействующим узлом присутствует,

$L_{\text{абон}}^{\text{НПЗ}}(f_{\text{ПРД}}^{\text{НПЗ}}, d_{\text{абон}}^{\text{НПЗ}})$ – потери на линии связи i-го абонента и воздействующего узла;

$f_{\text{ПРД}}^{\text{НПЗ}}$ – частота настройки передатчика воздействующего узла сети, влияние которого оценивается, МГц,

$d_{\text{абон}}^{\text{НПЗ}}$ – расстояние между абонентом и воздействующим узлом, км,

$L_{\text{порог}}$ – пороговое значение потерь на линиях связи, выше которого связь обрывается (зависит от мощности передатчика и уровня чувствительности приемника),

ΔF – полоса пропускания приемника абонента, МГц;

$f_{\text{ПРМ}}^{\text{абон.}}$ – частота настройки приемника i-го абонента, МГц.

Эту вероятность можно интерпретировать следующим образом:

$$P_{\text{связь}}\left(L_{\text{абон}}^{\text{НПЗ}}\left(f_{\text{ПРД}}^{\text{НПЗ}}, d_{\text{абон}}^{\text{НПЗ}}\right), L_{\text{порог}}\right) = \begin{cases} 0, & L_{\text{абон}}^{\text{НПЗ}} > L_{\text{порог}}, \\ \dfrac{L_{\text{порог}} - L_{\text{абон}}^{\text{НПЗ}}}{L_{\text{порог}}}, & L_{\text{абон}}^{\text{НПЗ}} \le L_{\text{порог}}. \end{cases}$$

Вероятность возникновения угрозы нарушения целостности и доступности информации от интермодуляции i-го узла на j-ый узел вычисляется следующим образом:

$$P_{\text{сос}}^{\text{им}} = P_{\text{связи}}(L, L_2) \times P_{\text{св}}^{\text{им}},$$

где L – порог, определяющий потери на линиях связи,

L_2 – порог, который определяет интермодуляционную избирательность приемника.

Вероятность возникновения угрозы нарушения целостности и доступности информации от собственной интермодуляции абонента вычисляется так:

$$P_{\text{св}}^{\text{им}} = \frac{\frac{\Delta F}{2}}{\frac{\Delta F}{2} + \left|f^{\text{им}} - f_{\text{прм}}^{\text{абон}}\right|} \times \frac{1}{K},$$

где ΔF – полоса пропускания приемника абонента,

$f^{\text{им}}$ – частота, на которой происходит интермодуляция,

$f_{\text{ПРМ}}^{\text{абон.}}$ – частота настройки приемника i-го абонента,

K – порядок интермодуляции.

Благодаря известным значениям координат можно определить точное расстояние между соседними абонентами

$$r_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2},$$

где $(x_i,\ y_i)$, $(x_j,\ y_j)$ – координаты i-го и j-го абонентов сети,

и построить матрицу расстояний следующим образом:

$$r = \begin{array}{c} \\ \nu_1 \\ \nu_2 \\ \cdots \\ \nu_n \end{array} \begin{array}{c} \begin{array}{cccc} \nu_1 & \nu_2 & \cdots & \nu_n \end{array} \\ \begin{bmatrix} 0 & r_{12} & \vdots & r_{1n} \\ r_{21} & 0 & \vdots & r_{2n} \\ \cdots & \ldots & \ddots & \ldots \\ r_{n1} & r_{n2} & \ldots & 0 \end{bmatrix} \end{array},$$

где r_{ij}– расстояние между i-м и j-м абонентами сети.

Полученные расстояния необходимо сравнить с уже имеющимися максимально необходимыми расстояниями, известными по условию.

Для каждого из абонентов беспроводной телекоммуникационной сети связи существует минимально необходимое количество передатчиков и приемников, матрица оборудования для которых строится так:

$$N_{\text{прм}} = N_{\text{прд}} = \begin{array}{c} \\ \nu_1 \\ \nu_2 \\ \cdots \\ \nu_n \end{array} \begin{array}{c} \begin{array}{cccc} \nu_1 & \nu_2 & \cdots & \nu_n \end{array} \\ \begin{bmatrix} D_1 & 0 & \vdots & 0 \\ 0 & D_2 & \vdots & 0 \\ \cdots & \cdots & \ddots & \cdots \\ 0 & 0 & \cdots & D_n \end{bmatrix} \end{array},$$

где $D_1, D_2, \ldots, D_n$ – степени узлов в сети.

Матрицы распределения частот для приемников и передатчиков строятся на основе матрицы связности, т. е. частота будет назначена только тем приемникам и передатчикам, которые непосредственно связаны между собой:

$$f_{\text{прм}} = \begin{array}{c} \\ \nu_1 \\ \nu_2 \\ \cdots \\ \nu_n \end{array} \begin{array}{c} \begin{array}{cccc} \nu_1 & \nu_2 & \cdots & \nu_n \end{array} \\ \begin{bmatrix} 0 & f_{21} & \vdots & 0 \\ f_{12} & 0 & \vdots & f_{n2} \\ \cdots & \cdots & \ddots & \cdots \\ 0 & f_{2n} & \cdots & 0 \end{bmatrix} \end{array},$$

где f_{ij} – частота, назначенная приемнику.

$$f_{\text{прд}} = \begin{array}{c} \\ \nu_1 \\ \nu_2 \\ \cdots \\ \nu_n \end{array} \begin{array}{c} \begin{array}{cccc} \nu_1 & \nu_2 & \cdots & \nu_n \end{array} \\ \begin{bmatrix} 0 & f_{12} & \vdots & 0 \\ f_{21} & 0 & \vdots & f_{2n} \\ \cdots & \cdots & \ddots & \cdots \\ 0 & f_{n2} & \cdots & 0 \end{bmatrix} \end{array},$$

где f_{nn}– частота, назначенная передатчику.

Значение риска узла сети оценивается как произведение вероятности совершения атаки P на ущерб от этой атаки U. Следовательно, чтобы уменьшить значение риска, необходимо сократить значение вероятности, либо значение ущерба.

В представленной методике значение ущерба зависит от четырех переменных:

I_i – эффективности *i*-го узла;

δ_{ij} – соединения между *i*-м и *j*-м узлами;

D_i – степени *i*-го узла;

n – количества узлов в сети.

Каждая из этих переменных связана с моделью беспроводной телекоммуникационной сети связи и будет меняться только посредством изменения самой модели. Это говорит о том, что на ущерб влияет только сама сеть связи, а не дополнительные параметры и значение ущерба может уменьшиться или увеличиться только в том случае, если количество абонентов и связей между ними в сети изменится.

Следовательно, на количественное значение риска может повлиять только вероятность совершения атаки P. Значение вероятности атаки P может быть уменьшено так:

- для абонента с наибольшим количеством связей с другими абонентами, так как значение вероятности атаки для него будет изначально самым большим;

- для всей сети связи, благодаря чему значение вероятности атаки уменьшится для всех абонентов этой сети.

Благодаря случайному назначению частот при множественном проведении испытаний, можно выбрать эталонный вариант распределения. Количество опытов может варьироваться от 1 до десятков миллионов. Чем больше количество опытов, тем точнее будет количественная оценка результатов исследования, но тем дольше будет длиться эксперимент. Получить приблизительные значения можно и при небольшом количестве экспериментов (рекомендуется минимум 100 опытов), однако результаты не будут до конца показательными и не передадут всю картину целиком.

Оценка и регулирование рисков нарушения целостности и доступности беспроводной сети связи

Для оценки рисков рассмотрим простой случай в беспроводной телекоммуникационной сети связи, где имеются два абонента, между которыми происходит обмен сигналами при помощи двух приемников и передатчиков, работающих на разных частотах.

Для расчета необходимо учитывать параметры абонентов сети, в данном случае это мощность передатчиков всех абонентов $P_{прд}$ = 0,02 Вт, чувствительность приемников абонентов $U_{абн}$ = 10 мкВ, и чувствительность приемников абонентов к интермодуляции $U_{ИМ}$ = 10000 мкВ.

Длину и ширину района позиционирования выберем 100 км. Диапазон рассматриваемых частот варьируется от 40 МГц до 90 МГц, с шагом 2,5. Полоса пропускания приемников абонентов равна 1 МГц. Порядок гармонической составляющей,

учитываемый при расчете продуктов интермодуляции равен 3.

Также вводятся координаты абонентов: *x* = [40,60]; *y* = [40,60] (координаты для *i*-го абонента (40, 40), для *j*-го (60,60)).

При переборе частот существуют случаи, при которых при вычислении значений вероятностей атаки их значение P(U) = 1. Значение ущерба не ограничено и зависит от количества абонентов и связей между ними. В этом случае значение риска определяется значением ущерба *U* и равно ему. Этот случай предложен для статистического анализа, но не учитывается при расчётах, так как значение риска становится больше 1.

При проведении эксперимента было исследовано 676 выборок. Из них 324 имеют позитивный исход, т. е. связь присутствует там, где она должна быть. На основе данных построены гистограммы, показанные на рис. 3.

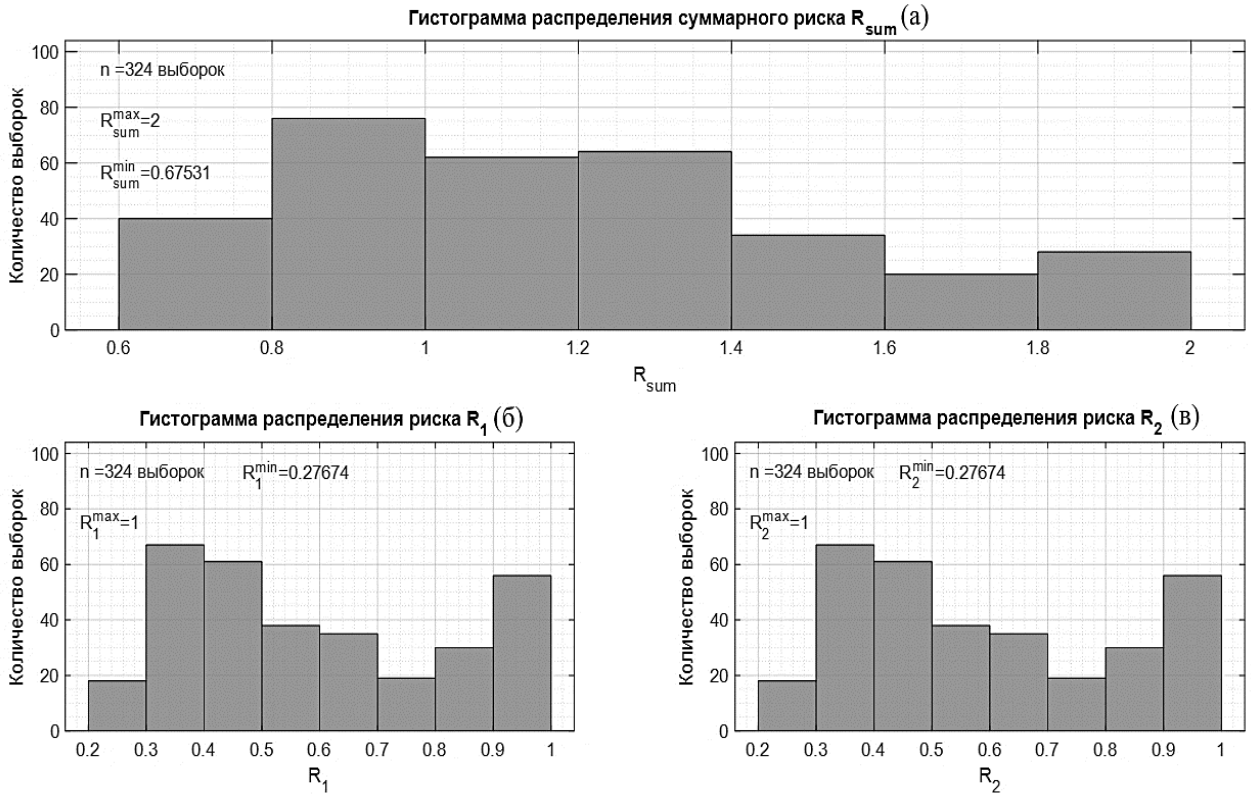

Рис. 3. Гистограммы распределения: а) суммарного риска R_{sum}, б) риска R_1, в) риска R_2

По полученным гистограмм можно сделать вывод, что для первого и второго абонентов минимальный риск составляет $R_{1,2}^{min} = 0{,}27674$. Наибольшее количество выборок подвержены риску в диапазоне от 0,3 до 0,5. Наибольший риск $R_{1,2}^{max} = 1$ и ему подвержены 56 выборок. Суммарный максимальный риск $R_{sum}^{max} = 2$. Суммарный минимальный риск $R_{sum}^{min} = 0{,}67531$.

На рис. 4 представлены функции распределения риска для абонентов сети и суммарный риск.

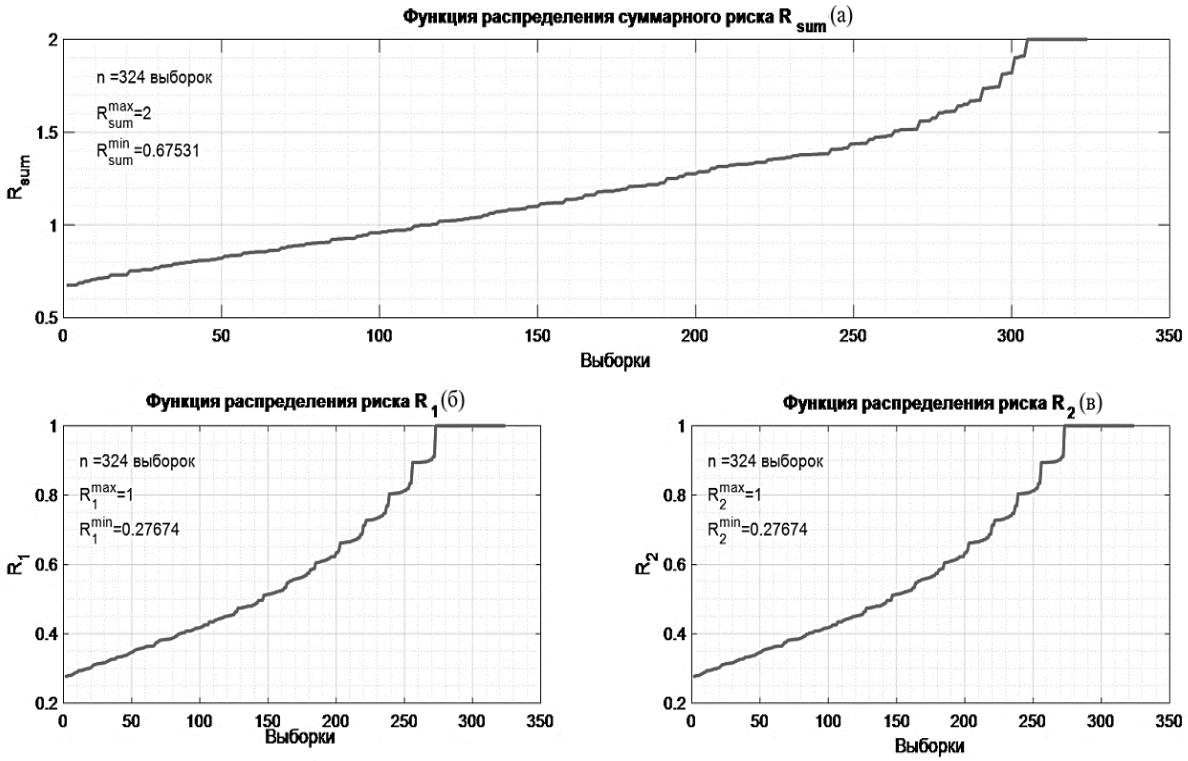

Рис. 4. Функции распределения: а) суммарного риска R_{sum}; б) риска R_1; в) риска R_2

Из этого следует, что для каждого абонента сети можно построить схему ландшафта опасности реализации в отношении его атак (рис. 5). В дальнейшем появится возможность сконцентрировать внимание на наиболее опасных сочетаниях «вектор атаки – уязвимость».

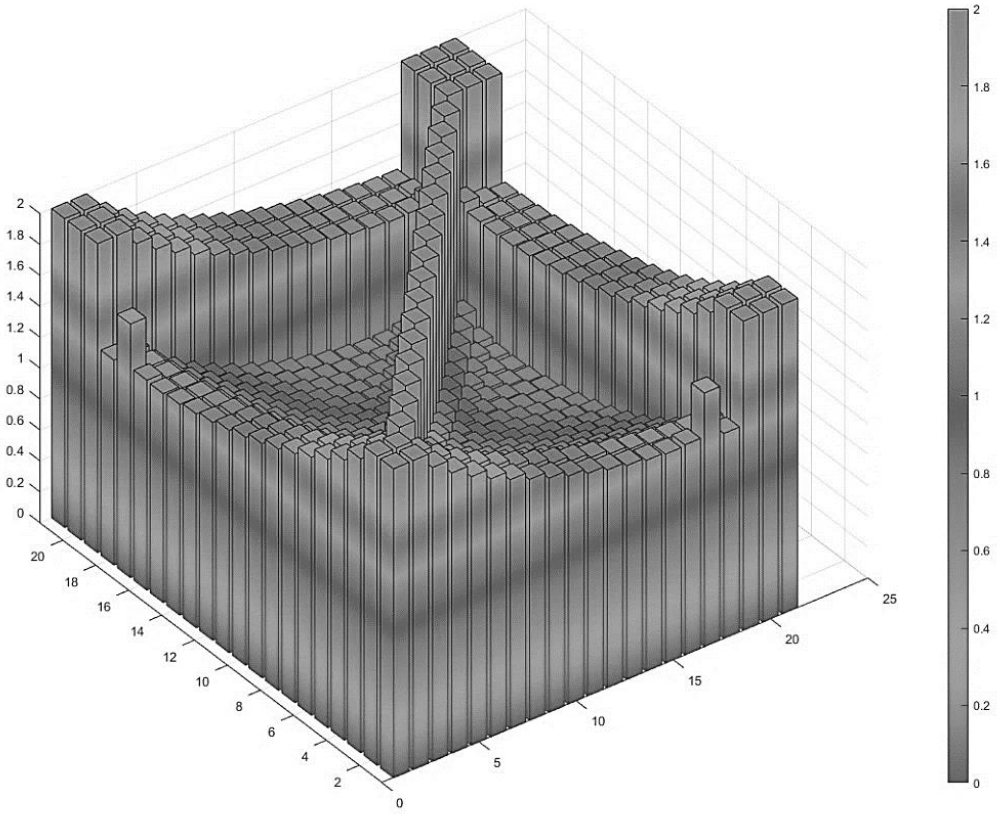

Рис. 5. Риск-ландшафт реализации атак на абонентов сети

Исходя из полученных данных по оценке риска, для его регулирования были выбраны рабочие квазиоптимальные значения частот с минимальным ущербом, с учетом координат абонентов, максимального расстояния между ними и интермодуляционной избирательности передатчиков (рис. 6):

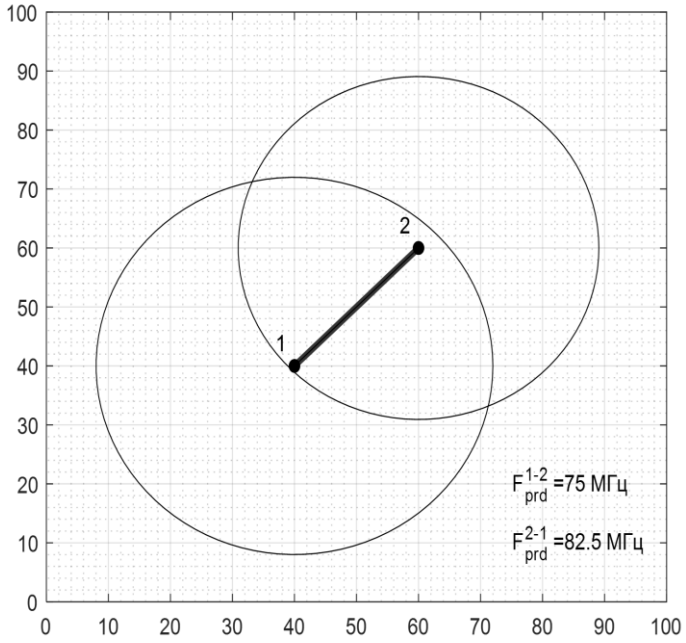

Рис. 6. Квазиоптимальные значения частот для минимизации рисков для абонентов 1 и 2

Для сбора статистических данных был проведен дополнительный эксперимент. Количество выборок увеличено до 251001, а длина шага уменьшена в 25 раз. Позитивных исходов выявлено $N_{поз}$ = 201601.

Гистограммы распределения рисков абонентов и суммарного риска представлены на рис. 7. Суммарный максимальный риск и минимальный риск абонентов уменьшились. Наибольшее количество выборок, подверженных риску, находятся в диапазоне от 1,34 до 1,36. Наибольший риск $R_{1,2}^{max} = 1$ и ему подвержены 13500 выборок. Суммарный максимальный риск $R_{sum}^{max} = 2$. Суммарный минимальный риск $R_{sum}^{min} = 0{,}64151$.

На рис. 8 представлены функции распределения риска для абонентов сети и их суммарный риск.

На рис. 9 представлен вариант квазиоптимального решения по назначению рабочих частот с минимальным риском нарушения доступности и целостности информации между абонентами.

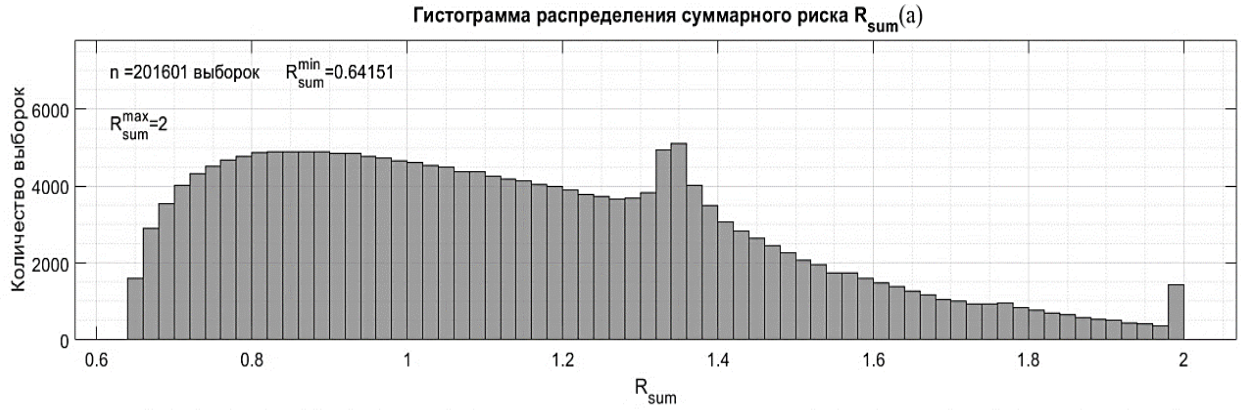

Рис. 7, а). Гистограмма распределения суммарного риска R_{sum}

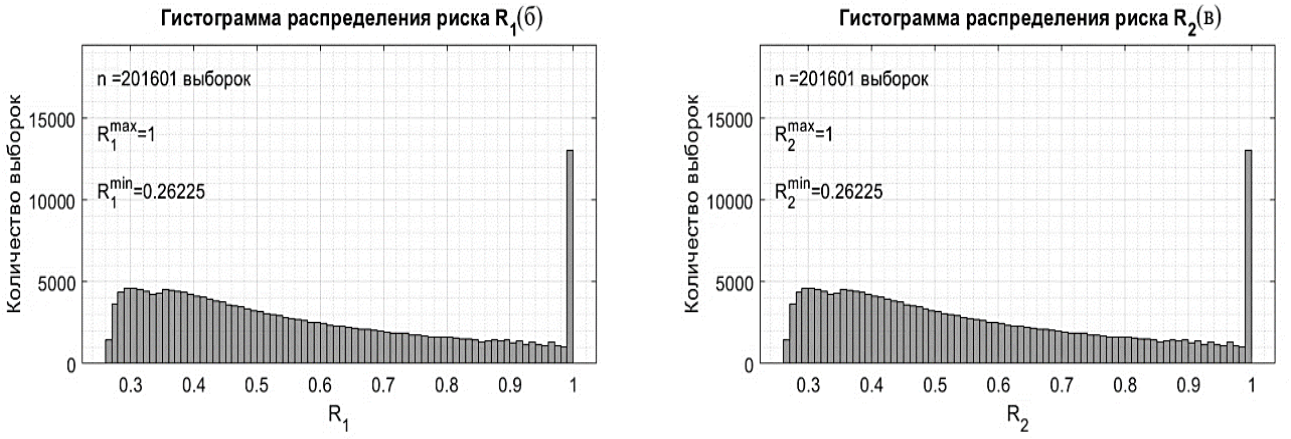

Рис. 8, б), в). Гистограммы распределения: б) риска R_1; в) риска R_2

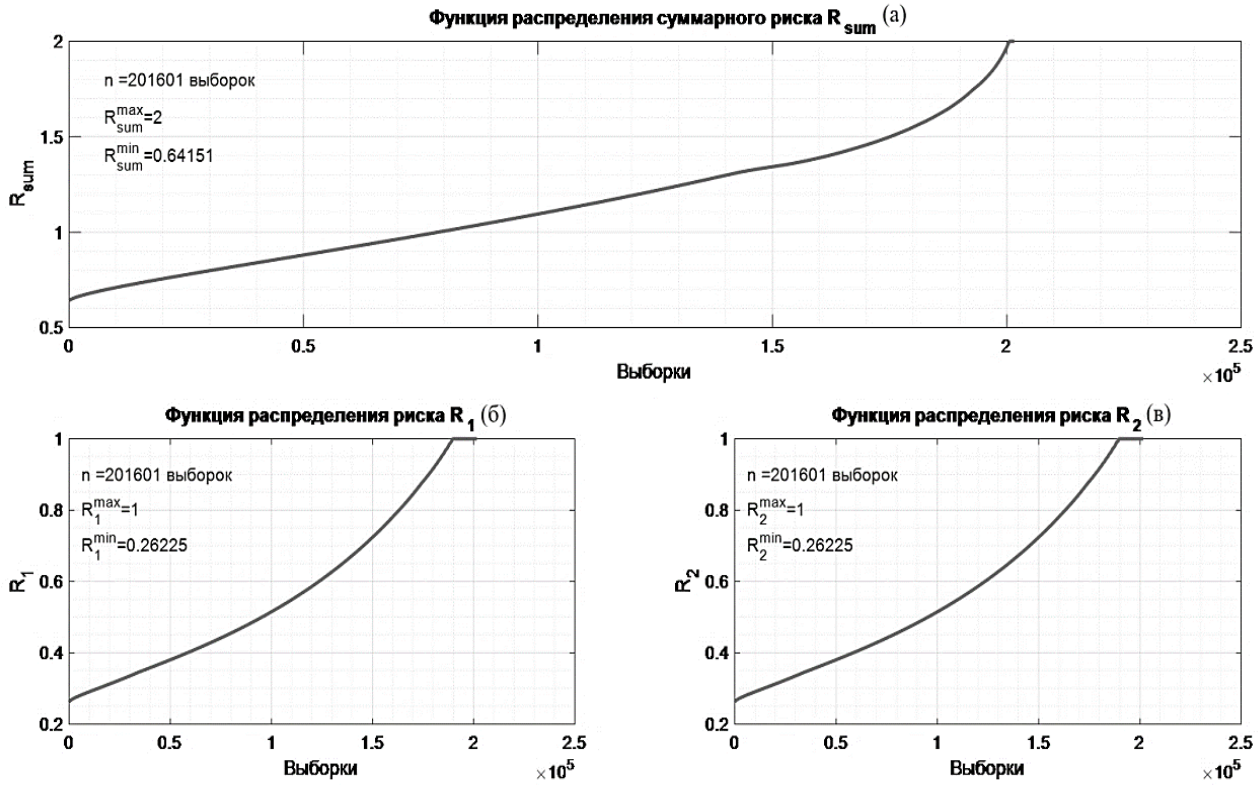

Рис. 9. Функции распределения: а) суммарного риска R_{sum}; б) риска R_1; в) риска R_2

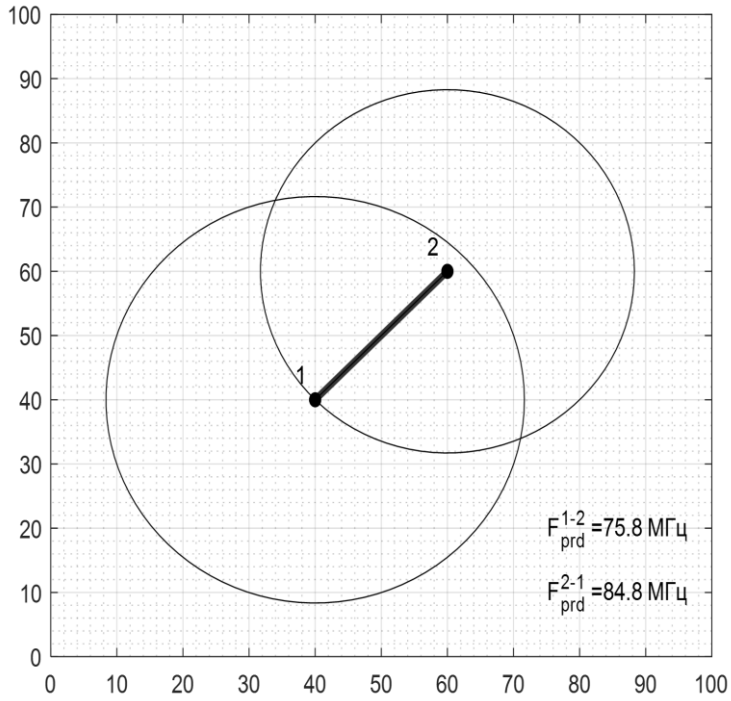

Рис. 10. Квазиоптимальные значения частот для минимизации рисков для абонентов 1 и 2

Стоит также рассмотреть более сложный вариант для оценки и регулирования рисков. Есть беспроводная телекоммуникационная сеть связи, состоящая из шести абонентов. Характеристики передатчиков и приемников остаются неизменными. Заданы новые координаты для абонентов: x = [40,40,60,30,40,50]; y = [70,25,90,20,10,20]. Длина шага равна 1. Схема сети представлена на рис. 10.

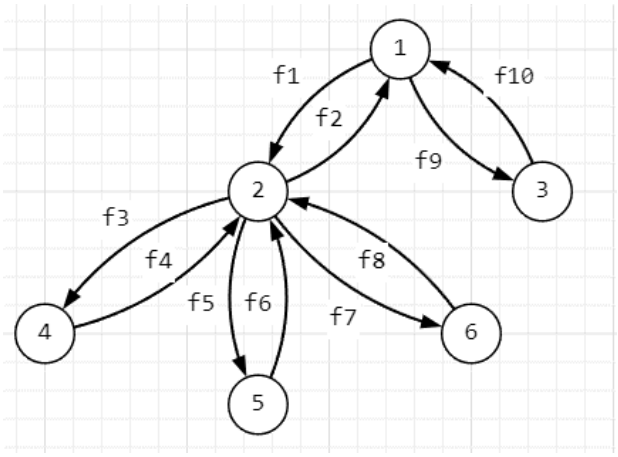

Рис. 11. Карта организации беспроводной телекоммуникационной сети связи

Для анализа риска было установлено оптимальное количество выборок равное 1000. На рис. 11 представлены гистограммы распределения рисков абонентов. Наиболее значимыми для регулирования рисков являются 1 и 2 абоненты сети, так как имеют высокие значения критичности узлов.

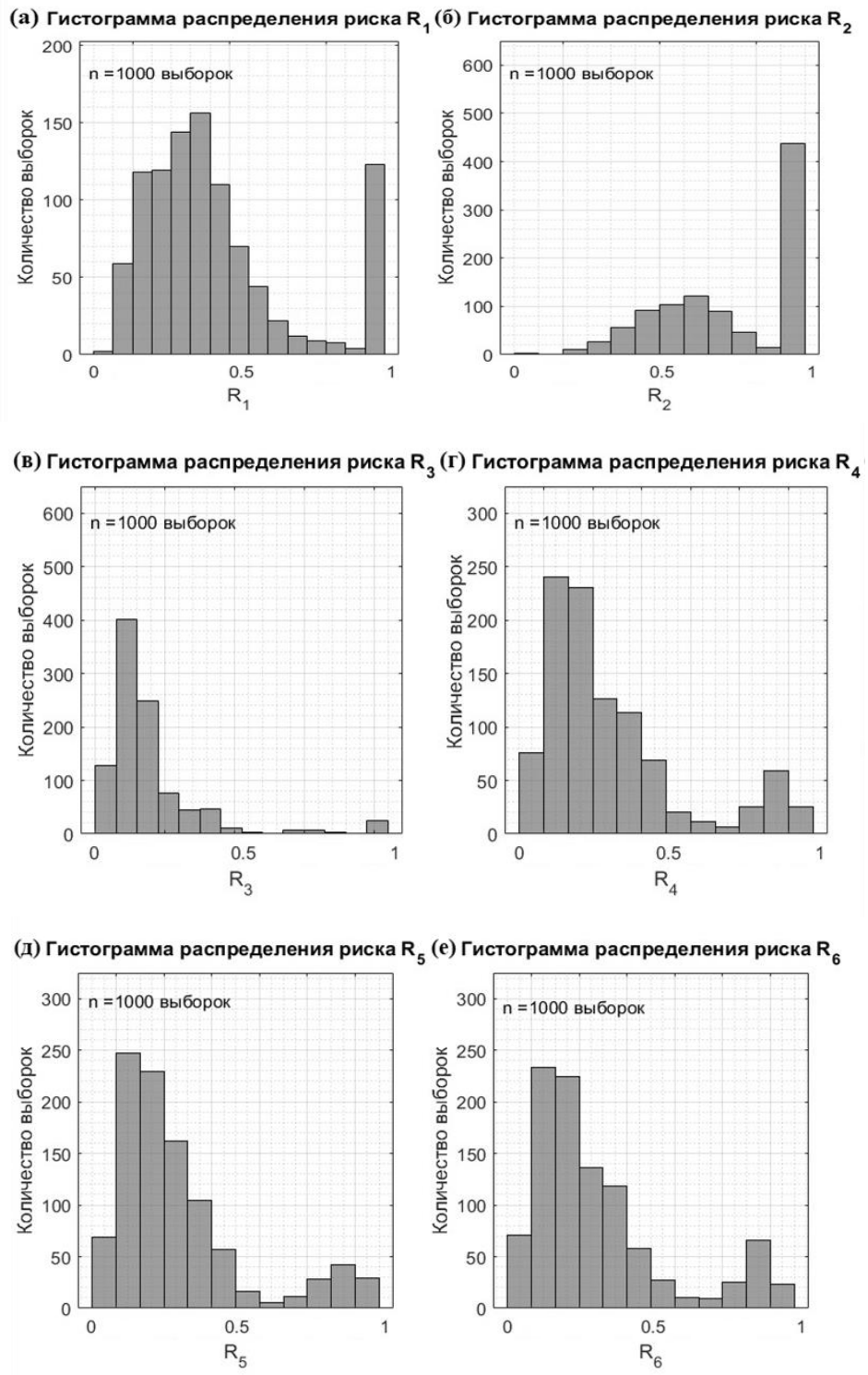

Рис. 12. Гистограммы распределения: а) риска R_1; б) риска R_2; в) риска R_3; г) риска R_4; д) риска R_5; е) риска R_6

Максимальный риск для первого абонента равен R_1 = 0,9108, для второго R_2 = 0,8974.

На рис. 12 представлены функции распределения риска для абонентов.

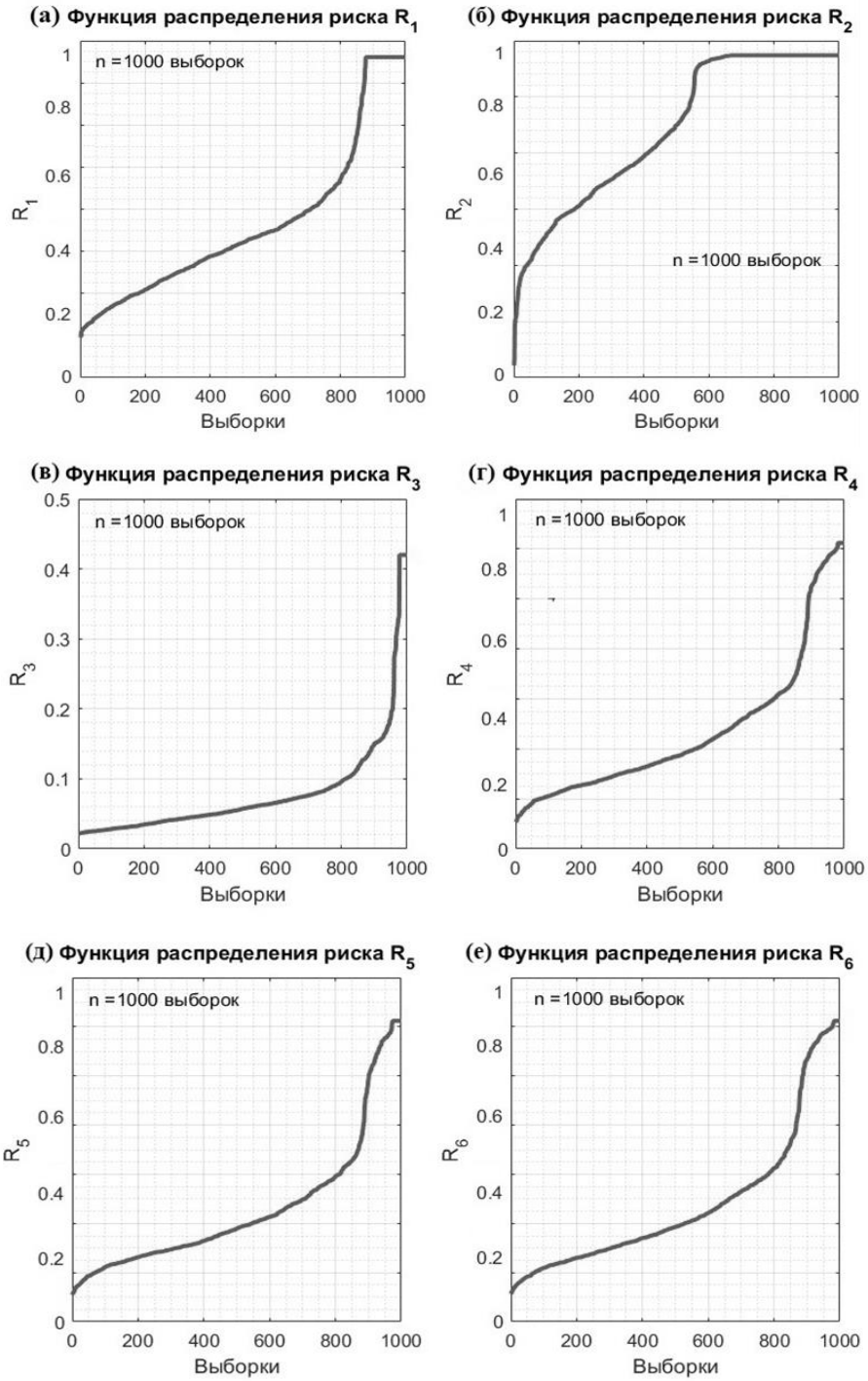

Рис. 13. Функции распределения: а) риска R_1; б) риска R_2; в) риска R_3; г) риска R_4; д) риска R_5; д) риска R_6

На рис. 13 представлен вариант квазиоптимального решения по назначению рабочих частот с минимальным риском нарушения доступности и целостности информации между абонентами.

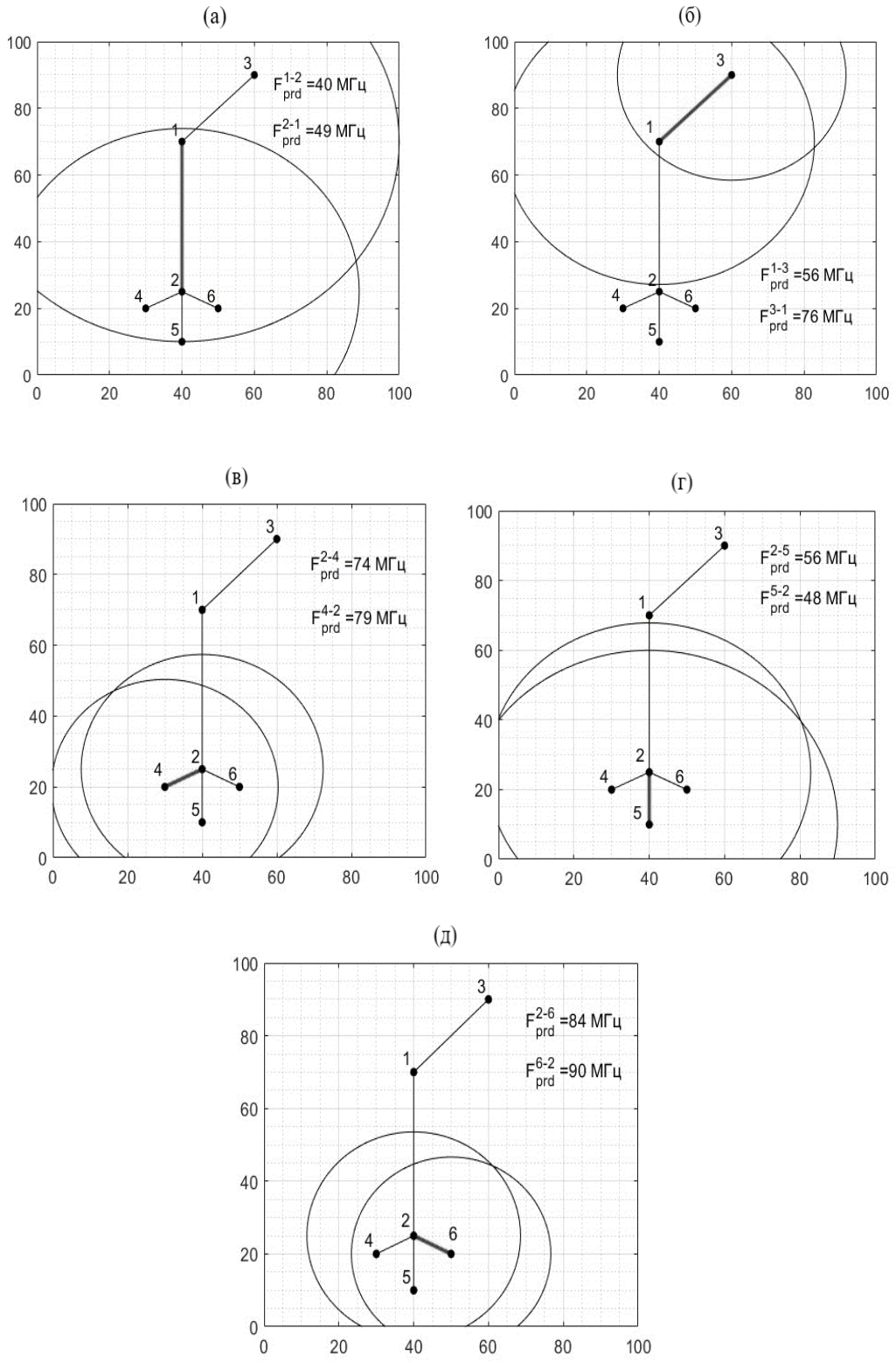

Рис.14. Назначение частот для квазиоптимальных значений рисков для абонентов: а) 1 и 2; б) 1 и 3; в) 2 и 4; г) 2 и 5; д) 2 и 6

Заключение

В статье приведена методика оценки и регулирования рисков нарушения целостности и доступности информации в беспроводной телекоммуникационной сети связи. Достоинством данной работы является расширенный анализ рисков, посредством введения новых параметров: координат абонентов, максимальных расстояний между абонентами сети и влияния продуктов интермодуляции. Так же было подробно рассмотрено дерево для сценариев атак

непреднамеренных злоумышленников на данную сеть. Предлагаемая методика регулирования рисков основана на частотном планировании. Случайным образом задав частоты, производится серия экспериментов и расчет рисков совершения атаки на сеть связи. После получения статистических данных для регулирования риска назначаются рабочие частоты с учетом минимальных значений ущерба. Методика в дальнейшем может совершенствоваться с добавлением дополнительных параметров.

Список литературы

1. Ампелонский, А. Ю. Рост уровня помех в работе беспроводных сетей, обусловленный увеличением числа сетей / А. Ю. Ампелонский // Молодой ученый. 2019. № 46 (284). С. 9-11.

2. Ермаков С.А. Оценка и регулирование рисков нарушения информационной безопасности телекоммуникационных сетей связи и управления промышленного интернета вещей / С.А. Ермаков, Я.М. Каценко, А.А. Болгов, В.В. Сафронова, К.В. Сибирко // Информация и безопасность. 2020. Т. 23. Вып. 1. С. 107-114.

3. Ермаков С.А. Повышение защищенности автоматизированной системы «умный дом»: алгоритм оценки рисков нарушения конфиденциальности информации / С.А. Ермаков, Ю.А. Гусарева, А.А. Болгов, В.Н. Кострова // Информация и безопасность. 2022. Т. 25. Вып. 3. С. 377-388.

4. Grime M.M. Delphi Method. / M.M. Grime, G. Wright. Wiley StatsRef: Statistics Reference Online. John Wiley & Sons Inc., New York, 2016. P. 1-6.

5. Liu Q. Improving VRSS-based vulnerability prioritization using analytic hierarchy process / Q. Liu, Y. Zhang, and Y. Kong, et al. // Journal of Systems and Software. 2012. V. 85. No. 8. P. 1699-1708.

6. Poolsappasit N. Dynamic security risk management using Bayesian attack graphs / N. Poolsappasit, R. Dewri, I. Ray // IEEE Transactions on Dependable & Secure Computing. 2012. V. 9. No. 1. P. 61-74.

7. Zhao D.M., Liu H.F. Risk assessment of information security based on BP neural network // Computer Engineering & Applications. 2007. V. 43. No. 1, pp. 139-141.

8. Luo S.-D. Information Security Risk Analysis of Airborne Communication Network / S.-D. Luo, X.-H. Bao, Y. Xin, // 2019 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE). 2019. P. 77-83.

Концерн «Созвездие»
Concern «Sozvezdie»

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 15.01.2023

Информация об авторах

Гречишкин Александр Владимирович – канд. техн. наук, Концерн «Созвездие», e-mail: mnac@comch.ru

Гулидова Елена Александровна – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Краснопольская Вероника Андреевна – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Завгородняя Юлия Владимировна – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Москалева Екатерина Алексеевна – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

ASSESSMENT AND REGULATION OF THE RISKS OF INTEGRITY AND AVAILABILITY VIOLATION IN A WIRELESS TELECOMMUNICATION NETWORK TAKING INTO ACCOUNT THE COORDINATES, THE DISTANCE BETWEEN ITS SUBSCRIBERS AND THEIR INFLUENCE ON EACH OTHER

A.V. Grechishkin, E.A. Gulidova, V.A. Krasnopolskaya, Yu.V. Zavgorodnyaya, E.A. Moskkaleva

This article proposes a method for quantifying and managing the risks of violating the integrity and availability of information circulating in a wireless telecommunications network. This technique is based on the application of the theory of complex networks to determine the key nodes of the network and on the use of an attack tree model to assess the probability of an attack. Algorithms have been developed to quantify and manage risks at the time of a possible attack. Risks are regulated by regulating the frequencies of receivers and transmitters of network subscribers, taking into account the coordinates, distances between subscribers and their influence on each other. A software and hardware complex is presented that allows, through statistical experiments, to compare network configurations and select quasi-optimal values with respect to risk in terms of the risk of successfully implementing an attack on integrity and availability in a wireless communication network.

Key words: Software and hardware complex, wireless telecommunications network, risk, assessment, regulation, security, integrity, availability.

Submitted 15.01.2023

Information about the authors

Grechishkin Alexander V. – Cand. Sc. (Technical), Concern «Sozvezdie», e-mail: mnac@comch.ru
Gulidova Elena A. – student, Voronezh State Technical University, e-mail: mnac@comch.ru
Krasnopolskaya Veronika A. – student, Voronezh State Technical University, e-mail: mnac@comch.ru
Zavgorodnyaya Yulia V. – student, Voronezh State Technical University, e-mail: mnac@comch.ru
Moskaleva Ekaterina A. – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: mnac@comch.ru