СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 621.391.7

Д.С. САЛЬНИКОВ, А.И. ЦОПА, д-р техн. наук

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ВОЛН

Введение

Повышение скорости передачи информации в современных беспроводных системах связи, связанное с увеличением трафика мультимедийной информации и развитием технологий *IP-TV*, требует перехода к более высокочастотным диапазонам волн. Новый стандарт технологии передачи информации *IEEE 802.11ad* использует диапазон 60 ГГц [1].

Беспроводные системы связи следующего поколения *5G*, использующие миллиметровые волны (ММ ДВ), обеспечивают чрезвычайно высокие скорости передачи информации с использованием узких сигнальных лучей. Обладая высокой направленностью и будучи восприимчивыми к блокировке объектами окружающей среды, каналы ММ ДВ часто считаются трудными для перехвата нарушителем [2].

Однако мелкомасштабные объекты внутри основного луча канала распространения вызывают отражения, что позволяет устройствам перехвата получать сигнал вне основного луча. В работе [3] экспериментально показано, что даже небольшие по площади отражатели позволяют принимать сигналы ММ ДВ нарушителем. Современные коммуникационные устройства с металлическими поверхностями, такие как мобильные телефоны или ноутбуки, могут также вызывать достаточное отражение сигнала, что может создавать угрозу для перехвата информации.

Для прогнозирования защищенности беспроводных систем передачи информации на физическом уровне в настоящее время широко используется концепция отводного канала (ОК) [4 – 6].

Цель работы – разработка модели угроз на канал связи ММ ДВ и оценка защищенности беспроводной системы передачи информации с ОК.

Основная часть

При разработке модели угроз для беспроводных систем передачи информации на физическом уровне модели OSI необходимо учитывать особенности распространения радиоволн и эффектов, возникающих в реальных условиях работы канала связи.

К числу главных преимуществ применения ММ ДВ в системах связи следует отнести прежде всего такие факторы, как увеличение объема и скорости передачи информации, высокое усиление антенн при малой их апертуре и повышенная помехозащищенность канала связи, возможность организации локальных широкополосных систем передачи данных, применение остронаправленных антенн и особенность распространения волн ММ-диапазона.

Характерной чертой любого радиосигнала является уменьшение уровня сигнала при распространении за счет ослабления в свободном пространстве, потерь в газах атмосферы и некоторых других видов дополнительных потерь. Особенность использования ММ ДВ для радиосвязи (наземной, спутниковой) состоит в том, что при их распространении радиоизлучение затухает в атмосферных газах и гидрометеорах [7].

Модель ослабления радиосигнала от расстояния d в свободном пространстве $FSPL$ (*FSPL – Free Space Path Loss*) определяется выражением [8]

$$FSPL = \left(\frac{4\pi \cdot d}{\lambda} \right)^2 , \qquad (1)$$

где d – расстояние между антеннами, м; λ – длина волны сигнала $\lambda = c/f$, м; c – скорость света в вакууме, $c = 299{,}97245 \cdot 10^6$ м/с; f – частота сигнала, Гц.

Мощность принимаемого сигнала снижается пропорционально квадрату расстояния d между передающей и приемной антеннами и существенно зависит от частоты сигнала f.

Формула (1) может быть выражена в децибелах при условии измерения расстояния d в километрах, а частоты f – в мегагерцах.

$$FSPL(d) = 32.4 + 20\log(f) + 20\log(d) \quad [дб], \tag{2}$$

На рис. 1 представлены зависимости потерь в свободном пространстве $FSPL(d)$ от расстояния для различных частот сигнала (2,4; 40; 60; 94 и 300 ГГц).

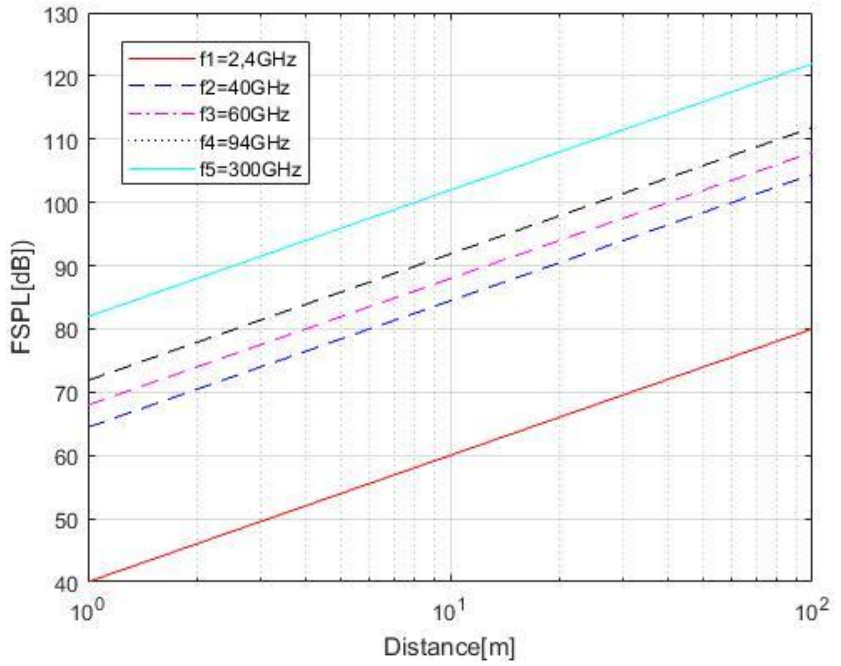

Рис. 1. Зависимость потерь в свободном пространстве FSPL от расстояния.

Как видно из графиков, сигналы ММ ДВ имеет довольно большое затухание в свободном пространстве и для обеспечения эффективной работы системы связи необходимо использовать высоконаправленные антенные системы, обладающие большим усилением и узкой диаграммой направленности. Например, рупорные антенны могут иметь ширину основного луча в пределах $(5 - 15)^\circ$. Стандарт связи *IEEE 802.11ad* [1] описывает алгоритм формирования луча с антенными решетками для достижения ширины луча 3°.

Системная модель беспроводной системы связи ММ ДВ, представленная на рис. 2, включает в себя канал передачи информации от передатчика Алисы до получателя информации приемника Боба, который называется основным, или легитимным каналом связи *(main channel)*. Алиса передает сигналы Бобу и для повышения защищенности канала использует узкую диаграмму направленности. Мы предполагаем, что обе антенны Алисы и Боба идеально выровнены и передают сигналы в оптимальном направлении.

Нарушитель Ева нацелена на перехват сигналов, которые Алиса посылает Бобу, не мешая ей. Она действует пассивно и только слушает сигналы и пытается принять отраженные сигналы от объектов расположенных в сигнальном луче. Для удобства анализа мы предполагаем, что Ева использует те же аппаратные средства, что и Алиса и Боб. Канал отвода от передатчика легитимного канала к приемнику незаконного потребителя (нарушителя) является отводным каналом ОК *(wiretap channel)*.

Исходя из системной модели, можно выделить три возможных варианта поведения нарушителя при атаке на канал связи:

– перемещение манипулятора объекта и помещение различных объектов в сигнальный луч, чтобы вызвать отражение сигнала к фиксированной позиции перехвата (рис. 2, *а*);

– перемещение самого нарушителя и использование отражения от существующих объектов в среде распространения, которую он не может изменить (рис. 2, *б*);

– стационарное положение нарушителя, который не может ни двигаться, ни манипулировать объектами окружающей среды и только попытается перехватить сигнал (рис. 2, *в*).

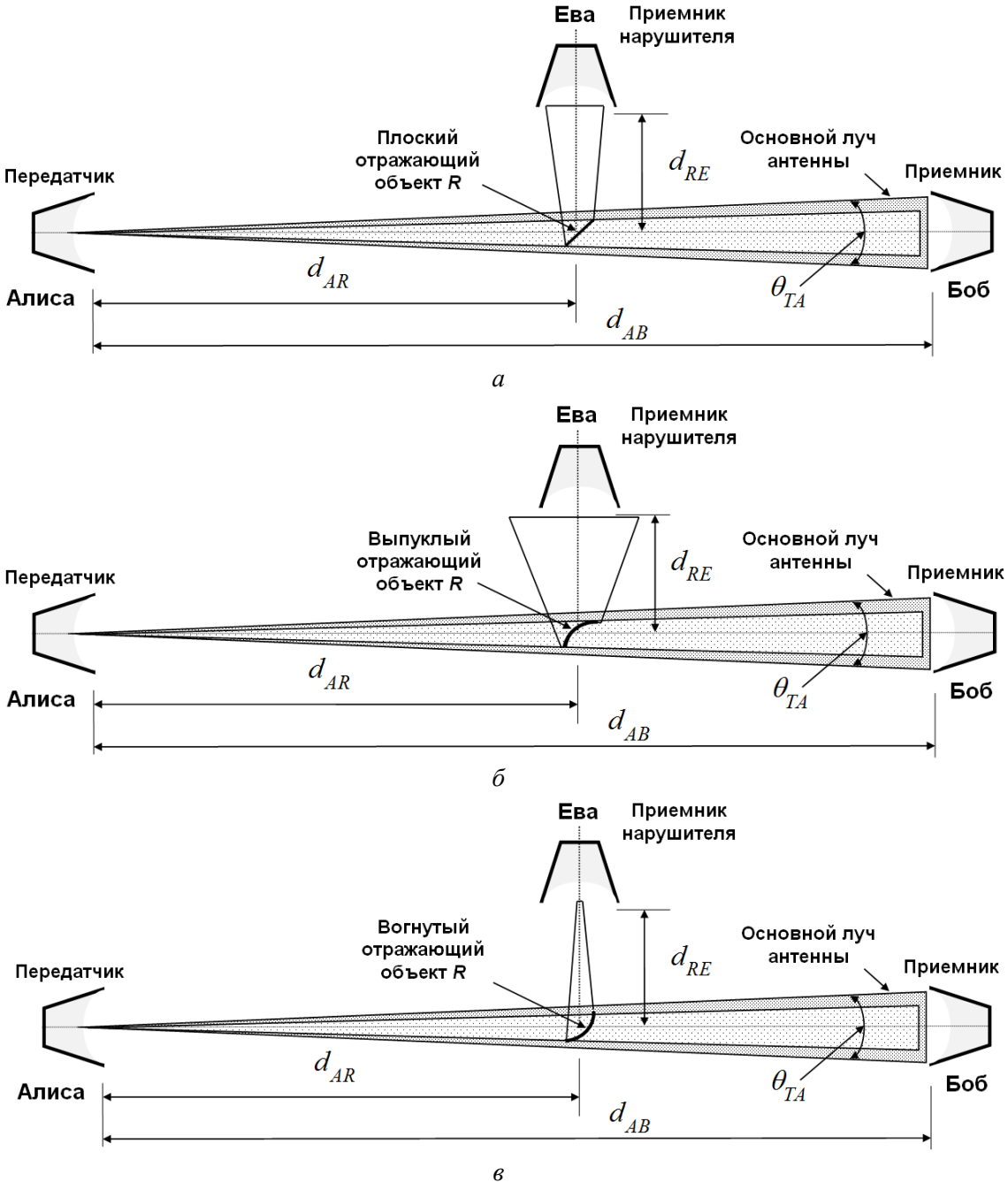

Рис. 2. Системная модель беспроводной связи ММ ДВ, показывающая возможные варианты отражения сигнального луча на разных формах объектов

Манипулирование объектом. Эта модель атаки предполагает, что нарушитель Ева находится в фиксированном положении вне основного сигнального луча и непосредственно оттуда невозможно принять сигнал. Однако Ева помещает произвольные объекты в окружающей среде, чтобы вызвать отклонение сигнала в нужную ей сторону. Она может управлять своей

антенной по направлению к этому объекту, чтобы наилучшим образом получать сигналы передаваемого сигнала и стремится получить достаточное качество сигнала для декодирования информации. В то же время Ева пытается оставаться невидимой для Алисы и Боба, вызывая лишь незначительную блокировку прямой передачи сигнала.

Позиционный перехват. В отличие от предыдущей модели, Ева не может изменить окружающую среду, но пытается использовать существующие эффекты распространения. Она может свободно выбирать место за пределами луча и направлять антенну на любой отражатель в окружающей среде. Поскольку она никак не может повлиять на блокировку, Ева стремится только максимизировать качество полученного сигнала, стремясь найти оптимальное местоположение антенны и ориентацию ее для перехвата. Несмотря на то, что использование существующих объектов может быть сложнее, обнаружить эту атаку сложно, потому что ничто в среде не меняется при нормальной работе системы связи.

Статическая (стационарная) атака. В этой модели Ева не может ни манипулировать окружающей средой, ни двигаться к оптимальному положению своей антенны. Это означает, что Ева должна полагаться на объекты окружающей среды в надежде на то, что сигнал отразится в нужном ей направлении. Как и для позиционного перехвата, Ева не влияет на блокировку, но она может управлять своей антенной только с фиксированного места для лучшего приема. Это самая слабая модель противника, но нарушителя Еву почти невозможно обнаружить, потому что ничего не меняется в окружающей среде при работе системы связи.

В общем случае для выполнения атаки манипуляции может использоваться управляемый рефлектор в любом месте сигнального луча. Для упрощения задачи анализа мы будем предполагать, что отраженные объекты должны находиться непосредственно на центральной линии узкого луча между Алисой и Бобом, что является оптимальным случаем, который вызывает как наибольшее отражение сигнала, так и блокировку сигнала.

Как показано на рис. 2, Боб получает сигнал в теневой области, заблокированной отражающим объектом. Ева, за пределами основного луча сигнала, получает только отраженные сигналы от объекта. Объект манипуляции может обладать различными характеристиками: размерами и формой объекта, видом и структурой материала, отражающей способностью и возможностями блокировки сигнала.

При рассмотрении плоских отражателей передаваемые и отраженные лучи имеют одинаковую ширину. Отражатели с выпуклыми формами рассеивают сигнал в разные стороны, а отражатели с вогнутый формой фокусируют сигнал к определенной фокальной точке.

Для анализа защищенности системы мы будем использовать критерии [9], которые характеризуют систему передачи информации на физическом уровне: пропускную способность канала, уровень сигнала, отношение сигнал/шум, вероятность битовой ошибки. В нашем дальнейшем анализе защищенности канала связи мы не будем учитывать дополнительные отражения сигнала на нескольких объектах.

Одной из метрик оценки защищенности канала связи на физическом уровне является секретная производительность C_S [8], которая определяется как максимальная разность между скоростью передачи информации в легитимном C_{AB} и отводном C_{AE} каналах:

$$C_S = \max\{0, C_{AB} - C_{AE}\} = \left[\log\left(1+SNR_{AB}\right) - \log\left(1+SNR_{AE}\right)\right]^+, \quad (3)$$

где SNR_{AB} – отношение сигнал/шум в основном канале; SNR_{AB} – отношение сигнал/шум в отводном канале.

Пропускная способность канала связи C между передатчиком и приемником при наличии аддитивного белого гауссовского шума N определяется формулой Шеннона [9]:

$$C = W\log_2\left(1+SNR\right) = W\log_2\left(1+\frac{P_R}{N}\right), \quad (4)$$

где W – полоса пропускания канала, Гц; P_R – уровень принимаемого сигнала, Вт; $N = W \cdot k \cdot T$ – уровень аддитивного белого гауссовского шума, k – постоянная Больцмана, равная $k = 1.3807 \cdot 10^{-23} Вт/Гц \cdot град$, $T = 290^o K$ – температура в градусах по Кельвину.

Уровень принимаемого сигнала $P_R(d)$, при затухании сигнала между антеннами по экспоненциальному закону, рассчитывается по формуле Фрииса [9]:

$$P_R(d) = P_T \cdot G_T \cdot G_R \left(\frac{\lambda}{4\pi}\right)^2 \cdot \left(\frac{1}{d}\right)^n , \quad (5)$$

где P_T – мощность передатчика, Вт; G_T – коэффициент усиления передающей антенны; G_R – коэффициент усиления приемной антенны; d – расстояние между антеннами, м; λ – длина волны сигнала $\lambda = c/f$, м; c – скорость света в вакууме, $c = 299{,}97245 \cdot 10^6$ м/с; f – частота сигнала, Гц; n – коэффициент, зависящий от условий распространения (2) – (6) [10].

В таблице представлены величины коэффициента n для различных условий распространения:

Условия распространения	n
Свободное пространство	2
Открытое пространство в городе	2,7-3,5
Пространство в городе с плотной застройкой	3-5
Внутри зданий LOS	1,76-1,8
Внутри зданий NLOS	4-6

Эффективность манипуляции объектом в основном сигнальном луче будем характеризовать коэффициентом отражения r и коэффициентом блокировки b:

$$r = \frac{\max(P_{R\,E})}{\max(P_{R\,opt})}, \quad (6)$$

$$b = 1 - \frac{\max(P_{R\,B})}{\max(P_{R\,opt})}, \quad (7)$$

где P_{OPT} – уровень принимаемого сигнала Боба при отсутствии отражений и блокировки.

Используя (4) и (5), можно записать соответствующие выражения для производительности основного канала C_{AB}, отводного канала C_{AE} и секретной производительности C_S:

$$C_{AB} = W \log_2 \left[1 + \frac{P_{TA} \cdot G_{TA} \cdot G_{RB}}{W \cdot k \cdot T} \left(\frac{\lambda}{4\pi}\right)^2 \cdot \left(\frac{1}{d}\right)^n\right], \quad (8)$$

$$C_{AE} = W \log_2 \left[1 + \frac{P_{TA} \cdot G_{TA} \cdot G_{RE}}{W \cdot k \cdot T} \left(\frac{\lambda}{4\pi}\right)^2 \cdot \left(\frac{1}{d}\right)^n\right], \quad (9)$$

$$C_S = C_{AB} - C_{AE} = W \log_2 \left\{\frac{\left[1 + \frac{P_{TA} \cdot G_{TA} \cdot G_{RB}}{W \cdot k \cdot T} \left(\frac{\lambda}{4\pi}\right)^2 \cdot \left(\frac{1}{d_{AB}}\right)^n\right]}{\left[1 + \frac{P_{TA} \cdot G_{TA} \cdot G_{RE}}{W \cdot k \cdot T} \left(\frac{\lambda}{4\pi}\right)^2 \cdot \left(\frac{1}{d_{AE}}\right)^n\right]}\right\}, \quad (10)$$

где G_{RB} – коэффициент усиления приемной антенны Боба; d_{AB} – расстояние между передающей антенной Алисы и приемной антенной Боба, м; G_{RE} – коэффициент усиления приемной антенны Евы; d_{AE} – расстояние между передающей антенной Алисы и приемной антенной Евы, м.

Чтобы оценить секретную производительность, мы использовали моделирование в математическом пакете *MATLAB*. Представленная модель является упрощенной и учитывает фактически пропускную способность канала C_{AB} и C_{AE} в зависимости от усиления антенны Евы и расстоянием от Алисы к Бобу и Еве.

В реальном случае у нас не будет никакой информации, как о расстоянии, так и усилении антенн, так как это параметры устройства злоумышленника, поэтому мы использовали для создания нашей модели и параметры которые взяты на основе типовых устройств:

W (полоса пропускания канала) – 1 ГГц;

P_A (мощность передатчика Алисы) – 30, mВт;

G_{TA} (коэффициент усиления передающей антенны Алисы) – 20, дБ;

G_{RB} (коэффициент усиления приемной антенны Боба) – 20, дБ;

G_{RE} (коэффициент усиления приемной антенны Евы) – 29, дБ;

D_{AB} – расстояние между антеннами Алисы и Боба, м;

D_{AE} – расстояние между антеннами Алисы и Евы, м;

F – частота радиосигнала – 60, ГГц.

Результаты моделирования представлены на рис. 3 – 6.

На рис. 3 показано 3D-представление зависимости секретной производительности C_S как функции расстояния d_{AB} от пользователя Алисы до Боба и d_{AE} к нарушителю. Поверхность на рис. 3 представляет максимальную скорость C_S.

На рис. 4 показано общее 2D-представление зависимости секретной производительности C_S как функции расстояния d_{AB} от пользователя Алисы до Боба и d_{AE} к нарушителю Еве. Частная зависимость секретной производительности C_S от расстояния от Алисы к Бобу d_{AB} и от Алисы к нарушителю Еве d_{AE} представлена на рис. 5, 6.

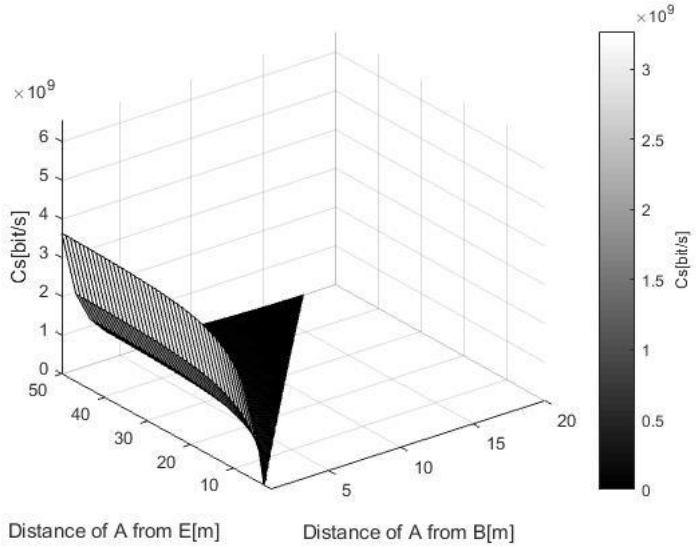

Рис. 3. 3D-зависимость секретной производительности C_S от пользователя Алисы до Боба d_{AB} и нарушителю Еве d_{AE}

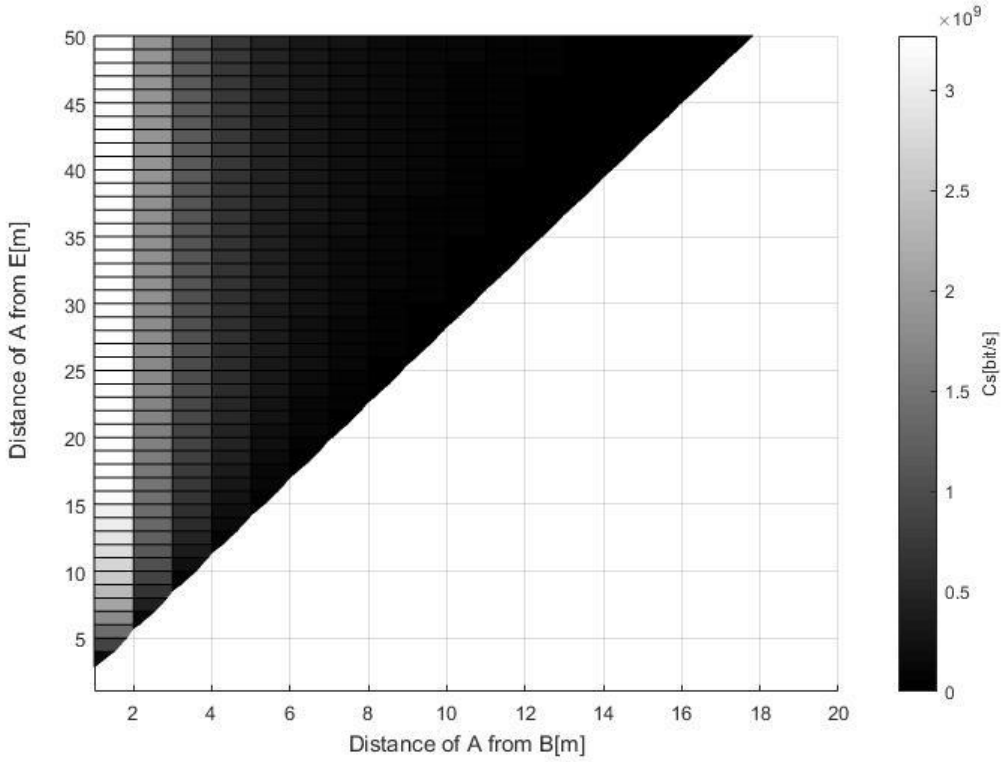

Рис. 4. Общая 2D-зависимости секретной производительности C_S от расстояния d_{AB} от пользователя Алисы до Боба и d_{AE} к нарушителю Еве d_{AE}

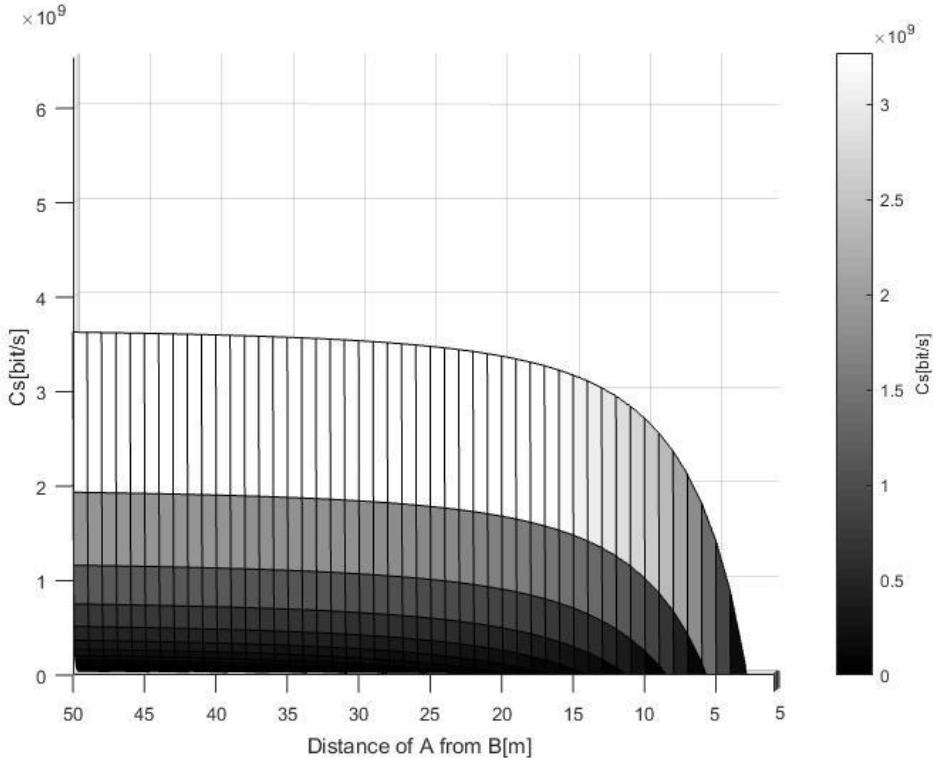

Рис. 5. 2D-зависимости секретной производительности C_S от d_{AE}.

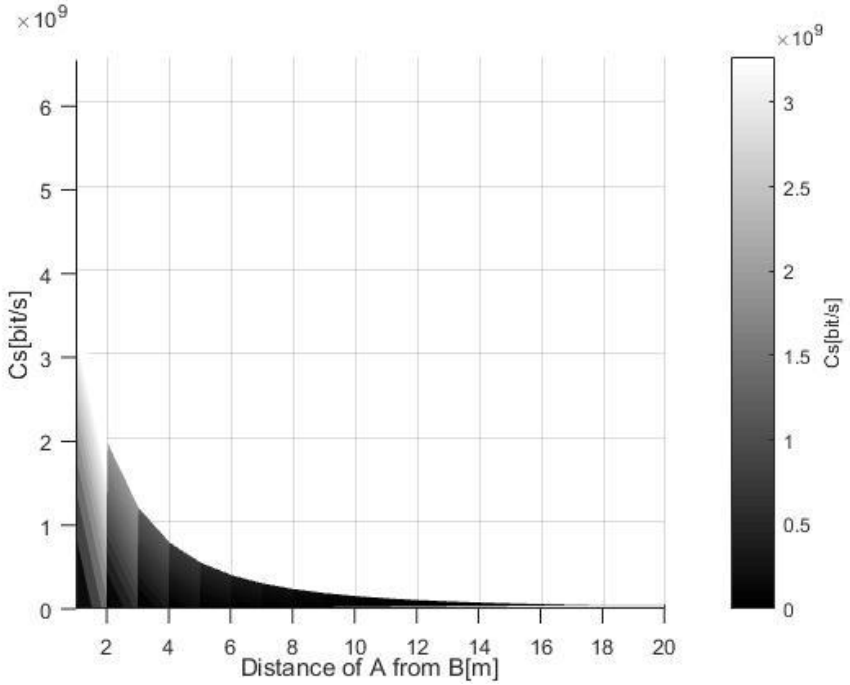

Рис. 6. 2D-зависимости секретной производительности C_S от d_{AB}.

На основании данных результатов можно выделить основные достоинства данной модели и преимущества, дающие 3D графики.

Во-первых, результаты подтверждают актуальность использования данной метрики по оценке защищенности канала связи на физическом уровне в ММ ДВ, а также дает возможность в дальнейшем использовать эту модель как основу для формирования более развернутой и сложной модели беспроводной системы связи. В дальнейшем при построении и анализе защищенности канала связи мы будем учитывать дополнительные отражения сигнала на нескольких объектах, а так же применение узкой диаграммы направленности.

Во-вторых, благодаря 3D-графикам наглядно видно особенности зависимости секретной производительности от расстояния при использовании миллиметровых волн (ММ ДВ), для данного расстояния d_{AB} есть минимальное расстояние d_{AE}, где минимальная скорость основного канала может быть удовлетворена, и связь при этом остается безопасна. Например, с параметрами представленных в данной статье, если Ева находится в 15 м от Алисы, то секретная производительность практически становится максимальной благодаря использованию миллиметровых волн и специфики их распространения в пространстве.

Представленная выше методика оценки уровня защищенности СПИ в основном и отводном канале связи на физическом уровне модели взаимодействия *OSI*, позволяет проводить сравнительную оценку различным методам, которые использует злоумышленник и спрогнозировать ряд средств и способов с целью обеспечения требований по защите информации.

Выводы

1. Рассмотрена и сформирована общая модель угроз для оценки параметров защищенности систем передачи информации на физическом уровне при использовании миллиметрового диапазона волн (ММ ДВ). Более детально показана модель угроз основанная на зависимости пропускной способности канала от усиления антенны и расстояния в основном и отводном канале связи.

2. Рассмотренная модель демонстрирует начальные возможности ММ ДВ в концепции использования в современных системах связи, а именно защищенность на физическом уровне. Однако при дальнейшем добавлении дополнительных параметров, таких как коэффици-

ент отражения и коэффициент блокировки объектами окружающей среды, мы получим детальную модель угроз на физическом уровне. Данная модель дает точное понимание конкретных уязвимостей и тем самым подчеркивает актуальность концепции отводного канала.

Список литературы

1. Nitsche T., Cordeiro C., Flores A. B., Knightly E. W., Perahia E. and Widmer J. C. IEEE 802.11ad: directional 60 GHz communication for multi-Gigabit-per-second Wi-Fi // IEEE Communications Magazine. 2014. vol. 52, № 12. pp. 132-141.

2. Yang N., Wang L., Geraci G., Elkashlan M., Yuan J. and. Renzo M. D. Safeguarding 5G wireless communication networks using physical layer security // IEEE Communications Magazine. 2015. vol. 53, №4. pp. 20-27.

3. Steinmetzer D., Chen J., Classen J., Knightly E., Hollick M. Eavesdropping with Periscopes: Experimental Security Analysis of Highly Directional Millimeter Waves // Proceedings of the IEEE Conference on Communications and Network Security (CNS). 2015, September 2015, Florence.

4. Wyner A. D. The wire-tap channel // Bell System Technical Journal. 1975. Vol. 54, № 8. pp. 1355-1387.

5. Liu R. and Trappe W. Securing Wireless Communications at the Physical Layer // New York : Springer, 2010.

6. Методы прогнозирования защищенности ведомственных систем связи на основе концепции отводного канала ; под ред. А. И. Цопы, В. М. Шокало. Харьков : КП «Городская типография», 2011. 502 с.

7. Быстров Р.П., Петров А.В., Соколов А.В. Миллиметровые волны в системах связи // Журнал радиоэлектроники. 2000. №5.

8. Barros J. and Rodrigues M. R. D. Secrecy Capacity of Wireless Channels // IEEE Int. Symp. on Information Theory, 2006; Shu Sun, George R. MacCartney Jr., Rappaport Theodore S. Millimeter-Wave Distance-Dependent Large-Scale Propagation Measurements and Path Loss Models for Outdoor and Indoor 5G Systems // 10th European Conference on Antennas and Propagation – Davos, Switzerland. April 2016, pp. 1-5.

9. Chrysikos T., Dagiuklas T., Kotsopoulos S. A Closed-Form Expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security // Proceedings of Security in Emerging Wireless Communication and Networking Systems (SEWCN'09). Springer, 2010. Vol. 42 of Lecture Notes in Computer Science. pp. 3-12.

10. Tsopa O.I. Estimation of the probability to detect signal with wiretap channels with antennas apertures of different sizes and relative position /A.A. Strelnitskiy, A.E. Strelnitskiy, O.I. Tsopa, V.M. Shokalo, E.V. Yagudina // Telecommunication and Radio Engineering. Begell House, 2011. Vol. 70(7). P. 601-606.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 17.02.2018