УДК 004.056.53
DOI: 10.53403/9785951505460_506

ВЫБОР ОПТИМАЛЬНОЙ РАБОЧЕЙ ТОЧКИ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ НА ОСНОВЕ ЗАТРАТ

Мартынова Юлия Олеговна (YuOTrusova@vniief.ru), Мулин Николай Николаевич, Пещенко Алексей Викторович

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

В этой статье мы рассмотрим расширение возможностей систем обнаружения вторжений (СОВ) на основе затрат. Для определения ожидаемой стоимости в каждой рабочей точке СОВ, использовался метод анализа дерева решений, и были построены графики ожидаемой стоимости и возможности обнаружения вторжения в зависимости от уровня ложноположительных результатов. Точка пересечения между максимальной способностью обнаружения вторжения и ожидаемой стоимостью выбирается в качестве оптимальной рабочей точки. Результат работы: найденная рабочая точка является оптимальной для данной СОВ.

Ключевые слова: Система обнаружения вторжений, Возможность обнаружения вторжений, Теория информации.

SELECTED THE OPTIMAL OPERATION POINT OF INTRUSION DETECTION SYSTEM CAPABILITY

Martynova Iulia Olegovna (YuOTrusova@vniief.ru), Mulin Nikolay Nikolaevich, Peshchenko Aleksey Viktorovich

FSUE «RFNC-VNIIEF», Sarov Nizhny Novgorod region

In this paper, we consider a cost-based extension of intrusion detection system (IDS) capability. In order to determine the expected cost at each IDS operating point, the decision tree method of analysis is employed, and plots of expected cost and intrusion detection capability against false positive rate were generated. The point of intersection between the maximum intrusion detection capability and the expected cost is selected as the optimal operating point. The result paper: calculated operating point is the most optimal for the given IDS.

Keywords: Intrusion detection system, Intrusion detection capability, Information theory.

С развитием вычислительной техники и повсеместного использования интернет-услуг риск несанкционированного доступа к компьютерным системам стремительно увеличивается. Это требует от организаций и корпораций принимать серьезные меры для защиты компьютерных систем от вторжений. В настоящее время используются парольные фразы, антивирусные приложения и брандмауэр для защиты сетей и конфиденциальных данных. К несчастью, эти алгоритмы имеют ограниченные возможности для защиты информации. Например, пароли могут быть скомпрометированы. А антивирусная защита может быть неэффективной и не иметь возможности осуществлять мониторинг в режиме реального времени. Поэтому важность систем обнаружения вторжений для повышения безопасности системы, посредством мониторинга в реальном времени и обнаружения атак и вторжений, переоценить невозможно. Система обнаружения вторжений (СОВ) относится к механизму для выявления злоупотреблений и/или взлома компьютерной системы злоумышленниками из внутренних/внешних источников. Поэтому задача защиты компьютерных систем от злоумышленников является необходимостью и должна восприниматься серьезно.

Хотя в СОВ было предпринято много исследований и разработок, надлежащая оценка СОВ все еще остается серьезной проблемой. Это связано с:

1) отсутствие стандартного эталонного теста, что затрудняет сравнение нескольких СОВ;

2) динамически изменяющейся средой, затрудняющей создание полностью описательного базового уровня;

3) проблемы с эмпирическими оценками (с использованием определенного набора данных для тестирования СОВ) так как всегда будет разница между оценочным набором данных и реальным сценарием.

Однако ключевая проблема в обнаружении вторжений состоит в том, как определить основные показатели для надлежащей оценки СОВ, особенно в определении способности СОВ классифицировать события как нормальные или навязчивые.

Хотя в литературе определены основные показателях, такие как истинно положительная скорость, ложно положительная частота, способность обнаружения вторжения, рабочие характеристики приемника и некоторые другие, которые измеряют различные аспекты системы обнаружения вторжения, очень трудно найти единственную метрику, которая полностью подходит для оценки возможностей СОВ, особенно в том, что касается затрат на эксплуатацию.

Способность обнаруживать вторжения, C_{ID} – это единая метрика, предложенная *G. Gu* на основе теории информации. Если данная СОВ настроен относительно C_{ID}, становится очень легко определить конкретную рабочую точку, которая дает минимальный уровень неопределенности относительно заданного входного события, для определения произошло оно из-за вторжения или нет. Тем не менее, единая метрика не учитывает ожидаемые затраты, связанные с этой рабочей точкой. Кроме того, определить с практической точки зрения нужный уровень неопределенности может быть достаточно дорого.

Применение метода затрат дополняет и увеличивает область применения C_{ID} как показателя оценки, а не просто уменьшает неопределенность вторжений. Это расширение помогает выбрать рабочую точку, а также определяет лучшее решение, которое необходимо принять в отношении используемого детектора.

Качественная СОВ должна уметь различать отслеживаемые события (входные данные) как навязчивые или нормальные. СОВ, как правило, предоставляют выходную информацию в виде сигналов тревоги, которые должны дать истинную картину отслеживаемых событий.

При тщательном анализе каждая единица входного потока данных может быть навязчивой или нормальной, и СОВ должна иметь возможность знать и записывать эту информацию для сведения администратора. Это подразумевает, что вход СОВ может быть тщательно смоделирован как случайная величина X.

Аналогично, выходная информация типичной СОВ может быть смоделирована как случайная величина Y.

Пусть значение X будет высоким ($X = 1$), тогда $Y = 1$ означает, что есть предупреждение о вторжении, а $Y = 0$, нет никакой информации о предупреждении от СОВ. Используем двоичный симметричный канал для моделирования обнаружения вторжения, представленный на рис. 1.

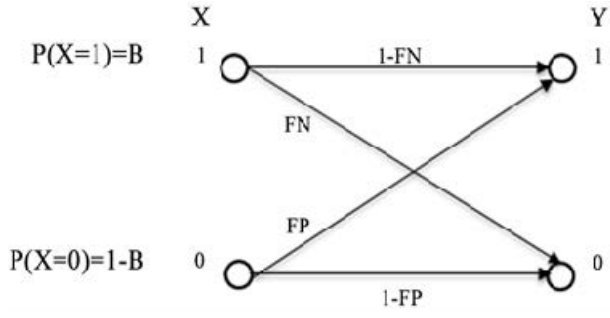

Рис. 1. Двоичный симметричный канал

$p(X = 1) = B$ означает вероятность наличия вторжений во входную информацию, обнаруженную СОВ.

Вероятность того, что событие вторжения можно рассматривать как нормальное, представлено как $p(Y = 0|X = 1)$, это ложноотрицательный коэффициент (FN), обозначаемый как γ. Точно так же вероятность того, что нормальное событие неправильно классифицируется как вторжение, представлена $p(Y = 1|X = 0)$, это ложноположительный показатель (FP), обозначаемый как α. Исходя из вышеизложенного, можно предположить, что X является случайной величиной, изображающей вход СОВ, а Y представляет случайную величину, изображающую выход СОВ. Следовательно, возможность обнаружения вторжения может быть определена как

$$C_{ID} = \frac{I(X;Y)}{H(X)} = \frac{H(X) - H(X \mid y)}{H(X)}. \qquad (1)$$

В идеале взаимная информация снижает уровень неопределенности входных данных путем оценки выходных данных СОВ. Из (1) можно сделать вывод, что C_{ID} дает коэффициент уменьшения неопределенности входных данных СОВ путем учета выходных данных СОВ. На практике, значение C_{ID} находится в диапазоне [0;1]. Чем выше значение C_{ID} тем способнее СОВ к точной классификации событий.

$$H(X) = -\sum_{x} p(x) \log p(x) =$$
$$-B \log B - (1-B) \log(1-B), \qquad (2)$$

$$H(X \mid Y) = \frac{-\sum_{x}\sum_{y} p(x)\,p(y \mid x) \log[\,p(x)\,p(x \mid y)]}{p(y)} =$$
$$= -B(1-\gamma) \log PPV - B\gamma \log(1-NPV) -$$
$$-(1-B)(1-\alpha) \log NPV - (1-B)\alpha \log(1-PPV). \qquad (3)$$

Отсюда

$$C_{ID} = \frac{-B \log B - (1-B) \log 1 - B}{-B(1-\gamma) \log PPV - B\gamma \log(1-NPV) - (1-B)(1-\alpha) \log NPV - (1-B)\alpha \log(1-PPV)}. \qquad (4)$$

В уравнении (4) C_{ID} - это возможность обнаружения вторжения, B – базовая скорость, γ – ложноотрицательная (FN) скорость, α – ложноположительная (FP) скорость, PPV – положительное прогнозируемое значение, а NPV – отрицательное прогнозируемое значение.

Базовая скорость (B) - это показатель среды, в которой работает СОВ. Если $B = 0$ или $B = 1$ (входной сигнал 100 % нормальный или 100 % вторжение). На практике может быть довольно сложно измерить или контролировать базовую скорость в СОВ. Это связано с тем, что базовая скорость часто рассматривается как параметр операции, отчасти из-за того, что она используется для измерения среды СОВ.

Скорость ложноположительная (FP): вероятность того, что СОВ выдаст сигнал тревоги, когда нет вторжения;

• Частота ложноотрицательная (FN): вероятность того, что СОВ не выдаст сигнал тревоги при вторжении;

• Положительное прогнозируемое значение (PPV): вероятность того, что произойдет вторжение, когда СОВ выдаст аварийный сигнал. То есть, сколько сигналов являются настоящими вторжениями. Это математически выражено в уравнении

$$PPV = \frac{B(1-\gamma)}{B(1-\gamma)+(1-B)\alpha}. \quad (5)$$

Отрицательное прогнозируемое значение (NPV): вероятность того, что не произойдет вторжения, когда СОВ не выдаст сигнал тревоги. Это означает, что нет предупреждений СОВ. Это математически выражено в уравнении

$$NPV\,\frac{(1-B)(1-\alpha)}{(1-B)(1-\alpha)+B\gamma}. \quad (6)$$

Количественно разница между нормальными событиями и вторжениями очень велика. Эта огромная разница может привести к возникновению множества ложных тревог. Поэтому, возникает заблуждение, что из-за низкой вероятности реальной атаки, особенно когда СОВ вызывает тревогу, вероятность реального вторжения минимальна.

Оценка обнаружения вторжения дается как $p = 6{,}52 \cdot 10^{-5}$.

Кривая рабочих характеристик приемника (ROC) показывает графическую иллюстрацию вероятности обнаружения по частоте ложных тревог. Это означает, что кривая способна показать вероятность обнаружения с точки зрения детектора с определенной частотой ложных тревог. В качестве альтернативы, кривая показывает зафиксированную частоту ложных срабатываний детектора при заявленной вероятности обнаружения.

Анализ ROC помогает выбрать оптимальную рабочую точку.

Для рабочей точки конкретного детектора можно определить ожидаемую стоимость путем анализа выходных данных дерева решений, представленного на рис. 2.

На дереве решений квадраты представляют последовательность действий, которые контролируются лицом, принимающим решения, в то время как круги представляют неопределенные события, которые находятся вне контроля лица, принимающего решение. Однако эти события дают полезную информацию о работе детектора и последующих действиях, которые необходимо предпринять в отчетах. Кроме того, дерево решений может содержать полезные советы о рисках, связанных с объединением некоторых действий и событий. Видно, что стоимость соответствует последствиям и отражает стоимость ошибочного решения. Например, стоимость не предоставления ответа при отсутствии тревоги (NA) и стоимость не предоставления ответа при вторжении представлена C. Здесь стоимость отсутствия ответа при вторжении равна нулю, и чем выше стоимость, тем меньше ценность результата. Следует отметить, что вероятность возникновения привязана к каждому неопределенному событию.

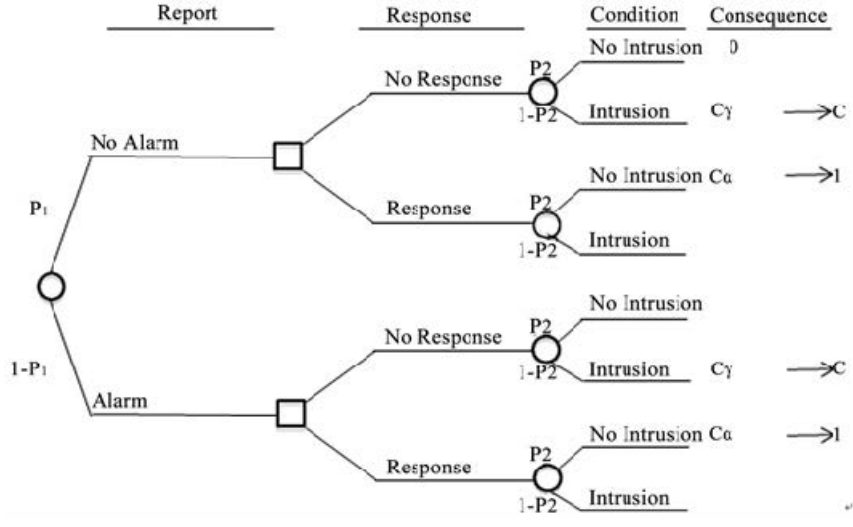

Рис. 2. Дерево решений

Вероятность p_1 относительная вероятности того, что детектор может сообщить о тревоге, p_2 – это условная вероятность того, что нет вторжения, учитывая, что детектор не сообщил о тревоге, и p_3 – это условная вероятность того, что нет никакого вторжения, учитывая, что детектор на самом деле сообщает о тревоге.

Традиционно дерево решений читается слева направо, и для расчета ожидаемых затрат, связанных с любой данной рабочей точкой, затраты тщательно рассчитываются для всех путей в дереве решений, а также вероятностей p_1, p_2 и p_3. Без ограничения общности соотношение затрат определяется как в уравнении

$$C = \frac{C_\gamma}{C_\alpha}, \tag{7}$$

где C_γ стоимость реагирования на присутствие вторжения, а C_α – стоимость реагирования на вторжение, когда фактически нет вторжения. В большинстве практических сценариев можно предположить, что стоимость правильных ответов на вторжение пренебрежимо мала или равна нулю.

Оценка вероятностей отчетов детектора:

$$p_1 = P(NA) = P(NA \mid NI)P(NI) + P(NA \mid I) = \\ = (1-\alpha)(1-p) + \gamma p, \tag{8}$$

$$1 - p_1 = P(A) = P(AN \mid I)P(NI) + P(A \mid I)P(I) = \\ = \alpha(1-p) + (1-\gamma)p. \tag{9}$$

Теорема Байеса может быть использована для расчета вероятностей состояния системы относительно отчетов, выданных детектором

$$p_2 = P(NI \mid NA) = \frac{P(NA \mid NI)P(NI)}{P(NA)} = \frac{(1-\alpha)(1-p)}{p_1} = \\ = \frac{(1-\alpha)(1-p)}{(1-\alpha)(1-p) + \gamma p}, \tag{10}$$

$$1 - p_2 = P(I \mid NA) = \frac{P(NA \mid I)P(I)}{P(NA)} = \frac{\gamma p}{p_1} = \\ = \frac{\gamma p}{(1-\alpha)(1-p) + \gamma p}, \tag{11}$$

$$p_3 = P(NI \mid A) = \frac{P(A \mid NI)P(NI)}{P(A)} = \\ = \frac{\alpha(1-p)}{\alpha(1-p) + (1-\gamma)p}, \tag{12}$$

$$1 - p_3 = P(I \mid A) = \frac{P(A \mid I)P(I)}{P(A)} = \\ = \frac{(1-\gamma)p}{\alpha(1-p) + (1-\gamma)p}. \tag{13}$$

Ожидаемая стоимость, которая зависит от отчета детектора, математически отображается путем нахождения суммы произведений вероятностей вместе со стоимостью узла после ответа. В любой рабочей точке ожидаемая стоимость эксплуатации СОВ дается в уравнениях

$$C_{EX} = \frac{p_1 \min\{C\gamma p, (1-\alpha)(1-p)\}}{p_1} + \\ + \frac{(1-p_1)\min\{C(1-\gamma)p, \alpha(1-p)}{1-p_1}, \tag{14}$$

$$C_{EX} = \min\{C\gamma p, (1-\alpha)(1-p)\} + \\ + \min\{C(1-\gamma)p, \alpha(1-p)\}. \tag{15}$$

На практике оптимальная рабочая точка описывается как наиболее подходящая точка, достижимая данной СОВ с точки зрения ее возможностей обнаружения вторжений и минимизации ожидаемой стоимости. Следовательно, выбор оптимальной рабочей точки будет эквивалентен лучшему выбору значений для параметров α и γ, которые могут обеспечить желаемую наименьшую ожидаемую стоимость.

Чтобы ввести функцию стоимости в C_{ID}, используем метод анализа дерева решений. Рассчитываем соответствующую стоимость, прикрепленную к каждому значению C_{ID}, чтобы получить приемлемый компромисс между стоимостью и возможностями. Для этого значения C_{ID} и C_{EX} наносятся на график относительно α. Самая низкая точка на кривой C_{EX} совпадает с самой высокой точкой на кривой C_{ID}. Наблюдаемые отклонения в значениях ожидаемой стоимости могут быть очень полезной метрикой, подходящей для сравнения двух детекторов вторжения.

Результаты значений C_{ID} были рассчитаны с использованием данных, извлеченных из двух кривых ROC, представленных в [1]. Здесь две ROC-кривые используются для представления двух систем обнаружения вторжений, обозначенных как IDS_1 и IDS_2.

Первоначальные результаты показали, что в 666000 сетевых сеансов в течение обычного дня было обнаружено около 43 попыток вторжения. Исходя из предположения о том, что ответы на вторжение достигаются за сеанс каждый раз, когда применяются детекторы вторжения, базовая скорость задается как

$$B = \frac{\text{Общее число попыток вторжения}}{\text{Общее число сеансов}} = \\ = \frac{43}{660000} = 6{,}52 \cdot 10^{-5}. \tag{16}$$

Кривая ROC IDS_1 может быть аппроксимирована

$$1 - \gamma = 0{,}6909 \cdot (1 - \exp(-65625{,}64\alpha^{1{,}19})), \tag{17}$$

$$1 - \gamma = 0{,}4909 \cdot (1 - \exp(-11932{,}6\alpha^{1{,}19})), \tag{18}$$

Результаты, полученные в результате оценки вероятности вторжения, представлены на рис. 3 и 4 для COB_1 и COB_2 соответственно.

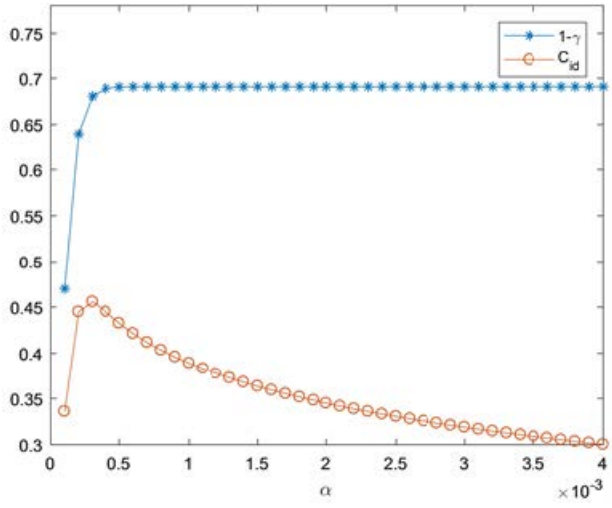

Рис. 3. График значений C_{ID}, рассчитанных для COB_1

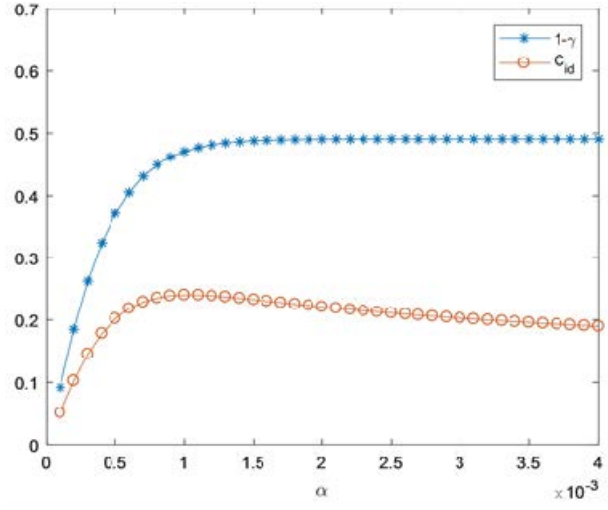

Рис. 4. График значений C_{ID}, рассчитанных для COB_2

На практике точка, в которой самая высокая способность обнаружения вторжения и ее предельное значение, называется оптимальной рабочей точкой. Здесь оптимальная рабочая точка для COB_1 происходит при $\alpha = 0{,}0003$, $1 - \gamma = 0{,}6807$, соответствующем C_{ID} 0,45567, в то время как точка COB_2 находится при $\alpha = 0{,}001$, $1 - \gamma = 0{,}47112$ и C_{ID} 0,2403. Исходя из вышеизложенного, COB_2 достигает лучшей возможности обнаружения, чем COB_1 . Расширяя сравнение двух детекторов на основе приведенного выше анализа, мы можем сделать вывод, что COB_2 лучше, чем COB_1. Однако это не касается затрат на эксплуатацию в выбранной оптимальной точке.

Для нахождения минимальной ожидаемой рабочей точки используется дерево решений, приведенное на рис. 2. Здесь дерево оценивается справа налево. Например, если соотношение затрат $C = 1000$, то не отреагировать на вторжение может быть в тысячу раз дороже, чем ложно отреагировать на отсутствие вторжения. Предположим также, что базовая скорость (вероятность проникновения) по-прежнему равна $6{,}52 \cdot 10^{-5}$.

Из рис. 5, максимальное значение C_{ID} для COB_1 находится при $\alpha = 0{,}0003$, с $C_{ID} = 0{,}4557$. Минимальная соответствующая стоимость, возникающая при $\alpha = 0{,}0003$, $C_{EX} = 0{,}0211$. Следовательно, оптимальная рабочая точка для COB_1 составляет (0,4557; 0,0211).

Из рис. 6, максимальное отношение C_{ID} для COB_2 находится при $\alpha = 0{,}0010$, с $C_{ID} = 0{,}2403$. Минимальная соответствующая стоимость, возникающая при $\alpha = 0{,}0010$, $C_{EX} = 0{,}0355$. Таким образом, оптимальная рабочая точка для COB_2 составляет (0,2403; 0,0355).

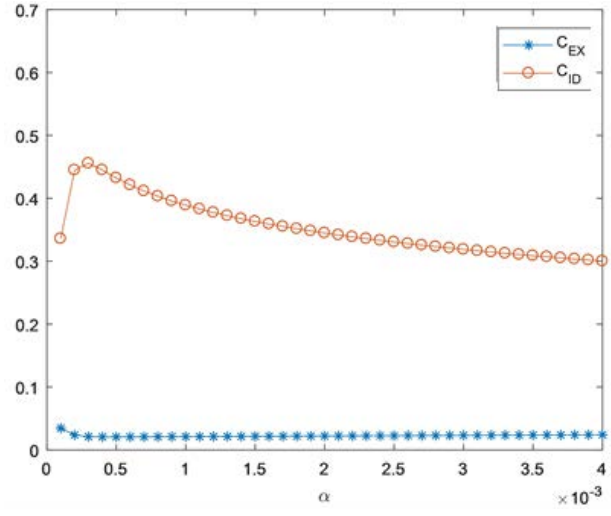

Рис. 5. График значений C_{ID} и C_{EX}, рассчитанных для COB_1

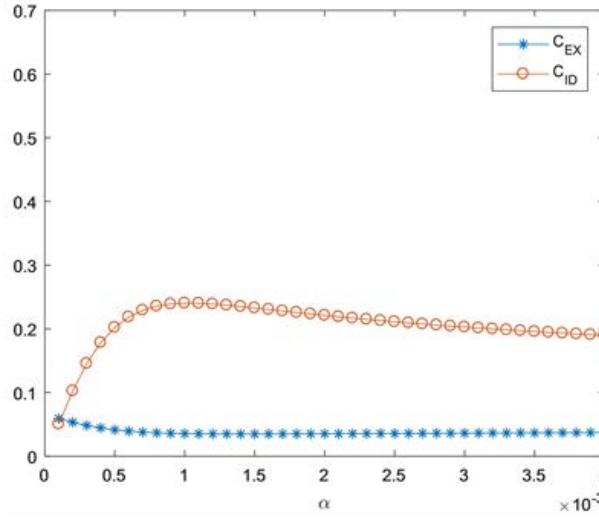

Рис. 6. График значений C_{ID} и C_{EX}, рассчитанных для COB_2

Сравнение COB_1 и COB_2 приведено в таблице.

Сравнение COB_1 и COB_2

	COB_1	COB_2
α	0,0003	0,0010
$1 - \gamma$	0,3699	0,4711
C_{ID}	0,4557	0,2403
C_{EX}	0,0211	0,0355

Видно что, COB_1 является лучшим детектором с C_{ID} = 0,2154 за сеанс выше, чем C_{ID} COB_2 и ожидаемой стоимостью C_{EX} = 0,0144 за сеанс меньше, чем C_{EX} COB_2.

В теории, COB можно не принимать во внимание значение базовой скорости, но это очень важный фактор, который следует учитывать при представлении отчетов о возможностях обнаружения вторжений, поскольку базовая скорость определяет среду работы. Влияние различных базовых скоростей на C_{ID} показано на рис. 7.

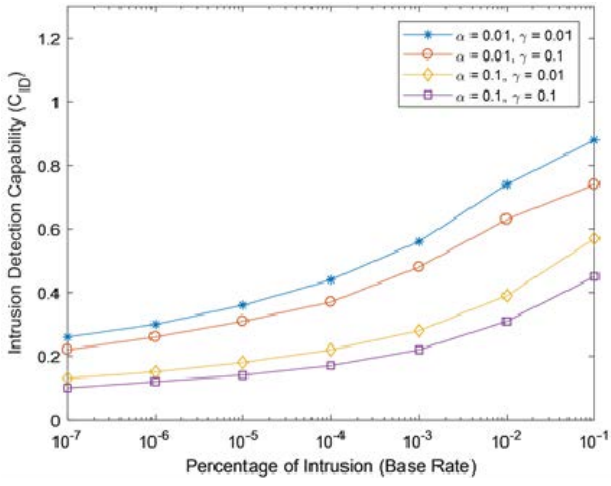

Рис.7. Влияние базовых скоростей на C_{ID}

Из рис. 7 видно, что C_{ID} более чувствительна к изменениям ложноположительного значения (FP), чем ложноотрицательного (FN). Следовательно, для низких базовых скоростей уменьшение FP улучшит C_{ID} больше, чем такое же снижение FN.

При постоянной базовой скорости даже небольшие изменения в FP приводят к большим изменениям в C_{ID}, что представлено на рис. 8. В то время как FN оказывает влияние на C_{ID} только при больших изменениях, что показано на рис. 9.

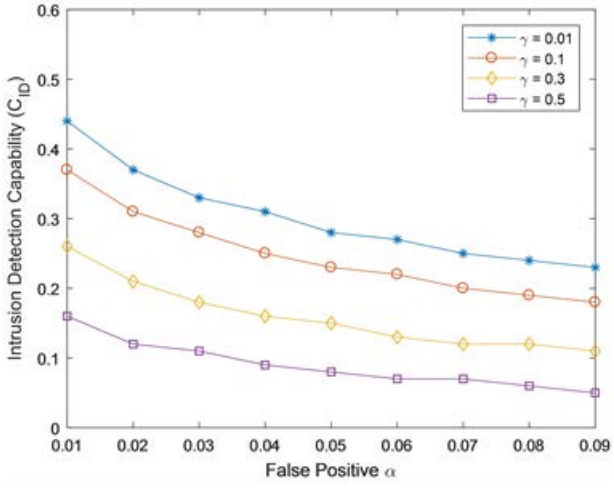

Рис. 8. Влияние FP (α) на C_{ID}

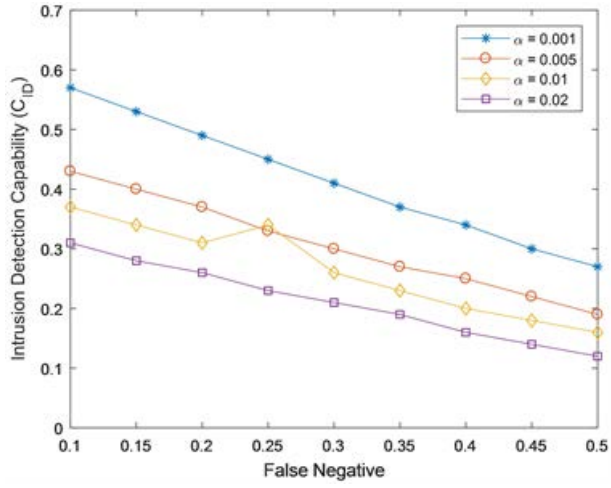

Рис. 9. Влияние FN (γ) на C_{ID}

Основным недостатком анализа ожидаемых затрат, является то, что соотношение затрат C выбирается субъективно. Таким образом, рассматривается влияние соотношения затрат на ожидаемую стоимость.

Из рис. 10 видно, что резкое падение ожидаемой стоимости составляет от α = 0,0001 и α = 0,0002. Поскольку FP увеличивается, ожидаемая стоимость остается довольно постоянной. Это наглядно доказывает, что для минимизации ожидаемой стоимости обязательно, чтобы FP (α) был низкой.

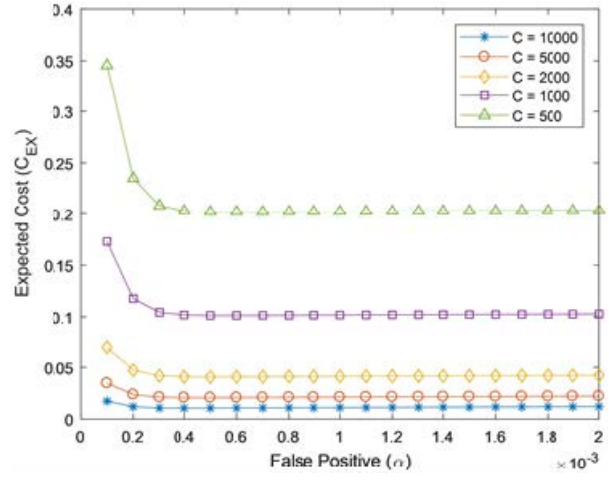

Рис. 10. Влияние соотношения затрат C на ожидаемые затраты C_{EX}

В реальной рабочей среде можно резонно предположить, что значения должны соответствовать условию

$$B < \alpha << \gamma < 1. \quad (19)$$

В этой работе рассмотрено расширение возможностей систем обнаружения вторжений на основе затрат (C_{ID}). Уровень затрат в каждой рабочей точке COB, определяется анализом дерева решений. Также были построены графики ожидаемой стоимости и возможности обнаружения вторжения в зависимости от заданного уровня ложноположительных результатов. Точка пересечения между максимальной способностью обнаружения вторжения и ожидаемой

стоимостью выбирается в качестве оптимальной рабочей точки.

Расширение на основе затрат используется для выбора оптимальной рабочей точки, расчета ожидаемой стоимости и сравнения двух фактических СОВ. Предлагаемое расширение возможностей системы обнаружения вторжений на основе затрат будет очень полезно для информационных технологий для принятия надлежащих решений при оценке пригодности СОВ для конкретной операционной среды.

Список литературы

1. Gandhi M. and Srivatsa S. Detecting and Preventing Attacks Using Network Intrusion Detection Systems // International Journal of Computer Science and Security. 2008. N 2. P. 49-58.

2. Gu G., Fogla P., Dagon D., Lee W. and Skoric B. Measuring Intrusion Detection Capability: An Information-Theoretic Approach. Proceedings of the 2006 ACM Symposium on Information // Computer and Communications Security. 2006. N. 3. P. 90–101.

3. Popoola E. and Adewumi A.O. Efficient Feature Selection Technique for Network Intrusion Detection System Using Discrete Differential Evolution and Decision // International Journal of Network Security. 2017. N 19. P. 600–669.

4. Singh M. and Pathak S. Xb@nd Implementation for Intrusion Detection System // International Journal of Engineering Research and Technology. 2012. N. 1. P. 1–6.