МАТЕРІАЛОЗНАВСТВО

УДК 004.056.53

С. В. БАЛАКИН

ОРГАНИЗАЦИЯ ПРЕСЕЧЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫЕ СЕТИ АЛГОРИТМАМИ ВЫЯВЛЕНИЯ ИЗМЕНЕНИЙ

Розглядається моделювання системи постановки діагнозу шляхом аналізу ймовірності достовірності оцінки різних наборів станів структури проникнення комбінованих доказів симптомів для дерева діагностики, представленого деревом специфікації, щоб максимально точно визначити захищеність системи чи організму. Дослідження полягає в наданні необхідної теоретичної бази для використання приведених концепцій і теорій, які можуть комбінуватися з сучасними напрацюваннями для підвищення результатів ефективності виявлення вторгнень в комп'ютерній мережі.

Ключові слова: моделювання, діагностика, діагноз, вторгнення, алгоритми змін, теорія Демпстера-Шефера, комп'ютерна мережа, основне переконання, правдоподібність, проникливість.

Рассматривается моделирование системы постановки диагноза путем анализа вероятности достоверности различных наборов состояний в структуре проникновения и комбинированных доказательств симптомов для дерева диагностики, представленного деревом спецификации, чтобы максимально точно определить защищенность системы или организма. Исследование заключается в предоставлении необходимой теоретической базы для использования приведенных концепций и теорий, которые могут комбинироваться с современными наработками для повышения результатов эффективности обнаружения вторжений в компьютерной сети.

Ключевые слова: моделирование, диагностика, диагноз, вторжения, алгоритмы изменений, теория Демпстера-Шефера, компьютерная сеть, основное убеждение, правдоподобность, проницательность.

The modeling of the diagnostic system is considered. Analyzing the probability of estimating the various sets of states of the structure of the penetration of the combined evidence of symptoms for the diagnostic tree is presented by the specification tree in order to ascertain precisely the security of the system or organism. Main aim of the study is to provide the necessary theoretical basis for using the above concepts and theories that can be combined with current develOПments to enhance the effectiveness of detecting intrusions in a computer network. Given description shows improved results that can improve diagnosis functions and can be used in real-time computer systems.

Keywords: Modeling, diagnosis, diagnosis, invasion, algorithms of change, Dempster-Shafer theory, computer network, basic belief, plausibility, insight.

Введение. В области компьютерной безопасности много ресурсов направлено на повышение эффективности защиты пользователей от несанкционированных действий. Одним из способов повышения безопасности компьютерной системы является использование систем обнаружения вторжений (СОВ). Метод диагностирования очень тесно связан с СОВ, но основан на принципах и способах развитых в медицине. С помощью информатизации в сфере медицины становится возможным и развитие новых вех компьютерных технологий. Основная сложность при их проектировании - это подбор правильной технологической и методологической базы, что позволит применить такие методы в реальных условиях. Эти методы получили название диагностическое обнаружения вторжений (ДОВ).

В ДОВ мониторятся соответствующие функции системы, таким же образом как в медицине проводится обследование при симптомах болезни. Симптомы используют значение обследований, чтобы вычислить вероятность обнаружения определенного недуга в организме человека. Теория Демпстера-Шафера (ТДШ) применяется для характеристики таких убеждений, оперируя основными понятиями по комбинированию и использованию операторов слияния.

Разработанная система постановки диагноза путем анализа вероятности достоверности оценки различных наборов состояний структуры проникновения комбинированных доказательств симптомов для дерева диагностики, представленного деревом спецификации, чтобы максимально точно определить защищенность системы или организма.

Анализ литературных данных и постановка проблемы. Существующие программные решения имеют определенную поддержку с точки зрения предотвращения и обнаружения вторжений, но в них отсутствует возможность диагностирования. Данные системы имеют недостатки в своевременности детектирования атак, но использование методов диагностирования может положительно повлиять на быстродействие и надежность известных методов, минимизируя затраты на проведение мониторинга сети и потоков. Основная идея заключается в сборе информации на нескольких архитектурных уровнях, с использованием нескольких фильтров безопасности для выполнения корреляционного анализа симптомов вторжения. Много таких работ базируется на теории Демпстер-Шафера (ТДШ), которая разработана Гленном Шафером и Артуром Демпстер и описана в работах [15, 63]. Теория отрабатывалась и развивалась в работах [14, 64, 88, 84, 62].

Идея сбора информации от источников принадлежит Джону Ф.Ф., и обосновывает само понятие атаки. Данные наработки были описаны теоретически в работах [3], [4] и [5]. Представленные работы используют понятие корреляции и мультианализа, но не решают проблему диагностики аномалий в системе. Актуальность данной статьи в том, что данная технология может расширить возможности систем обнаружения вторжений поднимая их на качественно новый уровень.

Цель и задачи исследования. Целью исследования является определение уровня развития рассматриваемых технологий, реализующих обнаружения вторжений в компьютерных сетях, с целью улучшения их эффективности.

Задачей исследования является обоснование актуальности использования указанных методов и возможности их внедрения в производство.

Для достижения поставленной цели были поставлены следующие задачи:

1. Исследование инструментальной базы для реализации диагностирования несанкционированных действий и подбор основных операторов.

2. Разработана математическая модель процесса диагностирования несанкционированных действий в компьютерных сетях посредством использования операторов теории Демпстера-Шефера (ТДШ), которая позволяет своевременно реагировать на нарушения работы системы и точно выявлять тип нарушения.

Выбор инструментальной базы для реализации диагностирования. Цель исследования заключается в предоставлении необходимой теоретической базы для использования приведенных концепций и теорий, которые могут комбинироваться с современными наработками для повышения эффективности обнаружения вторжений в компьютерной сети. Рассмотрены основные алгоритмы обнаружения изменения, потому что они будут использоваться при диагностике для контроля временных фрагментов и формирования данных для определения симптомов и сигнатур вторжений. ТДШ может объединить отдельные части доказательств для получения конечного результата и установление выводу о наличии или отсутствии вторжений (диагноз). ТДШ обладает всеми свойствами, которые могут помочь выявлять вторжения и несанкционированные действия в компьютерной сети.

Объектом исследования является процесс организации обнаружения вторжений и несанкционированных действий в сети.

Предметом исследования являются параметры операторов теории Демпстера-Шефера, с помощью которых будет реализовываться математическая модель диагностирования обнаружения вторжений.

В ТДШ все возможные состояния процесса можно описать с помощью структуры проницательности. Структура проницательности определяется массивом S = {S1, S2 ,… , SN}, де для 1 ≤ i ≤ N, Si определяет конкретное состояние системы. ТДШ применяется при определении «состояния процесса», потому что он позволяет установить диагноз и на его основе сделать вывод о наличии аномалий в системе.

Главной целью ТДШ есть на основе наблюдений и собранных доказательств определения вероятности того, насколько данное состояние Si является фактическим состоянием процесса. Диагноз формируется на основе доказательств ТДШ. DST формирует доказательства по достижении уровня уверенности в них, и такой результат называется основным убеждениям (ОП). Формально ОП представляет собой связанную структуру проникновения. fs отражает любую подмножество структуры проникновения для реального значения, fs: P(S) → R. Значение области представляет собой набор поддерживаемых состояний, а соответствующее значение диапазона представляет силу этой поддержки.

ОП это совокупность всех возможных «претензий», которые могут возникнуть в процессе в рамках конкретной структуры проникновения. Любой набор состояний, которому присваивается ненулевая масса, свидетельствует, что процесс может быть в одном из этих состояний. Присвоение нулевой массы означает, что процесс отсутствует. Используя описанные выше конструкции можно перейти к применению ТДШ. Нижняя граница субъективной вероятности (убеждения) (bl) вычисляется по формуле,

$$bl(f_s B A) = \sum_{B \subseteq A} f_s(\ )$$

где S - структура проницательности, fS - является ОП, и A будет набором состояний. Формула заключает, что масса убеждения содержится непосредственно во всех подмножествах наборов опрашиваемых и обычных состояний.

Верхний предел субъективной вероятности (правдоподобие) (pl) вычисляется формулой

$$pl(f_s B A) = \sum_{B \cap A \neq \varnothing} f_s(\ )$$

где переменные имеют такие же значения, как и в состояниях убеждения. Формула заключает, что массы убеждения любых состояний имеют по крайней мере один общий с опрашиваемым состояние.

Правдоподобие и убеждения связаны через уравнение $pl(f_s, A) = 1 - bl(f_s, S \setminus A)$ которое отражает альтернативную интерпретацию правдоподобия, где правдоподобие в A является остатками уверенности в A, после того как в A было добавлено правдоподобие. Получается, что нет возможности для отклонения текущего состояния от структуры проницательности, и эта структура гарантированно будет содержать данное состояние.

Операторы слияния в ТДШ могут скомпоновать вместе несколько доказательств по ОТ для формирования конечных ОП. Оператор слияния - это любая функция, которая принимает на входе две ОП, а в качестве выходного сигнала выдает одну (с условием что все ОП находятся в одной структуре проницательности).

Операторы слияния в ТДШ описываются уравнениями,

$$n(S, A_s, B_s) = \sum_{x,y \in P(S) \boxtimes \cap y = 0} A_s(x) B_s(y)$$

$$C_s(\varnothing) = dfo(S, A_s, B_s, \varnothing) = 0$$

Входные ОП (A_s, B_s) и виходные (C_s) находятся в одной структуре проницательности S. Вспомогательная функция n (когда заданные два ОП одной структуры проницательности) вычисляет общее количество масс в противоречивых друг другу частях доказательств (когда множества переходов не имеют

общих состояний) A_s, и B_s. Для конкретной множества состояний $z \in P(S)$, правило Демпстера DFO вычисляет общую массу, которая поддерживает z и добавляет массу с любого множества состояний A_s, и B_s, разделяющих z как общее состояние. Следует отметить, что полностью противоречивые данные не будут иметь общего состояния, поэтому такая масса не будет учитываться (потому что в случае $z = \varnothing$, где эти значения будут учитываться, $C_s(\varnothing) = dfo(S, A_s, B_s, \varnothing) = 0$ масса «исчезает»).

Важно определять когда поведение процесса отклоняется от предварительно определенной спецификации (то есть она претерпела «изменений»).

Обозначим алгоритм выявления изменений функцией C, для представления полученных с помощью мониторинга значений. Функция работает так же как и преобразования временных рядов, принимая временной ряд T, в качестве входных данных, и *C(T) = T′* в качестве выходного сигнала. Базовый тип временных фрагментов не ограничивается, однако C должен быть двоичным. Разрешены только значения {0, 1, NM}. Ввод и вывод временных фрагментов должно содержать равное количество значений $T_n = T_n'$, так же интервалы времени $T_p = T_p'$, а также одинаковое время возникновения для всех соответствующих индексов, $\forall_i \mid 0 \le i < T_n,\ t_i(T) = t_i'(T')$. При индексе и с временных рядов T, выход C, *C(T)(i) = T′(i)*, следует оценить в 0, если никаких изменений не обнаружено. *T′(i)* следует оценивать в 1, если изменение обнаружено и процесс отражает поведение, отклоняющееся от определенной модели (то есть, сигнал активный). Алгоритм обнаружения изменения CUSUM работает следующим образом. Пусть csm (T, ul, μ, σ, a) функция обнаружения изменения CUSUM, где T будет функцией ввода временных фрагментов, ul будет верхним / нижним селектором CUSUM, μ будет средним отклонением, σ будет стандартным отклонением, и a будет порогом тревоги.

Тип ввода временных фрагментов T, должен иметь строгий полный порядок, а также поддержку сложение и вычитание операций. ul это двоичное значение ul ε {0, 1}, представляющий верхний селектор при ul = 1, или нижний при ul = 0 в CUSUM алгоритме. μ и σ должны иметь тот же тип, что и временные фрагменты и представляют собой «нормальное» среднее и стандартное отклонение основного процесса. a - порог сигнализации, также разделяет тип временных фрагментов. Для данного индекса $i|0 \le i < T_n$ временных рядов *T, T(i),* значение CUSUM по индексу и задается следующим образом:

$$\mathrm{csm}(T, \mathrm{ul}, \mu, \sigma, a)_t(i) = i_t(\mathrm{ul} \neq \mathrm{ul} \quad 0$$

Если предположить, что при среднего значения μ будет фактическим ожидаемым значением основного процесса временных рядов, то потом значение CUSUM должны оставаться приближенными к нулю. Из этого следует, что значение параметра ul определяет, когда алгоритм отслеживает аномальное поведение в обоих направлениях. Фактический выход алгоритма обнаружения изменения определяется в каждый момент времени $T_t(i)$, путем сравнения текущего значения CUSUM с порогом тревоги a. Если порог превышен то возвращается 1, и это значит что процесс проявляет девиантное поведение. В противном случае возвращается 0, и процесс показывает нормальное поведение. При определении разницы между значениями временных рядов и ожидаемых значений T (i) - μ - это стандартизированная величина, в качестве условия использует значение отклонения σ. Это позволяет определить порог тревоги (a) для стандартных отклонений от ожидаемого значения процесса, используя всего лишь одно значение с порога тревоги a для вызовов функции CSM с различными значениями μ и σ.

Основой диагностики будет дерево спецификаций, используется для представления всех диагнозов в которых может находиться система S. Такую систему можно назвать деревом диагностирования. Симптом принимает значение наблюдаемых в момент времени t, и выдает на выходе ОП по сравнению с DT_f, что обеспечивает возможность диагностики S. Симптомы получают новые данные о наблюдаемых как только они становятся доступными, а по определению временных фрагментов они доступны через одинаковые промежутки времени. Симптомы поддерживают и принимают решения на основе внутренних состояний, таким образом одинаковые значения могут подаваться в симптом несколько раз, а это может привести к различным ОП на выходе. пусть набор ST_n симптомов представляется как

ST = $\{st_0, st_1, \ldots, st_{ST_{n-1}}\}$, где $st \in ST$, или $st_i \in ST$, где $0 \le i < ST_n$, относится к какому-либо конкретному симптому. Наблюдаемый, связанный с каждым симптомом, определяется функцией STO, которая принимает симптом и возвращает соответствующее значение наблюдения на выходе. Значение симптома st в момент времени t, определяется через *st(STO(st)(t)).*

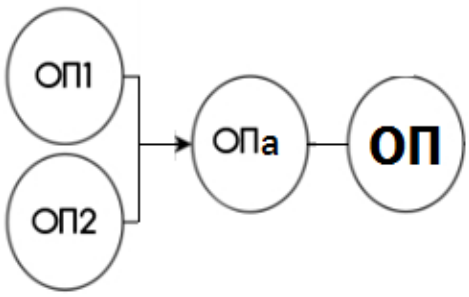

Рис. 1 – Комбинация ОП

Для постановки диагноза состояния S, нужно иметь целостную ОП. Необходимо соединить наборы

ОП для формирования единой ОП, которая будет отражать их суть. Сочетание ОП проводится операторами слияния DST. Это позволит сформировать набор независимых основ убеждений, будут эквивалентны по размеру к числу зависимых групп. В дальнейшем независимые ОП образуют конечную ОП. Пример такого процесса показан на рис. 1.

На заключительном этапе определяется, находится S в состоянии конкретной атаки a из массива связанных классов атак a∈ac. Каждая атака с DST будет содержать элемент из массива атак $\{a\} \subset A$. Вера и достоверность вычисляется для каждой атаки: $bl(B_{DT_f}, \{a\})$, $pl(B_{DT_f}, \{a\})$, $\forall\{a\} \in ac$. Если ни одна из вершин атак не обнаруживается, то система находится в состоянии неизвестной атаки и процесс диагностики заканчивается. Если обнаружена вершина атаки, то выбирается атака с наибольшей субъективной вероятностью, и система считается под угрозой этой конкретной атаки. После этого процесс диагностики заканчивается.

Проведенные исследования параметров операторов ТДШ доказали, что их использование в описанной последовательности позволят устанавливать симптомы и на их основе получить корректный диагноз.

Результаты исследования вторжений в компьютерные сети алгоритмами выявления изменений. В результате было проверено достоверность и возможности диагностирования при обнаружении атак и несанкционированных действий. Исследование происходило при одновременном или комбинированном запуска всех узлов, для того чтобы система могла диагностировать наличие НД. Реализована структура дерева диагностирования для работы с определенными типами атак, а также для реализации новых, неизвестных системе атак.

Для сравнения результатов приведена таблица с характеристиками работы предложенного метода, и метода-аналога, которые были протестированы с одинаковыми наборами входных данных. Результаты свидетельствуют, что данный метод значительно превосходит по эффективности выявления аналог (92 % против 54 %), при сравнительно одинаковой нагрузке на ЦП (табл. 1).

Таблица 1 – Результат сравнения методов

	Кол. угроз	% Определения	Время работы	Загрузка ЦП, %
ТДШ	44	92	12сек	32
DDIS(аналог)	26	54	16сек	31

Выводы. В ходе выполнения данной статьи было выполнено:

1. Исследование инструментальной базы для реализации диагностирования несанкционированных действий и подбор основных операторов.

2. Разработана математическая модель диагностирования несанкционированных действий в компьютерных сетях посредством использования операторов теории Демпстера-Шефера (ТДШ), которая позволяет своевременно реагировать на нарушения работы системы и точно выявлять тип нарушения.

3. Были проведены обзор и анализ существующих аналогов, что реализуют функции предметной области.

Выполненная работа будет использована для дальнейших исследований в данной области.

Список літератури:

1. Denning, D. E. An Intrusion-Detection Model [Text] / D. E. Denning // 1986 IEEE Symposium on Security and Privacy. – 1986. doi: 10.1109/sp.1986.10010
2. Sheyner, O. Scenario Graphs and Attacks [Text]: PhD thesis / O. Sheyner. – SCS, Carnegie Mellon University, 2004. – 141 p.
3. Kvarnström, H. A survey of commercial tools for diagnosis detection [Text] / H. Kvarnström. – Technical Report, Chalmers University, 1999. – 99 p.
4. Edward, G. Intrusion Detection [Text] / G. Edward. – 1st ed. – Intrusion.Net Books, Sparta, New Jersey, USA, 1999. – 218 p.
5. Eckmann, S. T. STATL: An attack language for state-based intrusion detection [Text] / S. T. Eckmann, G. Vigna, R. A. Kemmerer // Journal of Computer Security. – 2002. – Vol. 10, Issue 1-2. – P. 71–103. doi: 10.3233/jcs-2002-101-204
6. Dempster, A. P. Upper and Lower Probabilities Induced by a Multivalued Mapping [Text] / A. P. Dempster // The Annals of Mathematical Statistics. – 1967. – Vol. 38, Issue 2. – P. 325–339. doi: 10.1214/aoms/1177698950
7. Klir, G. J. Is there more to uncertainty than some probability theorists might have us believe?* [Text] / G. J. Klir // International Journal of General Systems. – 1989. – Vol. 15, Issue 4. – P. 347–378. doi: 10.1080/03081078908935057
8. Yager, R. R. Arithmetic and other operations on Dempster-Shafer structures [Text] / R. R. Yager // International Journal of Man-Machine Studies. – 1986. – Vol. 25, Issue 4. – P. 357–366. doi: 10.1016/s0020-7373(86)80066-9
9. Yager, R. R. On the dempster-shafer framework and new combination rules [Text] / R. R. Yager // Information Sciences. – 1987. – Vol. 41, Issue 2. – P. 93–137. doi: 10.1016/0020-0255(87)90007-7
10. Yager, R. R. Quasi-associative operations in the combination of evidence [Text] / R. R. Yager // Kybernetes. – 1987. – Vol. 16, Issue 1. – P. 37–41. doi: 10.1108/eb005755

Bibliography (transliterated):

1. Denning, D. E. (1986). An Intrusion-Detection Model. 1986 IEEE Symposium on Security and Privacy. doi: 10.1109/sp.1986.10010
2. Sheyner, O. (2004). Scenario Graphs and Attacks. SCS, Carnegie Mellon University, 141.
3. Kvarnström, H. (1999). A survey of commercial tools for diagnosis detection. Technical Report, Chalmers University, 99.
4. Edward, G. (1999). Intrusion Detection. Intrusion.Net Books, Sparta, New Jersey, USA, 218.
5. Eckmann, S. T., Vigna, G., Kemmerer, R. A. (2002). STATL: An attack language for state-based intrusion detection. Journal of Computer Security, 10 (1-2), 71–103. doi: 10.3233/jcs-2002-101-204
6. Dempster, A. P. (1967). Upper and Lower Probabilities Induced by a Multivalued Mapping. The Annals of Mathematical Statistics, 38 (2), 325–339. doi: 10.1214/aoms/1177698950
7. Klir, G. J. (1989). Is there more to uncertainty than some probability theorists might have us believe?* International Journal of General Systems, 15 (4), 347–378. doi: 10.1080/03081078908935057
8. Yager, R. R. (1986). Arithmetic and other operations on Dempster-Shafer structures. International Journal of Man-Machine Studies, 25 (4), 357–366. doi: 10.1016/s0020-7373(86)80066-9

9. Yager, R. R. (1987). On the dempster-shafer framework and new combination rules. Information Sciences, 41 (2), 93–137. doi: 10.1016/0020-0255(87)90007-7

10. Yager, R. R. (1987). Quasi-associative operations in the combination of evidence. Kybernetes, 16 (1), 37–41. doi: 10.1108/eb005755

Поступила (received) 20.07.2017

Бібліографічні описи / Библиографические описания / Bibliographic descriptions

Організація запобігання вторгнень в комп'ютерні мережі алгоритмами виявлення змін/ Балакін С. В. // Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2017. – No 20(1242). – С.3–7. – Бібліогр.: 10 назв. – ISSN 2079-5459.

Организация пресечения вторжений в компьютерные сети алгоритмами выявления изменений/ Балакин С. В. // Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2017. – No 20(1242). – С.3–7. – Бібліогр.: 10 назв. – ISSN 2079-5459.

Organization of prevention of intrusions in computer networks using algorithms for detecting changes / Balakin S. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 20 (1242).– P.3–7. – Bibliogr.:10. – ISSN 2079-5459

Відомості про авторів / Сведения об авторах / About the Authors

Балакін Сергій В'ячеславович – аспірант, Київський національний авіаційний університет, аспірант Кафедри комп'ютерних систем та мереж; проспект Космонавта Комарова, 1, м. Київ, Україна, 02000

Балакин Сергей Вячеславович – аспирант, Киевский национальный авиационный университет, аспирант Кафедри компьютерних систем и сетей; проспект Космонавта Комарова, 1, г. Киев, Украина, 02000; e-mail: desertq@mail.ua

Balakin Sergii – graduate student, Kyiv national aviational university; eve. Kosmonavta Komarova 1, Kyiv, Ukraine, 02000; e-mail: desertq@mail.ua

УДК 62-278

С. В. САВЧЕНКО, Г. С. ТИМЧИК

МЕТОД КОНТРОЛЯ СВАРНИХ СОЕДИНЕНИЙ БАЛЛИСТИЧЕСКИХ СТАЛЕЙ ПОСРЕДСТВОМ АКУСТИЧЕСКОЙ ЭМИССИИ

Рассматривается применение метода акустической эмиссии (АЭ) для контроля сварных соединений баллистических сталей AR. В основе метода лежит физическое явление излучения волн напряжений при быстрой локальной перестройке структуры материала. Исследование проводилось при снятии нагрузки с образца с применением широкополосных акустических пьезодатчиков и новой системой градуировки датчиков АЭ. Была выполнена стыковка системы градуировки с персональным компьютером, разработано специальное программное обеспечение, позволяющее в полуавтоматическом режиме получать амплитудно-частотную характеристику каждого датчика.

Ключевые слова: акустическая эмиссия, контроль сварных швов, баллистическая сталь, пьезодатчик, неразрушающий контроль, средство защиты.

Розглядається застосування методу акустичної емісії (АЕ) для контролю зварних з'єднань балістичних сталей AR. В основі методу лежить фізичне явище випромінювання хвиль напружень при швидкій локальній перебудові структури матеріалу. Дослідження проводилося при знятті навантаження зі зразка із застосуванням широкосмугових акустичних п'єзодатчиків і новою системою градуювання датчиків АЕ. Була виконана стиковка системи градуювання з персональним комп'ютером, розроблено спеціальне програмне забезпечення, що дозволяє в напівавтоматичному режимі отримувати амплітудно-частотну характеристику кожного датчика.

Ключові слова: акустична емісія, контроль зварних швів, балістична сталь, п'єзодатчик, неруйнівний контроль, засіб захисту.

The application of the acoustic emission method (AE) for the control of welded joints of ballistic steel AR is considered. The method is based on the physical phenomenon of radiation of stress waves during fast local rearrangement of the material structure. The study was carried out with the removal of the load from the sample using broadband acoustic piezoelectric sensors and a new system for calibrating the AE sensors. The calibration system was mapped to a personal computer, special software was developed that allows the semi-automatic mode to obtain the amplitude-frequency response of each sensor.

The use of this method of finding weld defects gives high accuracy and efficiency and allows a tangible reduction in costs and production time. A promising direction is the development of methods for filtering the acoustic signal to increase the accuracy of the method of control.

Keywords: acoustic emission, control of welded joints, ballistic steel, piezoelectric sensor, non-destructive testing, protective equipment.

Введение. Военная промышленность и сфера, связанная с системой безопасности, являются лидерами по максимальному внедрению новейших технологий. Современное оружие дает толчок для развития новейших средств защиты от нее, среди которых баллистическая сталь один из самых ярких представителей. Армия, полиция, различные частные охранные агентства, службы безопасности, а также инкассаторы - вот где используются как современные виды вооружений, так и системы защиты от них.

Изготовление баллистической стали и конструкций из нее, имеет ряд технологических сложностей. Одна из основных проблем это свариваемость этих