DOI: 10.18372/2410-7840.19.11902
УДК 004.056.53(045)

МОДЕЛИ ЭТАЛОНОВ ЛИНГВИСТИЧЕСКИХ ПЕРЕМЕННЫХ ДЛЯ ОБНАРУЖЕНИЯ СНИФФИНГ-АТАК

Игорь Терейковский, Анна Корченко, Павел Викулов, Александра Шаховал

Интенсивное развитие информационных систем привело к увеличению разрушающего программного обеспечения, множество которого направлено на получение конфиденциальной информации, что непосредственно связано с появлением атак типа 0-day и несигнатурных типов кибератак. Расширение воздействий кибератак направленных на различные ресурсы информационных систем инициирует создание специальных средств противодействия, способных оставаться эффективными при появлении новых видов угроз с неустановленными или нечетко определенными свойствами. Известны достаточно эффективные разработки, используемые для решения задач выявления кибератак, например, метод формирования лингвистических эталонов для систем выявления вторжений, в котором не раскрыт механизм процесса формирования эталонов параметров для сниффинг-атак. С этой целью разработана модель эталонов лингвистических переменных для обнаружения сниффинг-атак, которая, за счет оценки состояния информационной системы и процесса формирования эталонов параметров: количество входящих пакетов в сети, скорость обработки пакетов на стороне получателя, тайминг пакетов в канале, позволит формализовать процесс получения эталонов параметров для заданных лингвистических переменных конкретной среды окружения при решении задач выявления атак в компьютерных системах. Такие модели могут быть использованы для повышения эффективности средств информационной безопасности, направленные на противодействие сниффинг-атак в компьютерных сетях.

Ключевые слова: *атаки, кибератаки, аномалии, методы формирования лингвистических эталонов, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, обнаружение аномалий в компьютерных сетях.*

На сегодняшний день стремительное развитие информационных систем привело к расширению различных типов разрушающего программного обеспечения (ПО), воздействующего на ресурсы информационных систем (РИС). Множество такого ПО направлено на получение конфиденциальной информации, что может быть связано с появлением, например, различных несигнатурных типов атак и 0-day. Активное воздействие таких кибератак инициирует создание специальных средств противодействия, способных оставаться эффективными при появлении новых видов угроз с неустановленными или нечетко определенными свойствами. Другими словами, такие средства фактически могут функционировать в слабоформализованной, нечеткой среде окружения [1]. Использование методов, моделей и систем, основанных на нечетких множествах [1]–[21], для построения средств обнаружения аномалий, порожденных реализацией киберугроз, позволит усовершенствовать существующие системы выявления вторжений в информационных системах. Исходя из этого, разработка соответствующих технических решений, функционирующих в нечетких условиях, даст возможность выявлять новые и модифицированные типы кибератак.

Известны, достаточно эффективные разработки, используемые для решения задач выявления кибератак, например, метод формирования лингвистических эталонов для систем выявления вторжений [6, 18-21]. В этом методе не раскрыт механизм процесса формирования эталонов параметров для сниффинг-атак. Исходя из этого, создание моделей, позволяющих усовершенствовать процесс получения лингвистических эталонов параметров для систем выявления вторжений, является актуальной научной задачей.

Следует отметить, что одними из опасных средств, которые направлены на перехват паролей в сети являются снифферы, представляющие собой специализированное ПО. Для эффективного функционирования снифферу достаточно быть установленным хотя бы на одном компьютере в сети. Его принцип работы заключается в том, что он получает доступ к сетевой карте и, например, переключает ее в режим PROMISC (режим прослушивания). В этом случае сетевая карта будет принимать все пакеты (вкючая те, которые ей не адресуются), находящиеся в канале связи. Если в сети осуществляется активный обмен пакетов, то за достаточно короткое время сниффер может собрать различные данные, например, логины, пароли, e-mail переписку и др. Основная опасность состоит в том, что снифферов крайне сложно обнаружить, так как они работают в пассивном режиме и, как правило, пользователи не догадываются, что в данный момент происходит сниффинг-атака. Как показывает практика, такие атаки, в основном, остаются не замеченными (см. рис. 1).

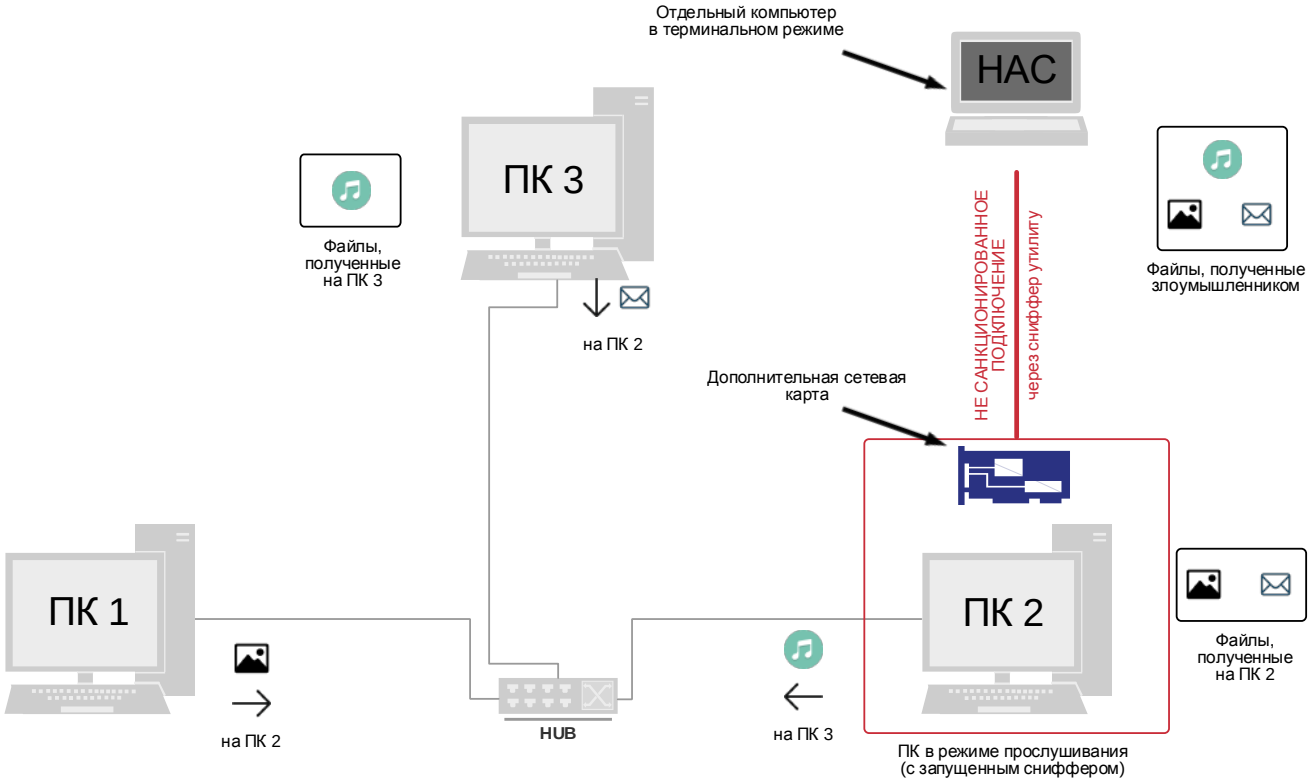

Рис. 1. Схема проведения сниффинг-атаки

Рассмотрим вид сниффинга, при котором неавторизированная сторона (НАС), проникнув в сеть, анализирует большое количество пакетов. Схема реализации такой атаки в соответствующем окружении показана на рис. 2. Здесь НАС внедряет снифер на ПК2 (осуществляется переключение его сетевой карты в режим PROMISC), вследствие чего соответствующий компьютер осуществляет мониторинг всех пакетов, которые находятся в сети. Из схемы видно, что НАС получает не только данные, которые пересылались на ПК2, но, например, email сообщение, которое было отправлено с ПК3 на ПК2. Также продемонстрировано, что пользователь ПК2 получит только данные, которые предназначались ему (изображение) (с ПК1), в то время как НАС с помощью снифера получит все данные, которые находились в сети (аудиофайл, изображение и email сообщение), что наглядно показывает его функционирование.

Поскольку прямое обнаружение сниффинг-атаки является довольно проблематичным, то для идентификации подобных вторжений необходимо исследовать возможные изменения параметров среды окружения системы, значения которых при возникновении определенных событий отличаются от штатно допустимых.

Например, для выявления описываемой атаки наиболее целесообразно использовать следующие параметры: количество входных пакетов в сети («КВП»), скорость обработки пакетов на стороне получателя («СОП») и тайминг пакетов в канале («ТП»), определяющего время ожидания для обработки очередного пакета на стороне получателя. Поскольку снифферу для анализа находящихся в сети пакетов необходимо время, то увеличение значения параметра ТП может являться признаком наличия в данной сети снифера. Для успешного проведения соответствующей атаки НАС должна внедрить снифер на один из компьютеров, подключенного к сети, данные из которой необходимы НАС.

Если при нормальном режиме работы сети значения выбранных параметров выходят за определенные границы, то это может свидетельствовать о том, что осуществляется сниффинг-атака в данном сетевом канале.

Для получения конкретных числовых параметров был проведен эксперимент на работающем Web-сервере. В качестве примера тестируемого сервера использовался компьютер со следующими характеристиками: процессор Intel(R) Core 2 Duo T5800 CPU 2,00GHz с частотой шины 800 МГц; оперативная память 6 Гб DDR2 800 МГц; сетевое подключение 100 Мбит/с; операционная система 64-битная Windows 10. Также в качестве

основы было установлено и использовано следующее ПО: VirtualBox; Nmap 7.12; WireShark; WIcd, которое на данный момент содержит обширный набор инструментов для сетевого менеджмента.

Для исследования параметров КВП, СОП и ТП в тестовой локальной сети, в которой функционирует сниффер, соответственно используются WIcd, WireShark и Nmap.

Как показывает практика, для получения необходимых данных требуется продолжительное время работы сниффера в сети. Благодаря этому становится возможным его обнаружение с помощью анализа совокупности вышеуказанных параметров. Например, параметр КВП при определенном увеличении количества пакетов в сети может быть использован как один из признаков наличия разрушающего ПО. Максимальное число пакетов, которое может пропустить канал, зависит от его физических характеристик, а также может быть ограничено программно. Максимальное значение параметра КВП ($max_{КВП}$) обычно определяется в настройках сервера.

Система, используемая для эксперимента, сконфигурирована таким образом, чтобы поддерживать одновременно не более 256 подключений, т.е. $max_{КВП}$=256. Согласно статистике, собранной с помощью утилиты *WIcd*, для данного сервера среднее количество таких подключений не превышало 100.

Для удобства оценивания параметров на основе суждений эксперта и точного их представления принято считать, что достаточно 3-7 термов на каждый параметр. Большинство применений вполне исчерпывается использованием минимального количества термов. Такое определение содержит два граничных значения (минимальное и максимальное) и среднее. Что касается максимального количества термов, то оно не ограничено и зависит от требуемой точности описания параметров. Число 7 же обусловлено емкостью кратковременной памяти человека, в которой, по современным представлениям, может храниться до семи единиц информации. Исходя из этого, целесообразней будет использовать пять термов со следующими интервалами $[0;8]$, $[9;32]$, $[33;64]$, $[65;128]$, $[129;256]$.

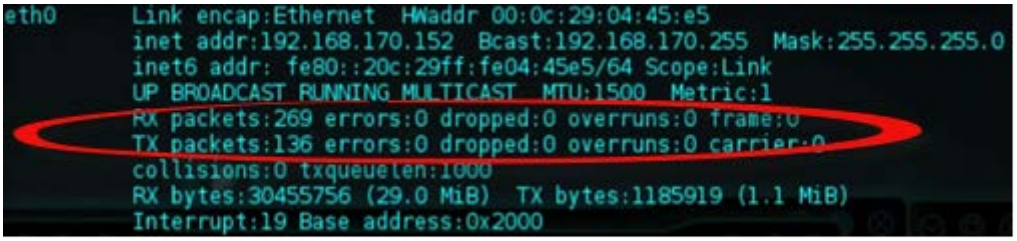

Рис. 2. Отображение параметра КВП с помощью утилиты WIcd

Параметр СОП – один из наиболее важных в механизме обнаружения сниффинг-атаки, поскольку он показывает время, необходимое для обработки входящих пакетов. Если сниффер был внедрен на компьютер, то этот параметр изменится одним из первых, так как переключив сетевую карту в режим PROMISC, сниффер увеличивает время обработки в 2 раза. В высоко нагруженном сетевом канале подобный параметр изменится через короткое время после начала работы сниффера в сети. Максимальная скорость обработки пакетов определяется на практике с помощью утилиты dsniff для конкретного пользователя в сети и задается параметром $max_{СОП}$.

Значения параметра СОП были получены по результатам теста, осуществляемого с помощью утилиты WireShark, которая является распространённым средством для анализа трафика компьютерных сетей. Измерения проводились при большом количестве пакетов, которые показали, что данный web-сервер может обработать до 3600 запросов в секунду в локальной сети и от 200 до 400 полученных из сети Internet. В нормальном режиме работы сервер за одну секунду обслуживает до 25 Internet-запросов, а максимальное количество, которое может быть обработано – 80. На основе этого, для параметра СОП возьмем следующие интервалы $[0;8]$, $[9;24]$, $[25;80]$, которые наглядно показывают диапазоны минимальных, средних допустимых и максимальных значений для данного параметра.

Из этого следует, что наиболее корректным будет определить максимальное значение для параметра СОП – 80.

При обнаружении сниффера по СОП можно использовать утилиту для мониторинга парамет-

ров сети WireShark. Она позволяет отследить скорость обработки пакетов в сети. На представленном скриншоте (см. рис. 3) виден скачек скорости до 42 секунд, что согласно указанным выше интервалам, может являться следствием работы снифера в сети.

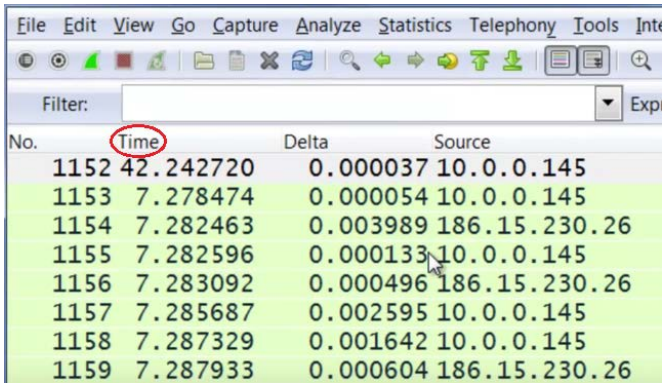

Рис. 3. Отображение значения параметра СОП при помощи утилиты WireShark

Параметр ТП характеризует время между последовательными получениями пакетов на стороне получателя от адресата. Увеличение времени между входящими пакетами может свидетельствовать о работе снифера, целью которого является анализ пакетов в сети. Значение ТП определяется величиной $max_{ТП}$, которая зависит от ПО и назначения сервера.

При нормальной нагрузке компьютерной сети значение параметра ТП не превышает 25 мс, а максимальное время задержки между пакетами – 64 мс. Из этого следует, что наиболее корректными интервалами, которые описывают параметр ТП, будут $[0;5]$, $[6;24]$, $[25;32]$, $[33;64]$.

Для обнаружения снифера по данному параметру использовалась утилита Nmap, благодаря которой эксперт, может определить время задержки между пакетами. Как видно со скриншота (см. рис. 4), задержка составила 63 секунды, что свидетельствует о работе снифера в сети.

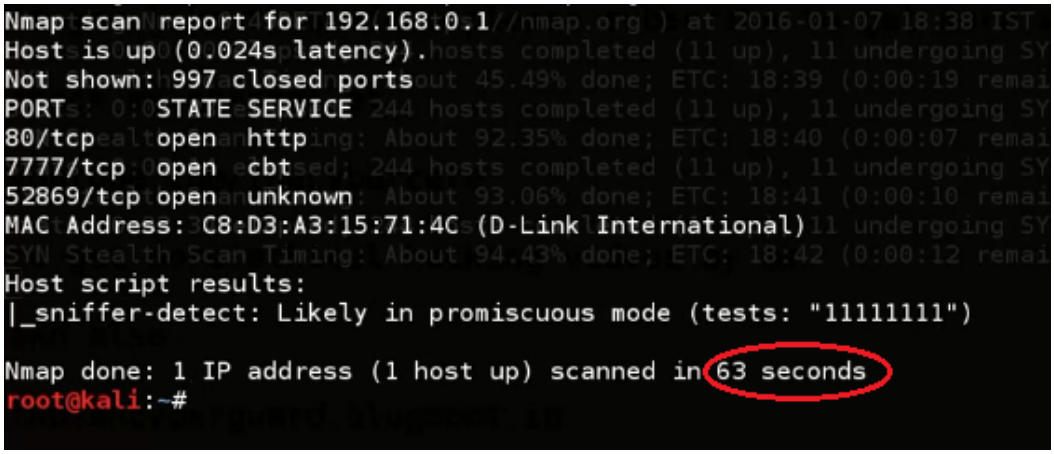

Рис. 4. Отображение значения параметра ТП при помощи утилиты Nmap

Интервалы, указанные для значений КВП, СОП, ТП основываются соответственно на: максимальном количестве пакетов, которые способен пропустить данный канал за единицу времени; максимальной скорости обработки пакетов данной системой; максимальным временем задержки пакетов в канале.

Учитывая, что для всех параметров, значения в диапазоне от средне допустимого до максимального – говорят о работе снифера в сети. Необходимо определить минимальные и максимальные значения, которые свидетельствуют о потенциальном наличии снифера.: КВП $[129;256]$, СОП $[25;80]$ и ТП $[25;64]$.

В связи с этим, целью данной работы является разработка модели эталонов лингвистических переменных для обнаружения сниффинг-атак (МЭСА), позволяющей формализовать процесс получения эталонов параметров для заданных лингвистических переменных конкретной среды окружения при решении задач выявления атак в информационных системах. Предложенная МЭСА частично основывается на МЛТС [1], а также на методе формирования лингвистических эталонов для систем выявления вторжений МФЛЭ [6, 21].

С учетом этого сформируем подмножество идентификаторов (ИД) суждений эксперта при $n=1$ для кибератаки с ИД $CA_1 = CA_{SNF} = SNF$, $m_1 = 3$, $r_1 = 5$, $r_2 = 3$, $r_3 = 4$ согласно этапа 1 выражения (7) в [6, 21]

$$\{\bigcup_{i=1}^{1}\mathbf{LE}_1\}=\{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{m_1}\mathbf{LE}_{ij}\}\}=\{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{m_1}\{\bigcup_{k=1}^{r_j}LE_{ijk}\}\}\}=$$
$$\{\{LE_{SNFKBП1},LE_{SNFKBП2},LE_{SNFKBП3},LE_{SNFKBП4},LE_{SNFKBП5}\},$$
$$\{LE_{SNFCOП1},LE_{SNFCOП2},LE_{SNFCOП3}\},\{LE_{SNFTП1},LE_{SNFTП2},LE_{SNFTП3},LE_{SNFTП4}\}\}=$$
$$\{\{"ОМ","М","С","Б","ОБ"\},\{"Н","С","В"\},\{"Н","С","В","ОВ"\}\}, \quad (1)$$

где SNF – «Sniffing-атака», а $LE_{SNFKBП1}="ОМ"$, $LE_{SNFKBП2}="М"$, $LE_{SNFKBП3}="С"$, $LE_{SNFKBП4}="Б"$, $LE_{SNFKBП5}="ОБ"$, $LE_{SNFCOП1}="Н"$, $LE_{SNFCOП2}="С"$, $LE_{SNFCOП3}="В"$ и $LE_{SNFTП1}="Н"$, $LE_{SNFTП2}="С"$, $LE_{SNFTП3}="В"$, $LE_{SNFTП4}="ОВ"$ соответственно являются ИД таких лингвистических оценок эксперта, которые отображают состояние параметров $P_{SNFKBП}=КВП$, $P_{SNFCOП}=СОП$ и $P_{SNFTП}=ТП$ в *3*-мерной параметрической подсреде [13].

Далее, согласно этапа 2, в [6, 21] следует сформировать базовую матрицу частот. Для этого построим подмножество ИД интервалов $\mathbf{N}_{ij}$ $(j=\overline{1,m_i})$ (см. выражение (12) в [6, 21]), характеризующие кибератаку с ИД $CA_{SNF}=SNF$, на области определения которой эксперт осуществляет лингвистическое оценивание относительно значений параметров $P_{SNFKBП}$, $P_{SNFCOП}$ и $P_{SNFTП}$.

При $n=1$, $m_1=3$, $r_1=5$, $r_2=3$, $r_3=4$ получим

$$\{\bigcup_{i=1}^{1}\mathbf{N}_i\}=\{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{3}\mathbf{N}_{ij}\}\}=\{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{3}\{\bigcup_{k=1}^{k_j}N_{ijk}\}\}\}=$$
$$\{\{N_{SNFKBП1},N_{SNFKBП2},N_{SNFKBП3},N_{SNFKBП4},N_{SNFKBП5}\},$$
$$\{N_{SNFCOП1},N_{SNFCOП2},N_{SNFCOП3}\},$$
$$\{N_{SNFTП1},N_{SNFTП2},N_{SNFTП3},N_{SNFTП4}\}\}. \quad (2)$$

С учетом элементов подмножеств $\mathbf{LE}_{ij}$ и $\mathbf{NE}_{ij}$ на основе обобщенной таблицы (см. табл. (1) в [6, 21]) построим текущие оценки (см. табл. 1-3) по элементам подмножеств, $LE_{SNFKBПk}(r_1=5,k=\overline{1,5})$, $N_{SNFKBПk}$, т.е. $N_{SNFKBП1}=[N^{min}_{SNFKBП1};N^{max}_{SNFKBП1}]\Leftrightarrow[0;8]$, $N_{SNFKBП2}=[N^{min}_{SNFKBП2};N^{max}_{SNFKBП2}]\Leftrightarrow[9;32]$, $N_{SNFKBП3}=[N^{min}_{SNFKBП3};N^{max}_{SNFKBП3}]\Leftrightarrow[33;64]$, $N_{SNFKBП4}=[N^{min}_{SNFKBП4};N^{max}_{SNFKBП4}]\Leftrightarrow[65;128]$, $N_{SNFKBП5}=[N^{min}_{SNFKBП5};N^{max}_{SNFKBП5}]\Leftrightarrow[129;256]$ и $LE_{SNFCOПk}(r_2=3,k=\overline{1,3}),N_{SNFCOПk}$, т.е. $N_{SNFCOП1}=[N^{min}_{SNFCOП1};N^{max}_{SNFCOП1}]\Leftrightarrow[0;8]$, $N_{SNFCOП2}=[N^{min}_{SNFCOП2};N^{max}_{SNFCOП2}]\Leftrightarrow[9;24]$, $N_{SNFCOП3}=[N^{min}_{SNFCOП3};N^{max}_{SNFCOП3}]\Leftrightarrow[25;80]$, а также $LE_{SNFTПk}(r_2=3,k=\overline{1,3})$, $N_{SNFTПk}$, т.е. $N_{SNFTП1}=[N^{min}_{SNFTП1};N^{max}_{SNFTП1}]\Leftrightarrow[0;5]$, $N_{SNFTП2}=[N^{min}_{SNFTП2};N^{max}_{SNFTП2}]\Leftrightarrow[6;24]$, $N_{SNFTП3}=[N^{min}_{SNFTП3};N^{max}_{SNFTП3}]\Leftrightarrow[25;32]$, $N_{SNFTП4}=[N^{min}_{SNFTП4};N^{max}_{SNFTП4}]\Leftrightarrow[33;64]$.

Таблица 1

Текущая таблица оценок по $\mathbf{LE}_{\mathbf{SNFKBП}}$

$\mathbf{LE}_{\mathbf{SNFKBП}}$	$\mathbf{N}_{\mathbf{SNFKBП}}$				
	$N_{SNFKBП1}$	$N_{SNFKBП2}$	$N_{SNFKBП3}$	$N_{SNFKBП4}$	$N_{SNFKBП5}$
“ОМ”	5	3	0	0	0
“М”	1	6	1	0	0
“С”	0	1	4	1	0
“Б”	0	0	2	6	4
“ОБ”	0	0	0	4	6

Таблица 2

Текущая таблица оценок по $\mathbf{LE_{SNFCOII}}$

$\mathbf{LE_{SNFCOII}}$	$\mathbf{N_{SNFCOII}}$		
	$N_{SNFCOII1}$	$N_{SNFCOII2}$	$N_{SNFCOII3}$
“Н”	4	1	0
“С”	1	2	1
“В”	0	1	3

Таблица 3

Текущая таблица оценок по $\mathbf{LE_{SNFTII}}$

$\mathbf{LE_{SNFTII}}$	$\mathbf{N_{SNFTII}}$			
	$N_{SNFTII1}$	$N_{SNFTII2}$	$N_{SNFTII3}$	$N_{SNFTII4}$
“Н”	3	1	0	0
“С”	2	3	3	0
“В”	0	2	4	3
“ОВ”	0	1	3	4

Далее, с учетом данных таблиц 1-3 и выражения (13) в [6, 21], сформируем матрицы частот при $n=1,\ m_1=\overline{1,3},\ s,q=\overline{1,r_1},\ s,q=\overline{1,r_2},\ s,q=\overline{1,r_3}$

$$F_{11}=F_{SNFKBII}=\left\|f_{11sq}\right\|=\begin{vmatrix} f_{1111} & f_{1112} & f_{1113} & f_{1114} & f_{1115} \\ f_{1121} & f_{1122} & f_{1123} & f_{1124} & f_{1125} \\ f_{1131} & f_{1132} & f_{1133} & f_{1134} & f_{1135} \\ f_{1141} & f_{1142} & f_{1143} & f_{1144} & f_{1145} \\ f_{1151} & f_{1152} & f_{1153} & f_{1154} & f_{1155} \end{vmatrix},$$

$$F_{12}=F_{SNFCOII}=\left\|f_{12sq}\right\|=\begin{vmatrix} f_{1211} & f_{1212} & f_{1213} \\ f_{1221} & f_{1222} & f_{1223} \\ f_{1231} & f_{1232} & f_{1233} \end{vmatrix} \text{ и } F_{13}=F_{SNFTII}=\left\|f_{13sq}\right\|=\begin{vmatrix} f_{1311} & f_{1312} & f_{1313} & f_{1314} \\ f_{1321} & f_{1322} & f_{1322} & f_{1322} \\ f_{1331} & f_{1332} & f_{1333} & f_{1334} \\ f_{1341} & f_{1342} & f_{1343} & f_{1344} \end{vmatrix}$$

Далее, для формирования производной матрицы частот, при $n=1,\ m_1=3$ построим по соответствующим столбцам матриц $F_{SNFKBII}$, $F_{SNFCOII}$ и F_{SNFTII} с учетом выражения (15) в [6, 21] векторы сумм

$$VS_{SNFKBII}=\left\|vs_{SNFKBIIq}\right\|=$$

$$\left\|vs_{SNFKBII1},vs_{SNFKBII2},vs_{SNFKBII3},vs_{SNFKBII4},vs_{SNFKBII5}\right\|=$$

$$\left\|\bigcup_{q=1}^{5}\sum_{s=1}^{5}f_{SNFKBIIsq}\right\|=\left\|6,10,7,11,10\right\|,\ (q=\overline{1,5}),$$

$$VS_{SNFCOII}=\left\|vs_{SNFCOIIq}\right\|=$$

$$\left\|vs_{SNFCOII1},vs_{SNFCOII2},vs_{SNFCOII3}\right\|=\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{SNFCOIIsq}\right\|$$

$$=\left\|5,4,4\right\|,\ (q=\overline{1,3}),$$

$$VS_{SNFTII}=\left\|vs_{SNFTIIq}\right\|=$$

$$\left\|vs_{SNFTII1},vs_{SNFTII2},vs_{SNFTII3},vs_{SNFTII4}\right\|=\left\|\bigcup_{q=1}^{4}\sum_{s=1}^{4}f_{SNFTIIsq}\right\|$$

$$=\left\|5,7,10,7\right\|,\ (q=\overline{1,4}).$$

Затем, с учетом (16) в [6, 21], из $VS_{SNFKBII}$, $VS_{SNFCOII}$, VS_{SNFTII} определим максимальный элемент

$$vsm_{SNFKBII}=\bigvee_{q=1}^{5}vs_{SNFKBIIq}=$$

$$vs_{SNFKBII1}\vee vs_{SNFKBII2}\vee vs_{SNFKBII3}\vee vs_{SNFKBII4}\vee vs_{SNFKBII5}=$$

$$6\vee 10\vee 7\vee 11\vee 10=vsm_{SNFKBII}=11,$$

$$vsm_{SNFCOII}=\bigvee_{q=1}^{3}vs_{SNFCOIIq}=$$

$$vs_{SNFCOII1}\vee vs_{SNFCOII2}\vee vs_{SNFCOII3}=5\vee 4\vee 4=vsm_{SNFCOII}=5,$$

$$vsm_{SNFTII}=\bigvee_{q=1}^{4}vs_{SNFTIIq}=vs_{SNFTII1}\vee vs_{SNFTII2}$$

$$\vee vs_{SNFTII3}\vee vs_{SNFTII4}=5\vee 7\vee 10\vee 7=vsm_{SNFTII}=10,$$

а согласно (17) в [6, 21] получим производную матрицу частот,

$$F'_{SNFKBП} = (vsm_{SNFKBП} / vsm_{SNFKBПq})F_{SNFKBП} = \begin{Vmatrix} 9,2 & 3,3 & 0 & 0 & 0 \\ 1,8 & 6,6 & 1,6 & 0 & 0 \\ 0 & 1,1 & 6,3 & 1 & 0 \\ 0 & 0 & 3,1 & 6 & 4,4 \\ 0 & 0 & 0 & 4 & 6,6 \end{Vmatrix},$$

$$F'_{SNFCOП} = (vsm_{SNFCOП} / vsm_{SNFCOПq})F_{SNFCOП} = \begin{Vmatrix} 4 & 1,3 & 0 \\ 1 & 2,5 & 1,3 \\ 0 & 1,3 & 3,8 \end{Vmatrix},$$

$$F'_{SNFTП} = (vsm_{SNFTП} / vsm_{SNFTПq})F_{SNFTП} = \begin{Vmatrix} 6 & 1,4 & 0 & 0 \\ 4 & 4,3 & 3 & 0 \\ 0 & 2,9 & 4 & 4,3 \\ 0 & 1,4 & 3 & 5,7 \end{Vmatrix}.$$

Далее, согласно (22) в [6, 21], сформируем подмножество нечетких термов $\mathbf{T_{SNFKBП}}$, $\mathbf{T_{SNFCOП}}$, $\mathbf{T_{SNFTП}}$ при $n=1$ (т.е. для кибератак с ИД $CA_{SNF} = SNF$), $m_1 = 3$, $r_1 = 5$, $r_2 = 3$, $r_3 = 4$

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{1}} \mathbf{T_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{T_{ij}}\}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}\}\}\} =$$

$$\{\{\underset{\sim}{T}_{SNFKBП1}, \underset{\sim}{T}_{SNFKBП2}, \underset{\sim}{T}_{SNFKBП3}, \underset{\sim}{T}_{SNFKBП4}, \underset{\sim}{T}_{SNFKBП5}\},$$

$$\{\underset{\sim}{T}_{SNFCOП1}, \underset{\sim}{T}_{SNFCOП2}, \underset{\sim}{T}_{SNFCOП3}\},$$

$$\{\underset{\sim}{T}_{SNFTП1}, \underset{\sim}{T}_{SNFTП2}, \underset{\sim}{T}_{SNFTП3}\}\} =$$

$$\{\{\underset{\sim}{OM}_{SNFKBП}, \underset{\sim}{M}_{SNFKBП}, \underset{\sim}{C}_{SNFKBП},$$

$$\underset{\sim}{Б}_{SNFKBП}, \underset{\sim}{OБ}_{SNFKBП}\},$$

$$\{\underset{\sim}{H}_{SNFCOП}, \underset{\sim}{C}_{SNFCOП}, \underset{\sim}{B}_{SNFCOП}\},$$

$$\{\underset{\sim}{H}_{SNFTП}, \underset{\sim}{C}_{SNFTП}, \underset{\sim}{B}_{SNFTП}, \underset{\sim}{OB}_{SNFTП}\}\}.$$

Согласно (23) в [6, 21], по соответствующим строкам $F'_{SNFKBП}$, $F'_{SNFCOП}$, $F'_{SNFTП}$ построим векторы максимумов т.е.

$$FM_{SNFKBП} = \| fm_{SNFKBПs} \| =$$

$$\| fm_{SNFKBП1}, fm_{SNFKBП2}, fm_{SNFKBП3}, fm_{SNFKBП4}, fm_{SNFKBП5} \| =$$

$$\|9,2;6,6;6,3;6;6,6\|,$$

$$FM_{SNFCOП} = \| fm_{SNFCOПs} \| =$$

$$\| fm_{SNFCOП1}, fm_{SNFCOП2}, fm_{SNFCOП3} \| = \|4;2,5;3,8\|,$$

$$FM_{SNFTП} = \| fm_{SNFTПs} \| =$$

$$\| fm_{SNFTП1}, fm_{SNFTП2}, fm_{SNFTП3}, fm_{SNFTП4} \| = \|6;4,3;4;5,7\|.$$

На основании $FM_{SNFKBП}$, $FM_{SNFCOП}$ и $FM_{SNFTП}$ по выражению (24) в [6, 21] сформируем матрицы функций принадлежности:

$$M_{SNFKBП} = \|\mu_{SNFKBПsq}\| = \begin{Vmatrix} 1 & 0,5 & 0 & 0 & 0 \\ 0,2 & 1 & 0,3 & 0 & 0 \\ 0 & 0,2 & 1 & 0,2 & 0 \\ 0 & 0 & 0,5 & 1 & 0,7 \\ 0 & 0 & 0 & 0,7 & 1 \end{Vmatrix},$$

$$M_{SNFCOП} = \|\mu_{SNFCOПsq}\| = \begin{Vmatrix} 1 & 0,5 & 0 \\ 0,3 & 1 & 0,3 \\ 0 & 0,5 & 1 \end{Vmatrix}, \; M_{SNFTП} = \|\mu_{SNFTПsq}\| = \begin{Vmatrix} 1 & 0,3 & 0 & 0 \\ 0,7 & 1 & 0,8 & 0 \\ 0 & 0,7 & 1 & 0,8 \\ 0 & 0,3 & 0,8 & 1 \end{Vmatrix},$$

где $\mu_{SNFKBПsq} = f'_{SNFKBПsq} / fm_{SNFKBПs}$, $(s,q = \overline{1,5})$, $\mu_{SNFCOПsq} = f'_{SNFCOПsq} / fm_{SNFCOПs}$, $(s,q = \overline{1,3})$, $\mu_{SNFTПsq} = f'_{SNFTПsq} / fm_{SNFTПs}$, $(s,q = \overline{1,4})$.

На основе полученных данных, $\mu_{SNFKBПsq}$, $\mu_{SNFCOПsq}$, $\mu_{SNFTПsq}$ и вычисленных по выражению (26) в [6, 21] $x_{SNFKBПsq}$, $x_{SNFCOПsq}$, $x_{SNFTПsq}$ определим наборы нечетких термов согласно (25) в [6, 21]

$\underset{\sim}{T}_{SNFKBПs} = \{ \mu_{SNFKBПs1} / x_{SNFKBПs1}, \mu_{SNFKBПs2} / x_{SNFKBПs2}, \mu_{SNFKBПs3} / x_{SNFKBПs3}, \mu_{SNFKBПs4} / x_{SNFKBПs4}, \mu_{SNFKBПs5} / x_{SNFKBПs5} \}$, $(s,q = \overline{1,5})$, где, согласно (26) в [6, 21], $X_{SNFKBПsq} = N^{max}_{SNFKBПq} / N^{max}_{SNFKBПr}$, $(q = \overline{1,5})$ или $\{\bigcup_{q=1}^{5} X_{SNFKBПsq}\} = \{0,03;0,13;0,25;0,5;1\}$. $\underset{\sim}{T}_{SNFCOПs} = \{ \mu_{SNFCOПs1} / x_{SNFCOПs1}, \mu_{SNFCOПs2} / x_{SNFCOПs2}, \mu_{SNFCOПs3} / x_{SNFCOПs3} \}$, $(s,q = \overline{1,3})$, где $X_{SNFCOПsq} = N^{max}_{SNFCOПq} / N^{max}_{SNFCOПr}$, $(q = \overline{1,3})$ или $\{\bigcup_{q=1}^{3} X_{SNFCOПsq}\} = \{0,1;0,3;1\}$.

$\underset{\sim}{T}_{SNFTПs} = \{ \mu_{SNFTПs1} / x_{SNFTПs1}, \mu_{SNFTПs2} / x_{SNFTПs2}, \mu_{SNFTПs3} / x_{SNFTПs3}, \mu_{SNFTПs4} / x_{SNFTПs4} \}$, $(s,q = \overline{1,4})$, где $X_{SNFTПsq} = N^{max}_{SNFTПq} / N^{max}_{SNFTПr}$, $(q = \overline{1,4})$ или $\{\bigcup_{q=1}^{4} X_{SNFTПsq}\} = \{0,08;0,4;0,5;1\}$.

Таким образом, полученные члены подмножества $\mathbf{T}_{\mathbf{SNFKBП}}$, $\mathbf{T}_{\mathbf{SNFCOП}}$, $\mathbf{T}_{\mathbf{SNFTП}}$ (числовая форма), соответственно являются отображением членов подмножества $\mathbf{LE}_{\mathbf{SNFKBП}}$, $\mathbf{LE}_{\mathbf{SNFCOП}}$, $\mathbf{LE}_{\mathbf{SNFTП}}$ (лингвистическая форма) и представляются в следующем виде:

$\underset{\sim}{T}_{SNFKBП1} = \underset{\sim}{OM} = \{1 / 0,03; 0,5 / 0,13; 0 / 0,25; 0 / 0,5; 0 / 1\}$;
$\underset{\sim}{T}_{SNFKBП2} = \underset{\sim}{M} = \{0,2 / 0,03; 1 / 0,13; 0,3 / 0,25; 0 / 0,5; 0 / 1\}$;
$\underset{\sim}{T}_{SNFKBП3} = \underset{\sim}{C} = \{0 / 0,03; 0,2 / 0,13; 1 / 0,25; 0,2 / 0,5; 0 / 1\}$;
$\underset{\sim}{T}_{SNFKBП4} = \underset{\sim}{Б} = \{0 / 0,03; 0 / 0,13; 0,5 / 0,25; 1 / 0,5; 0,7 / 1\}$;
$\underset{\sim}{T}_{SNFKBП5} = \underset{\sim}{OБ} = \{0 / 0,03; 0 / 0,13; 0 / 0,25; 0,7 / 0,5; 1 / 1\}$,

$\underset{\sim}{T}_{SNFCOП1} = \underset{\sim}{H} = \{1 / 0,1; 0,5 / 0,3; 0 / 1\}$;
$\underset{\sim}{T}_{SNFCOП2} = \underset{\sim}{C} = \{0,3 / 0,1; 1 / 0,3; 0,3 / 1\}$;
$\underset{\sim}{T}_{SNFCOП3} = \underset{\sim}{B} = \{0 / 0,1; 0,5 / 0,3; 1 / 1\}$,

$\underset{\sim}{T}_{SNFTП1} = \underset{\sim}{H} = \{1 / 0,08; 0,3 / 0,4; 0 / 0,5; 0 / 1\}$
$\underset{\sim}{T}_{SNFTП2} = \underset{\sim}{C} = \{0,7 / 0,08; 1 / 0,4; 0,8 / 0,5; 0 / 1\}$
$\underset{\sim}{T}_{SNFTП3} = \underset{\sim}{B} = \{0 / 0,08; 0,7 / 0,4; 1 / 0,5; 0,8 / 1\}$
$\underset{\sim}{T}_{SNFTП4} = \underset{\sim}{OB} = \{0 / 0,08; 0,3 / 0,4; 0,8 / 0,5; 1 / 1\}$.

Далее, согласно (29) в [6, 21], сформируем эталонные НЧ $\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFKBП}} \subseteq \mathbf{T}^{\mathbf{e}}$, $\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFCOП}} \subseteq \mathbf{T}^{\mathbf{e}}$, $\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFTП}} \subseteq \mathbf{T}^{\mathbf{e}}$:

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFKBП}} = \{\bigcup_{s=1}^{5} \underset{\sim}{T}^{e}_{SNFKBПs}\} = \{\underset{\sim}{T}^{e}_{SNFKBП1}, \underset{\sim}{T}^{e}_{SNFKBП2}, \underset{\sim}{T}^{e}_{SNFKBП3}, \underset{\sim}{T}^{e}_{SNFKBП4}, \underset{\sim}{T}^{e}_{SNFKBП5}\} = \{\underset{\sim}{OM}^{e}_{SNFKBП1}, \underset{\sim}{M}^{e}_{SNFKBП2}, \underset{\sim}{C}^{e}_{SNFKBП3}, \underset{\sim}{Б}^{e}_{SNFKBП4}, \underset{\sim}{OБ}^{e}_{SNFKBП5}\}, \quad (s = \overline{1,5}),$$

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFCOП}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^{e}_{SNFCOПs}\} = \{\underset{\sim}{T}^{e}_{SNFCOП1}, \underset{\sim}{T}^{e}_{SNFCOП2}, \underset{\sim}{T}^{e}_{SNFCOП3}\} = \{\underset{\sim}{H}^{e}_{SNFCOП1}, \underset{\sim}{C}^{e}_{SNFCOП2}, \underset{\sim}{B}^{e}_{SNFCOП3}\}, \quad (s = \overline{1,3}),$$

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFTП}} = \{\bigcup_{s=1}^{4} \underset{\sim}{T}^{e}_{SNFTПs}\} = \{\underset{\sim}{T}^{e}_{SNFTП1}, \underset{\sim}{T}^{e}_{SNFTП2}, \underset{\sim}{T}^{e}_{SNFTП3}, \underset{\sim}{T}^{e}_{SNFTП4}\} = \{\underset{\sim}{H}^{e}_{SNFTП1}, \underset{\sim}{C}^{e}_{SNFTП2}, \underset{\sim}{B}^{e}_{SNFTП3}, \underset{\sim}{OB}^{e}_{SNFTП4}\}, \quad (s = \overline{1,4}),$$

где члены подмножества $\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFKBП}}$ – $\underset{\sim}{OM}^{e}_{SNFKBП1}$, $\underset{\sim}{M}^{e}_{SNFKBП2}, \underset{\sim}{C}^{e}_{SNFKBП3}, \underset{\sim}{Б}^{e}_{SNFKBП4}, \underset{\sim}{OБ}^{e}_{SNFKBП5}$; $\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFCOП}}$ – $\underset{\sim}{H}^{e}_{SNFCOП1}$, $\underset{\sim}{C}^{e}_{SNFCOП2}$, $\underset{\sim}{B}^{e}_{SNFCOП3}$; $\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFTП}}$ – $\underset{\sim}{H}^{e}_{SNFTП1}$, $\underset{\sim}{C}^{e}_{SNFTП2}, \underset{\sim}{B}^{e}_{SNFTП3}, \underset{\sim}{OB}^{e}_{SNFTП4}$ являются эталонными НЧ.

Далее преобразуем нечеткие термы $\underset{\sim}{OM}_{SNFKBП}$, $\underset{\sim}{M}_{SNFKBП}$, $\underset{\sim}{C}_{SNFKBП}$, $\underset{\sim}{Б}_{SNFKBП}$ и $\underset{\sim}{OБ}_{SNFKBП}$ таким образом, что бы для всех $\underset{\sim}{T}_{SNFKBПs}$ было справедливо

отношения порядка, т.е. $\forall x_{SNFKBПsq}$: $x_{SNFKBПsq} < x_{SNFKBПsq+1}$, $(q = \overline{1,4})$ (согласно шага 1, этапа 5 в [6, 21]). Если в качестве компонентов таких термов использовать конкретные значения, полученные в примере выше, то для них такое отношение будет истинным. Так, например, для $\underset{\sim}{OM}_{SNFKBП}$ это $x_{SNFKBП11} < x_{SNFKBП12} < x_{SNFKBП13} < x_{SNFKBП14} < x_{SNFKBП15} = 0,03 < 0,13 < 0,25 < 0,5 < 1$.

Также аналогично будет истинным отношения для $\underset{\sim}{H}_{SNFCOП}$ – это $x_{SNFCOП11} < x_{SNFCOП12} < x_{SNFCOП13} = 0,1 < 0,3 < 1,$ и для $\underset{\sim}{H}_{SNFTП}$ – это $x_{SNFTП11} < x_{SNFTП12} < x_{SNFTП13} < x_{SNFTП14} = 0,08 < 0,4 < 0,5 < 1$.

Далее, согласно шага 2 этапа 5 в [6, 21], для каждого $\underset{\sim}{T}_{SNFKBПs}$ осуществим процедуру поглощения.

Для $\underset{\sim}{OM}_{SNFKBП1}$ (где мода $x_{SNFKBП1M} = x_{SNFKBП11} = 0,03$, а ее порядковый номер $M = 1$) при условии U_2 (т.е. $\mu_{SNFKBП13} = \mu_{SNFKBП14} = \mu_{SNFKBП15} = 0$) осуществляется поглощение одним компонентом $0 / x^{max}_{SNFKBП1}$ ряда других согласно выражения $x^{max}_{SNFKBП1} = x_{SNFKBП13} \wedge x_{SNFKBП14} \wedge x_{SNFKBП15} = 0,25 \wedge 0,5 \wedge 1 = 0,25$ $(q = \overline{1,5})$. Таким образом, $\mu_{SNFKBП13} / x_{SNFKBП13} = 0 / 0,25$, $\mu_{SNFKBП14} / x_{SNFKBП14} = 0 / 0,5$, $\mu_{SNFKBП15} / x_{SNFKBП15} = 0 / 1$ поглощаются компонентом $\mu_{SNFKBП13} / x_{SNFKBП13} = 0 / 0,25$.

Аналогично для $\underset{\sim}{M}_{SNFKBП1}$ (где мода $x_{SNFKBП2M} = x_{SNFKBП21} = 0,13$, а ее порядковый номер $M = 2$) при условии U_2 (т.е. $\mu_{SNFKBП24} = \mu_{SNFKBП25} = 0$) осуществляется поглощение одним компонентом $0 / x^{max}_{SNFKBП2} = \mu_{SNFKBП24} / x_{SNFKBП24} = 0 / 0,5$ согласно выражения $x^{max}_{SNFKBП2} = x_{SNFKBП24} \wedge x_{SNFKBП25} = 0,5 \wedge 1 = 0,5$. Таким образом, $\mu_{SNFKBП24} / x_{SNFKBП24} = 0 / 0,5$ и $\mu_{SNFKBП25} / x_{SNFKBП25} = 0 / 1$ поглощаются компонентом $\mu_{SNFKBП24} / x_{SNFKBП24} = 0 / 0,5$.

Далее видно, что для НЧ $\underset{\sim}{C}_{SNFKBП1}$ условие U_1 и U_2 не выполняется и поэтому операция поглощения не осуществляется.

Для $\underset{\sim}{Б}_{SNFKBП1}$ (где мода $x_{SNFKBП4M} = x_{SNFKBП41} = 0,5$, а ее порядковый номер $M = 4$) при условии U_1 (т.е. $\mu_{SNFKBП41} = \mu_{SNFKBП42} = 0$) компонент $0 / x^{min}_{SNFKBП4} = \mu_{SNFKBП42} / x_{SNFKBП42} = 0 / 0,13$ согласно выражения $x^{min}_{SNFKBП4} = x_{SNFKBП41} \vee x_{SNFKBП42} = 0,03 \vee 0,13 = 0,13$ получим значение $\mu_{SNFKBП41} / x_{SNFKBП42} = 0 / 0,03$ и $\mu_{SNFKBП42} / x_{SNFKBП42} = 0 / 0,13$, поглощаемые компонентом $\mu_{SNFKBП41} / x_{SNFKBП42} = 0 / 0,03$.

Аналогично для $\underset{\sim}{ОБ}_{SNFKBП1}$ ($x_{SNFKBП5M} = x_{SNFKBП55} = 1$, а ее порядковый номер $M = 5$) при условии U_1 (т.е. $\mu_{SNFKBП51} = \mu_{SNFKBП52} = \mu_{SNFKBП53} = 0$) осуществляется поглощение одним компонентом $0 / x^{min}_{SNFKBП5}$ ряда других согласно выражения $x^{min}_{SNFKBП5} = x_{SNFKBП51} \vee x_{SNFKBП52} \vee x_{SNFKBП53} = 0,03 \vee 0,13 \vee 0,25 = 0,25$. Таким образом, $\mu_{SNFKBП51} / x_{SNFKBП51} = 0 / 0,03$, $\mu_{SNFKBП52} / x_{SNFKBП52} = 0 / 0,13$, $\mu_{SNFKBП53} / x_{SNFKBП53} = 0 / 0,25$ поглощаются компонентом $\mu_{SNFKBП53} / x_{SNFKBП53} = 0 / 0,25$.

Далее для каждого $\underset{\sim}{T}_{SNFCOПs}$ ($\underset{\sim}{H}$, $\underset{\sim}{C}$, $\underset{\sim}{Б}$) условия U_1 и U_2 не выполняются и поэтому операция поглощения не осуществляется, а для $\underset{\sim}{T}_{SNFTПs}$ ($\underset{\sim}{H}$, $\underset{\sim}{C}$, $\underset{\sim}{Б}$, $\underset{\sim}{ОБ}$) выполняется только условие U_1. С учетом описанных преобразований, а также выражения (28) в [6, 21], определим промежуточные термы в виде:

$$\underset{\sim}{T}'_{SNFKBП1} = \underset{\sim}{OM}'_{SNFKBП1} = \{1 / 0,03; 0,5 / 0,13; 0 / 0,25\};$$

$$\underset{\sim}{T}'_{SNFKBП2} = \underset{\sim}{M}'_{SNFKBП2} = \{0,2 / 0,03; 1 / 0,13; 0,3 / 0,25; 0 / 0,5\};$$

$$\underset{\sim}{T}'_{SNFKBП3} = \underset{\sim}{C}'_{SNFKBП3} = \{0 / 0,03; 0,2 / 0,13; 1 / 0,25; 0,2 / 0,5; 0 / 1\};$$

$$\underset{\sim}{T}'_{SNFKBП4} = \underset{\sim}{Б}'_{SNFKBП4} = \{0/0,13; 0,5/0,25; 1/0,5; 0,7/1\};$$

$$\underset{\sim}{T}'_{SNFKBП5} = \underset{\sim}{ОБ}'_{SNFKBП5} = \{0/0,25; 0,7/0,5; 1/1\},$$

$$\underset{\sim}{T}'_{SNFCOП1} = \underset{\sim}{Н}'_{SNFCOП1} = \{1/0,1; 0,5/0,3; 0/1\};$$

$$\underset{\sim}{T}'_{SNFCOП2} = \underset{\sim}{С}'_{SNFCOП2} = \{0,3/0,1; 1/0,3; 0,3/1\};$$

$$\underset{\sim}{T}'_{SNFCOП3} = \underset{\sim}{В}'_{SNFCOП3} = \{0/0,1; 0,5/0,3; 1/1\},$$

$$\underset{\sim}{T}'_{SNFTП1} = \underset{\sim}{Н}'_{SNFTП1} = \{1/0,08; 0,3/0,4; 0/0,5\};$$

$$\underset{\sim}{T}'_{SNFTП2} = \underset{\sim}{С}'_{SNFTП2} = \{0,7/0,08; 1/0,4; 0,8/0,5; 0/1\};$$

$$\underset{\sim}{T}'_{SNFTП3} = \underset{\sim}{В}'_{SNFTП3} = \{0/0,08; 0,7/0,4; 1/0,5; 0,8/1\};$$

$$\underset{\sim}{T}'_{SNFTП4} = \underset{\sim}{ОВ}'_{SNFTП4} = \{0/0,08; 0,3/0,4; 0,8/0,5; 1/1\}.$$

Согласно шага 3 этапа 5 в [6], при реализации второго шага в выражении (28) для набора промежуточных термов $\underset{\sim}{ОМ}'_{SNFKBП}$ и $\underset{\sim}{М}'_{SNFKBП}$ $\exists \underset{\sim}{T}'_{SNFKBП1} : \{0/x^{min}_{SNFKBП1}\} \in \varnothing$ и $\exists \underset{\sim}{T}'_{SNFKBП2} : \{0/x^{min}_{SNFKBП2}\} \in \varnothing$ (т.е. $\mu_{SNFKBП11} = 1 \neq 0$ и $\mu_{SNFKBП21} = 0,2 \neq 0$), а для $\underset{\sim}{Б}'_{SNFKBП}$ и $\underset{\sim}{ОБ}'_{SNFKBП}$ $\exists \underset{\sim}{T}'_{SNFKBП4} : \{0/x^{max}_{SNFKBП4}\} \in \varnothing$ и $\exists \underset{\sim}{T}'_{SNFKBП5} : \{0/x^{max}_{SNFKBП5}\} \in \varnothing$ (т.е. $\mu_{SNFKBП45} = 0,67 \neq 0$ и $\mu_{SNFKBП55} = 1 \neq 0$), то формирование подмножеств $\underset{\sim}{T}^{e}_{SNFKBП1}$, $\underset{\sim}{T}^{e}_{SNFKBП2}$ и $\underset{\sim}{T}^{e}_{SNFKBП4}$, $\underset{\sim}{T}^{e}_{SNFKBП5}$ осуществим за счет расширения $\underset{\sim}{T}'_{SNFKBП1}$, $\underset{\sim}{T}'_{SNFKBП2}$ и $\underset{\sim}{T}'_{SNFKBП4}$, $\underset{\sim}{T}'_{SNFKBП5}$ (см.(28) в [6]) посредством введения дополнительных $\mu_{SNFKBП1\beta-1} / x_{SNFKBП1\beta-1} = 0/0,3$, $\mu_{SNFKBП2\beta-1} / x_{SNFKBП2\beta-1} = 0/0,3$ и $\mu_{SNFKBП4r_j-\gamma+2} / x_{SNFKBП4r_j-\gamma+2} = 0/1$, $\mu_{SNFKBП5r_j-\gamma+2} / x_{SNFKBП5r_j-\gamma+2} = 0/1$ соответственно, после чего в НЧ осуществляется переиндексация компонент начиная с первой.

С учетом этого, набор промежуточных термов для $\underset{\sim}{ОМ}'_{SNFKBП}$ будет иметь следующий вид $\underset{\sim}{T}'_{SNFKBП1} = \underset{\sim}{ОМ}'_{SNFKBП1} = \{\mu_{SNFKBП11} / x_{SNFKBП11}, \mu_{SNFKBП12} / x_{SNFKBП12}, \mu_{SNFKBП13} / x_{SNFKBП13}, \mu_{SNFKBП14} / x_{SNFKBП14}\} = \{0/0,03; 1/0,03; 0,5/0,13; 0/0,25\}$, где $\mu_{SNFKBП1\beta-1} = 0$. Аналогичным способом получаем промежуточные термы для $\underset{\sim}{М}'_{SNFKBП}$, $\underset{\sim}{Б}'_{SNFKBП}$ и $\underset{\sim}{ОБ}'_{SNFKBП}$, где $\mu_{SNFKBП2\beta-1} = \mu_{SNFKBП4r_j-\gamma+2} = \mu_{SNFKBП5r_j-\gamma+2} = 0$. Таким образом, компоненты подмножества эталонов $\underset{\sim}{T}^{e}_{SNFKBП1}$ согласно (29) в [6] будут определяться как

$$\mu^{e}_{SNFKBП11} / x^{e}_{SNFKBП11} = 0/0,03,$$

$$\mu^{e}_{SNFKBП12} / x^{e}_{SNFKBП12} = 1/0,03,$$

$$\mu^{e}_{SNFKBП13} / x^{e}_{SNFKBП13} = 0,5/0,13,$$

$$\mu^{e}_{SNFKBП14} / x^{e}_{SNFKBП14} = 0/0,25$$

и аналогичным образом для $\underset{\sim}{T}^{e}_{SNFKBП2}$, $\underset{\sim}{T}^{e}_{SNFKBП4}$, $\underset{\sim}{T}^{e}_{SNFKBП5}$.

Далее, согласно (29) в [6], для $\underset{\sim}{ОМ}'_{SNFKBП1}$, $\underset{\sim}{М}'_{SNFKBП1}$, $\underset{\sim}{Б}'_{SNFKBП1}$, $\underset{\sim}{ОБ}'_{SNFKBП1}$ сформируем эталонные значения, т.е.:

$$\underset{\sim}{T}^{e}_{SNFKBП1} = \underset{\sim}{ОМ}^{e}_{SNFKBП1} = \{0/0,03; 1/0,03; 0,5/0,13; 0/0,25\};$$

$$\underset{\sim}{T}^{e}_{SNFKBП2} = \underset{\sim}{М}^{e}_{SNFKBП2} = \{0/0,03; 0,2/0,03; 1/0,13; 0,3/0,25; 0/0,5\};$$

$$\underset{\sim}{T}^{e}_{SNFKBП3} = \underset{\sim}{С}^{e}_{SNFKBП3} = \{0/0,03; 0,2/0,13; 1/0,25; 0,2/0,5; 0/1\};$$

$$\underset{\sim}{T}^{e}_{SNFKBП4} = \underset{\sim}{Б}^{e}_{SNFKBП4} = \{0/0,13; 0,5/0,25; 1/0,5; 0,7/1; 0/1\};$$

$$\underset{\sim}{T}^{e}_{SNFKBП5} = \underset{\sim}{ОБ}^{e}_{SNFKBП5} = \{0/0,25; 0,7/0,5; 1/1; 0/1\}.$$

Также по аналогии формируются и следующие эталонные значения:

$$\underset{\sim}{T}^{e}_{SNFCOП1} = \underset{\sim}{H}^{e}_{SNFCOП1} = \{0/0,1; 1/0,1; 0,5/0,3; 0/1\};$$

$$\underset{\sim}{T}^{e}_{SNFCOП2} = \underset{\sim}{C}^{e}_{SNFCOП2} = \{0/0,1; 0,3/0,1; 1/0,3; 0,3/1; 0/1\};$$

$$\underset{\sim}{T}^{e}_{SNFCOП3} = \underset{\sim}{B}^{e}_{SNFCOП3} = \{0/0,1; 0,5/0,3; 1/1; 0/1\} \text{ и}$$

$$\underset{\sim}{T}^{e}_{SNFTП1} = \underset{\sim}{H}^{e}_{SNFTП1} = \{0/0,08; 1/0,08; 0,3/0,4; 0/0,5\};$$

$$\underset{\sim}{T}^{e}_{SNFTП2} = \underset{\sim}{C}^{e}_{SNFTП2} = \{0/0,08; 0,7/0,08; 1/0,4; 0,8/0,5; 0/1\};$$

$$\underset{\sim}{T}^{e}_{SNFTП3} = \underset{\sim}{B}^{e}_{SNFTП3} = \{0/0,08; 0,7/0,4; 1/0,5; 0,8/1\};$$

$$\underset{\sim}{T}^{e}_{SNFTП4} = \underset{\sim}{OB}^{e}_{SNFTП4} = \{0/0,08; 0,3/0,4; 0,8/0,5; 1/1\}.$$

Для подмножества эталонов $\mathbf{T}^{e}_{SNFKBП}$, $\mathbf{T}^{e}_{SNFCOП}$ и $\mathbf{T}^{e}_{SNFTП}$ с учетом полученных конкретных значений можно реализовать их графическую интерпретацию (см. рис. 5-7), воспользовавшись соответствующими эталонами НЧ.

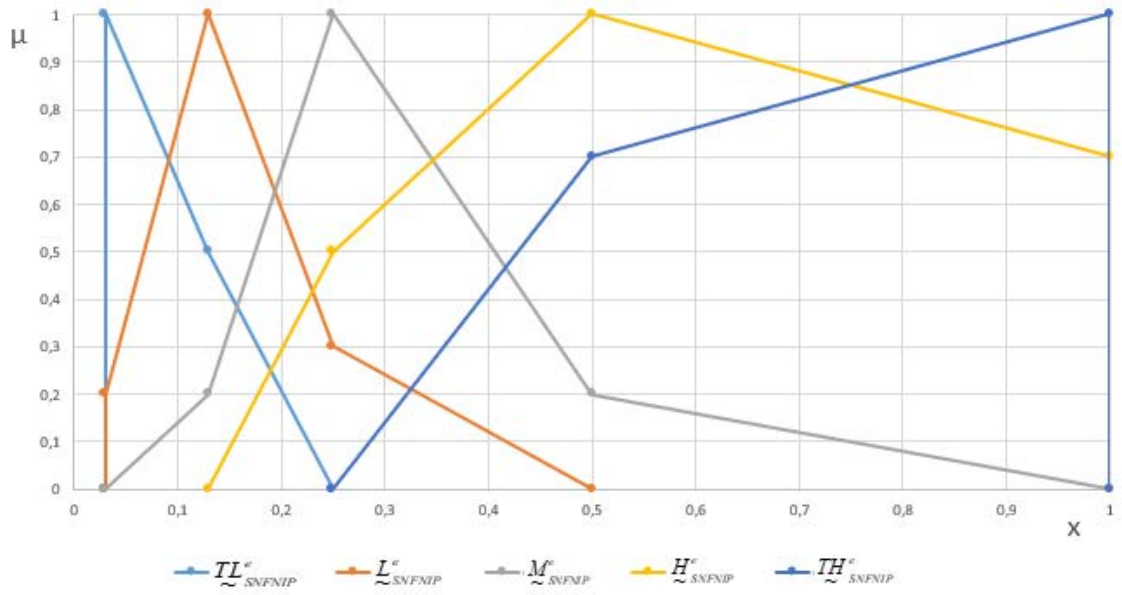

Рис. 5. Лингвистические эталоны для $\mathbf{T}^{e}_{SNFKBП}$

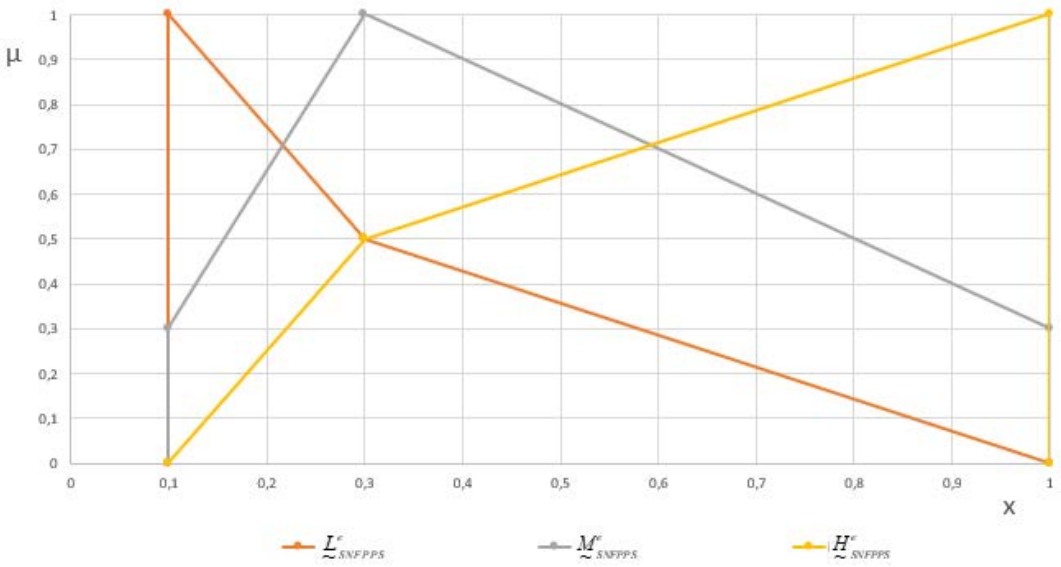

Рис. 6. Лингвистические эталоны для $\mathbf{T}^{e}_{SNFCOП}$

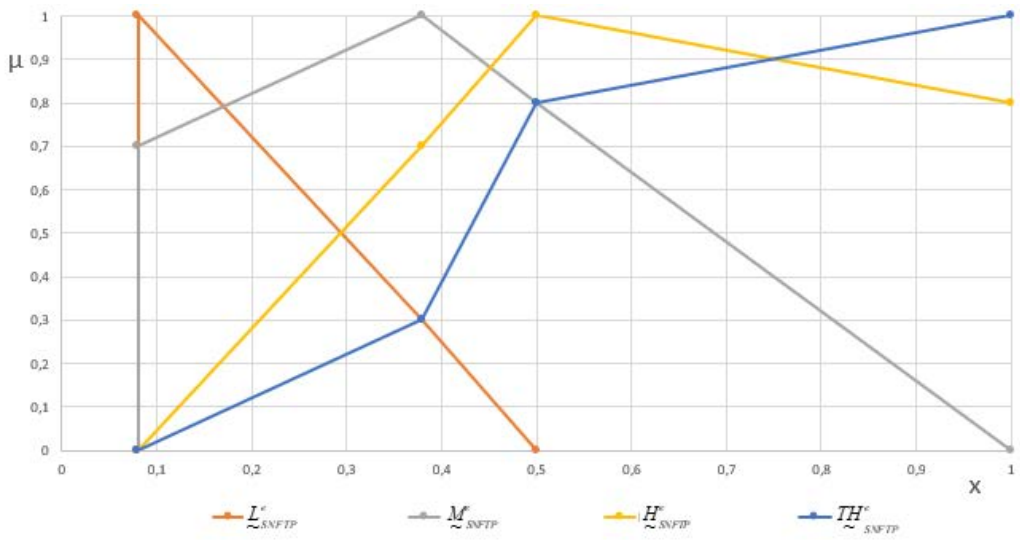

Рис. 7. Лингвистические эталоны для $\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFTII}}$

На основе определенных параметров КВП, СОП, ТП и сформированных их эталонных значений, а также с учетом [13-16, 20] можно построить подмножество базовых детекционных правил, используемых для обнаружения Sniffing-атаки. Например, одно из правил можно интерпретировать как: «Если текущее значение нечеткого параметра СОП в момент времени τ_f наиболее близко к эталонному нечеткому числу «Среднее» или текущее значение нечеткого параметра ТП в момент времени τ_f наиболее близко к эталонному нечеткому числу «Среднее», при этом, текущее значение нечеткого параметра КВП в момент времени τ_f наиболее близко к эталонному нечеткому числу «Большое», то уровень аномального состояния, который может быть порожден сниффингом, будет «Больше высокий чем низкий».

Предложенные в работе модели, которые, за счет экспертной оценки состояния информационной системы и реализованного процесса формирования эталонов параметров КВП, СОП и ТП, позволяют формализовать процедуру получения эталонных значений определенных величин, что даст возможность построить решающие правила для идентификации сниффинг-атак.

Такие модели могут быть использованы для повышения эффективности средств информационной безопасности, направленных на противодействие сниффинг-атаками в информационных системах.

ЛИТЕРАТУРА

[1]. А. Корченко *Построение систем защиты информации на нечетких множествах. Теория и практические решения.* К. : МК-Пресс, 2006, 320 с.

[2]. А. Корченко, "Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах*", Захист інформації*, № 4 (57), С. 112-118, 2012.

[3]. А. Стасюк, А. Корченко, "Базовая модель параметров для построения систем выявления атак", *Захист інформації*, № 2 (55), С. 47-51, 2012.

[4]. М. Луцкий, А. Корченко, А. Гавриленко, А. Охрименко, "Модели эталонов лингвистических переменных для систем выявления атак", *Захист інформації*, № 2 (55), С. 71-78, 2012.

[5]. А. Стасюк, А. Корченко, "Метод выявления аномалий порожденных кибератаками в компьютерных сетях", *Захист інформації,* №4 (57), С. 129-134, 2012.

[6]. А. Корченко, "Метод формирования лингвистических эталонов для систем выявления вторжений", *Захист інформації*, Т. 16, №1, С. 5-12, 2014.

[7]. А. Корченко, "Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак", *Безпека інформації*, № 1 (20), С. 21-28, 2014.

[8]. А. Корченко, "Метод α-уровневой номинализации нечетких чисел для систем обнаружения вторжений", *Захист інформації*, Т. 16, №4, С. 292-304, 2014.

[9]. А. Корченко, "Метод определения идентифицирующих термов для систем обнаружения вторжений", *Безпека інформації*, Т. 20, №3, С. 217-223, 2014.

[10]. А. Корченко, "Система выявления аномального состояния в компьютерных сетях", *Безпека інформації,* № 2 (18), С. 80-84, 2012.

[11]. А. Корченко, "Система формирования нечетких эталонов сетевых параметров", *Захист інформації,* Т. 15, №3, С. 240-246, 2013.

[12]. А. Корченко, "Система формирования эвристических правил для оценивания сетевой активности", *Захист інформації,* Т. 15, №4, С. 353-359, 2013.

[13]. А. Корченко, "Кортежная модель формирования набора базовых компонент для выявления кибератак", *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, №.2 (28), С. 29-36, 2014.

[14]. A. Korchenko, K. Warwas, A. Kłos-Witkowska, "The Tupel Model of Basic Components' Set Formation for Cyberattacks", *Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015),* Vol. 1., pp. 478-483, 2015.

[15]. Н. Карпинский, А. Корченко, С. Ахметова, "Метод формирования базовых детекционных правил для систем обнаружения вторжений", *Захист інформації,* Т. 17, №4, С. 312-324, 2015.

[16]. A. Korchenko, K. Warwas, A. Kłos-Witkowska, "The Tupel Model of Basic Components' Set Formation for Cyberattacks", *Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015),* Vol. 1., pp. 478-483, 2015.

[17]. А. Корченко, В. Щербина, Н. Вишневская, "Методология построения систем выявления аномалий порожденных кибератаками", *Захист інформації*, Т. 18, №1, С. 30-38, 2016.

[18]. B. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, "Improved method for the formation of linguistic standards for of intrusion detection systems", *Journal of Theoretical and Applied Information Technology*, Vol. 87, №.2, pp. 221-232, 2016.

[19]. А. Корченко, Н. Жуманғалиева, П. Викулов, "Построение лингвистических эталонов для выявления сниффинг атак", *Актуальні питання забезпечення кібербезпеки та захисту інформації : ІІІ міжнар. наук.-практ. конф. : Тези доп*., С. 93-97.

[20]. M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan, "The Etalon Models of Linguistic Variables for Sniffing-Attack Detection", *Proceedings of the 2017 IEEE 9th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2017)*, Vol. 1, pp. 258-264.

[21]. B. Akhmetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, "Improved method for the formation of linguistic standards for of intrusion detection systems", *Journal of Theoretical and Applied Information Technology*, vol. 87, no. 2, pp. 221-232, 2016.

REFERENCES

[1]. A. Korchenko, "The development of information protection systems based on the fuzzy sets", *The theory and practical solutions*, Kiev, 2006, 320 p.

[2]. A. Korchenko, "The model of heuristic rules on the set of logical-linguistic tangles for abnormality detection in computer systems", *Zahist ìnformacìï*, no. 4(57), pp. 112-118, 2012.

[3]. A. Stasiuk, A. Korchenko, "The basic model of parameters in attack detection (Identification) systems construction", *Zahist ìnformacìï*, no. 2(55), pp. 47-51, 2012.

[4]. M. Lutskiy, A. Korchenko, A. Gavrylenko, A. Okhrimenko, "The models of linguistic variables for attack detection systems", *Zahist ìnformacìï*, no. 2 (55), pp. 71-78, 2012.

[5]. A. Stasiuk, A. Korchenko, "A method of abnormality detection caused by cyber attacks in computer networks", *Zahist ìnformacìï*, no. 4 (57), pp. 129-134, 2012.

[6]. A. Korchenko, "The formation method of linguistic standards created for the intrusion detection systems", *Zahist ìnformacìï*, vol. 16, no. 1, pp. 5-12, 2014.

[7]. A. Korchenko, "The method of parameter fuzzification based on linguistic standards for cyber attacks detection", *Bezpeka ìnformacìï*, vol. 20, no. 1, pp. 21-28, 2014.

[8]. A. Korchenko, "The method of α-level of nominalization for intrusion detection systems", *Zahist ìnformacìï*, vol. 16, no. 4, pp. 292-304, 2014.

[9]. A. Korchenko, "The detection method of identification terms for intrusion detection system", *Bezpeka ìnformacìï*, vol. 20, no. 3, pp. 217-223, 2014.

[10]. A. Korchenko, "Anomaly-based detection system in computer networks", *Bezpeka ìnformacìï*, no. 2 (18), pp. 80-84, 2012.

[11]. A. Korchenko, "The system development of fuzzy standards of network parameters", *Zahist ìnformacìï*, vol. 15, no. 3, pp. 240-246, 2013.

[12]. A. Korchenko, "The system of heuristic rules formation for network activity assessment", *Zahist ìnformacìï*, vol. 15, no. 4, pp. 353-359, 2013.

[13]. A. Korchenko, "The tupel model of basic components' set formation for cyberattacks*", Legal, regulatory and metrological support information security system in Ukraine*, no. 2 (28), pp. 29-36, 2014.

[14]. A. Korchenko, K. Warwas, A. Kłos-Witkowska, "The Tupel Model of Basic Components' Set Formation for Cyberattacks", *Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015),* Vol. 1., pp. 478-483, 2015.

[15]. M. Karpinski, A. Korchenko, S. Akhmetova, "The method of developmentof basic detection rules for intrusion detection systems", *Zahist ìnformacìï*, vol. 17, no. 4, pp. 312-324, 2015.

[16]. A. Korchenko, K. Warwas, A. Kłos-Witkowska, "The Tupel Model of Basic Components' Set Formation for Cyberattacks", *Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015),* Vol. 1., pp. 478-483, 2015.

[17]. A. Korchenko, V. Shcherbina, N. Vishnevskaya, "Methodology of constructing systems for detecting anomalies generated by cyber attacks", *Information security*, vol.18, no. 1, pp. 30-38, 2016.

[18]. B. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, "Improved method for the for-

mation of linguistic standards for of intrusion detection systems", *Journal of Theoretical and Applied Information Technology*, Vol. 87, №.2, pp. 221-232, 2016.

[19]. A. Korchenko, N. Zhumangaliyeva, P. Vikulov, "Constructing linguistic standards for sniffing attacks identification ", *Topical issues of cybersecurity and information security : III International Scientific and Practical Conference : Theses,* pp. 93-97.

[20]. M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan, "The Etalon Models of Linguistic Variables for Sniffing-Attack Detection", *Proceedings of the 2017 IEEE 9th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2017)*, Vol. 1, pp. 258-264.

[21]. B. Akhmetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, "Improved method for the formation of linguistic standards for of intrusion detection systems", *Journal of Theoretical and Applied Information Technology*, vol. 87, no. 2, pp. 221-232, 2016.

МОДЕЛІ ЕТАЛОНІВ ЛІНГВІСТИЧНИХ ЗМІННИХ ДЛЯ ВИЯВЛЕННЯ СНІФФІНГ-АТАК

Інтенсивний розвиток інформаційних систем призвів до збільшення руйнівного програмного забезпечення, множина якого направлена на отримання конфіденційної інформації, що безпосередньо пов'язано з появою атак типу 0-day і несигнатурних типів кібератак. Збільшення впливу кібератак, спрямованих на різні ресурси інформаційних систем, ініціює створення спеціальних засобів протидії, які здатні залишатися ефективними при появі нових видів загроз з невстановленими або нечітко визначеними властивостями. Відомі досить ефективні розробки, які використовуються для вирішення завдань виявлення кібератак, наприклад, метод формування лінгвістичних еталонів для систем виявлення вторгнень, в якому не розкритий механізм процесу формування еталонів параметрів для сніффінг-атак. З цією метою розроблена модель еталонів лінгвістичних змінних для виявлення сніффінг-атак, яка, за рахунок оцінки стану інформаційної системи і процесу формування еталонів параметрів: кількість вхідних пакетів в мережі, швидкість обробки пакетів на стороні одержувача, таймінг пакетів в каналі, дозволить формалізувати процес отримання еталонів параметрів для заданих лінгвістичних змінних конкретного середовища оточення при вирішенні задач виявлення атак в комп'ютерних системах. Такі моделі, можуть бути використані для підвищення ефективності засобів інформаційної безпеки, спрямовані на протидію сніффінг-атак в комп'ютерних мережах.

Ключові слова: атаки, кібератаки, аномалії, методи формування лінгвістичних еталонів, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, виявлення аномалій в комп'ютерних мережах.

THE ETALONS MODELS OF LINGUISTIC VARIABLES FOR SNIFFING ATTACKS DETECTION

The intensive development of information systems has led to an increase in destructive software, many of which are aimed at obtaining confidential information, which is directly related to the emergence of attacks like 0-day and non-signature types of cyber attacks. Expanding the impact of cyber attacks directed at various resources of information systems initiates the creation of special countermeasures that can remain effective when new types of threats emerge with undefined or indistinctly defined properties. There are known, quite effective developments used to solve problems of detecting cyber attacks, for example, the method of forming linguistic etalons for intrusion detection systems, in which the mechanism of the process of forming parameter etalons for attack sniffing is not disclosed. For this purpose, a model of linguistic variables has been developed to detect sniffing attacks, which is due to the evaluation of the state of the information system and the process of forming parameter standards: the number of incoming packets in the network, the speed of processing packets on the receiver side, the timing of packets in the channel, will allow to formalize the process of obtaining parameter etalons for given linguistic variables of a particular environment in solving problems of detecting attacks in computer systems. Such models can be used to improve the effectiveness of information security tools aimed at countering sniffing attacks in computer networks.

Keywords: attacks, cyber attacks, anomalies, methods of forming linguistic etalons, intrusion detection systems, anomaly detection systems, attacks detection systems, detection of anomalies in computer networks

Терейковский Игорь Анатольевич, доктор технических наук, доцент кафедры безопасности инфор-мационных технологий Национального авиацион-ного университета.
E-mail: terejkowski@ukr.net

Терейковський Ігор Анатолійович, доктор технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Tereykovsky Igor, Doctor of Science in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University.

Корченко Анна Александровна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: annakor@ukr.net

Корченко Анна Олександрівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Korchenko Anna, PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Викулов Павел Александрович, аспирант кафедры безопасности информационных технологий Национального авиационного университета.
Email: p.vikulov@ukr.net
Вікулов Павло Олександрович, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.
Vikulov Pavlo, PhD student of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Шаховал Александра Анатольевна, старший лаборант кафедры безопасности информационных технологий Национального авиационного университета.
Email: shakhoval.al@gmail.com
Шаховал Олександра Анатоліївна, старший лаборант кафедри безпеки кафедри безпеки інформаційних технологій Національного авіаційного університету.
Shakhoval Oleksandra, senior laboratory assistant of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

DOI: 10.18372/2410-7840.19.11903
УДК 003.26:004.056.55

КРИПТОГРАФІЧНИЙ МЕТОД ЗАХИСТУ КРИТИЧНИХ АВІАЦІЙНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Сергій Гнатюк, Василь Кінзерявий, Берік Ахметов, Каріна Кириченко, Кирило Ануфрієнко

Забезпечення конфіденційності даних є важливим етапом у процесі забезпечення кібербезпеки критичних авіаційних інформаційних систем та авіаційної галузі у цілому. Відомі методи не дозволяють у повній мірі забезпечити стійкість до кібератак лінійного та диференціального криптоаналізу і необхідну швидкість криптографічної обробки даних. З огляду на це, у роботі розроблено криптографічний метод захисту критичних авіаційних інформаційних систем. На основі даного методу побудовано блоковий симетричний шифр Lmna-2k17 та у роботі наведена специфікація даного шифру. Також, розраховано значення верхніх оцінок параметрів, що характеризують його практичну стійкість до кібератак лінійного та диференціального криптоаналізу. За однакових умов, проведені експериментальні дослідження з оцінки швидкісних характеристик шифрів, які показали, що шифр Lmna-2k17 швидший за шифр ГОСТ 28147-89 приблизно у 3,11 рази, а за шифри Калина та AES у 1,271 рази.
Ключові слова: *криптографія, блоковий шифр, лінійний криптоаналіз, диференціальний криптоаналіз, захист інформації.*

Вступ. Цивільна авіація є галуззю критичної інфраструктури держави, внутрішнє середовище якої швидко і суттєво змінюється із впровадженням сучасних інформаційно-комунікаційних технологій. Відповідно до керівних документів у галузі цивільної авіації найбільшого захисту потребують критичні авіаційні інформаційні системи (КАІС) [1], до яких згідно [2] відносяться, наприклад, системи управління повітряним рухом, системи дистанційного технічного обслуговування, диспетчерські системи та ін. Для мінімізації впливу кіберзагроз на ресурси КАІС необхідно вжити низку заходів [3], серед яких забезпечення конфіденційності даних (інформації). Одним із найважливіших напрямів діяльності щодо забезпечення конфіденційності даних був і залишається захист інформації криптографічними методами [4], беззаперечною перевагою яких є забезпечення захисту безпосередньо самих даних, а не доступу до них. Основним критерієм при виборі криптосистем є стійкість, проте для деяких завдань ключову роль відіграє швидкість криптографічної обробки даних [4-5]. Незважаючи на різноманітність сучасних криптографічних методів та систем, далеко не всі володіють необхідним рівнем ефективності (швидкодії та стійкості) для забезпечення захисту даних, а розвиток і здешевлення інформаційно-комунікаційних технологій позитивно впливає на ефективність криптоаналізу, одними з найефективніших методів якого є лінійний та диференціальний криптоаналіз [6-8].

Постановка завдання. Таким чином, розробка криптографічного методу захисту КАІС та обґрунтування його ефективності є *актуальним* науковим завдання. Зважаючи на це, *метою роботи* є підвищення ефективності криптографічного захисту КАІС на базі розробки нового