

АНАЛИЗ ПРОЦЕССОВ ДЕГРАДАЦИИ СИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ, ОСНОВАННЫХ НА МАНДАТНЫХ МОДЕЛЯХ С ВОЗМОЖНОСТЬЮ «ЗАПИСИ ВНИЗ»

Гайдамакин Н. А.¹

DOI: 10.21681/2311-3456-2025-6-2-13

Цель статьи: провести теоретический анализ функционирования мандатных систем управления доступом, в которых с целью расширения функциональных возможностей по обработке информации субъектам доступа разрешается осуществление «записей вниз».

Метод исследования: применение аппарата пуассоновских потоков событий для формализации и анализа функционирования мандатных систем управления доступом с возможностью «записей вниз».

Результаты исследования: процесс функционирования мандатной системы управления доступом с возможностью «записей вниз» рассматривается как пуассоновский поток однородных событий возникновения и реализации высоковероятными субъектами доступа (пользователями с высоким уровнем доступа) потребностей записей информации в низкоуровневые объекты доступа (файлы, документы с низким уровнем конфиденциальности). В результате каждого такого события после завершения «записи вниз», чтобы не допустить в дальнейшем возможного ознакомления низкоуровневых пользователей с высоковероятной информацией, уровень конфиденциальности объекта доступа повышается до уровня доступа соответствующего (записывающего) субъекта. Вводится понятие деградации системы управления доступом, которое заключается в том, что при двух уровнях доступа и конфиденциальности (высокий и низкий) со временем все объекты доступа по уровню конфиденциальности становятся высоковероятными, и соответственно недоступными по «чтению» для субъектов (пользователей) с низким уровнем доступа.

Анализируется вероятность наступления деградации системы управления доступом в случае стационарности и нестационарности пуассоновского потока событий «записей вниз». При убывающей со временем интенсивности событий «записей вниз» рассматривается необычный на первый взгляд характер изменения со временем вероятности деградации, который можно назвать эффектом «последнемаксимумного затухания», заключающийся сначала в увеличении со временем вероятности деградации с достижением в определенный момент времени некоторого максимального значения, а затем в постепенном уменьшении вероятности деградации до нулевого значения. При линейном и экспоненциальном характере убывания интенсивности потока событий «записей вниз» получены соотношения для момента времени с максимальной вероятностью деградации, который определяется величиной скорости уменьшения интенсивности потока событий.

Научная новизна: введено и рассмотрено понятие «деградации» мандатных систем управления доступом с возможностью «записей вниз». Процесс функционирования мандатных систем управления доступом с возможностью «записей вниз» в контексте анализа деградации рассмотрен как пуассоновский поток однородных событий. Проанализирован т.н. «эффект «последнемаксимумного затухания» вероятности деградации при убывающей со временем интенсивности потока событий «записей вниз».

Ключевые слова: мандатный принцип управления доступом, «запись вниз», поток событий «записей вниз», деградация системы управления доступом, эффект «последнемаксимумного затухания».

Введение

Политика мандатного управления доступом к конфиденциальной информации, регламентированная для применения в компьютерных системах государственных организаций, основывается на исходной формальной модели Д. Белла и Л. Лападулы [1]. Принцип управления доступом в модели Белла Лападулы выражается двумя правилами – «запрет чтения вверх» и «запрет записи вниз», что обеспечивает математически доказуемую невозможность ознакомления пользователем с низким уровнем доступа

(низким уровнем допуска-доверия) с информацией высокого уровня конфиденциальности.

Вместе с тем, «запрет записи вниз» существенно снижает функциональные возможности по обработке информации в компьютерных системах, означая принципиальную невозможность записи (корректировки, редактирования) пользователем с высоким уровнем доступа (например, руководителем организации) в объекты (документы) с низким уровнем конфиденциальности.

¹ Гайдамакин Николай Александрович, доктор технических наук, профессор, профессор кафедры алгебры и фундаментальной информатики Уральского федерального университета имени первого Президента России Б. Н. Ельцина. г. Екатеринбург, Россия. E-mail: n.a.gaidamakin@urfu.ru

Для преодоления данного ограничения был предложен подход [2], иногда не совсем правильно именуемый моделью «Low-Water-Mark»², заключающийся во введении в модель Белла Лападулы дополнительной команды *reset*, которая «поднимает» уровень конфиденциальности объекта доступа до максимального и тем самым становится возможной запись в него любым пользователем, в т.ч. с самым высоким уровнем доступа.

Вместе с тем, нетрудно увидеть, что в практической реализации данный подход может приводить к переходу со временем всех низкоуровневых объектов доступа в высокоуровневые и в результате становится невозможным доступ к ним по чтению для низкоуровневых пользователей, что, в свою очередь, приводит также к существенному ограничению функциональности систем обработки информации. Подобные особенности функционирования мандатных систем управления доступом с возможностью «записей вниз» можно именовать тенденцией к деградации.

С учетом отмеченного выше широкого применения мандатных систем управления доступом и стремления в создании не только безопасных, но и полнофункциональных современных компьютерных систем, представляется актуальной задача теоретического анализа отмеченной тенденции деградации при возможности «записи вниз».

Исходные положения

Как и в классической модели Белла Лападулы будем основываться на субъектно-объектной теоретико-множественной формализации, в рамках которой в контексте анализа безопасности информации компьютерная система представляется совокупностью сущностей двух видов – субъектов доступа $s \in S$ и объектов доступа $o \in O$, множество которых $S \cup O$ отражено на линейно упорядоченное множество уровней безопасности L . В каждый момент времени любой экземпляр $x \in (S \cup O)$ сущностей компьютерной системы (субъект или объект доступа) характеризуется параметром $f_L(x)$, который является элементом множества L , т.е. характеризует определенный уровень безопасности $l \in L$ соответствующего элемента множества $S \cup O$. Уровень безопасности субъектов является аналогом степени (уровня) допуска сотрудников (пользователей), уровень безопасности объектов является аналогом уровня (грифа) конфиденциальности документов.

2 Следует отметить, что в большинстве работ по формальным моделям безопасности (см., например, [3, 4, 5]) под термином «Low-Water-Mark» понимается принцип присвоения наиболее критичным в аспекте нарушения целостности сущностям (объектам и субъектам доступа) наиболее низких уровней в решетке безопасности, трактуемой как решетка уровней конфиденциальности [6]. Данный принцип, как и в целом известная мандатная модель целостности К. Бибы [6], является инверсией принципа «High-Water-Mark», при котором наиболее критичным в аспекте конфиденциальности сущностям присваиваются наиболее высокие уровни в решетке безопасности [3, 7].

Критерием безопасности доступов субъектов к объектам является запрет потоков информации «сверху-вниз», т.е. от сущностей с высоким уровнем безопасности к сущностям с более низким уровнем безопасности. Потоки «сверху-вниз» прямо (при чтении высокоуровневого объекта низкоуровневым субъектом) или транзитивно (при записи высокоуровневым субъектом низкоуровневый объект с последующим его чтением низкоуровневым субъектом) приводят к нарушению одного из 3-х составляющих безопасности информации компьютерных систем – нарушению конфиденциальности.

Соответственно доступ на чтение безопасен тогда и только тогда, когда уровень безопасности субъекта равен или превышает уровень безопасности объекта $f_L(s) \geq f_L(o)$ – т.н. правило NRU (no read up, нельзя читать вверх). Отметим, что в случае $f_L(s) \geq f_L(o)$ реализуется или безопасный «горизонтальный» поток (между равноуровневыми сущностями) или безопасный поток «снизу-вверх», т.е. из низкоуровневого объекта к высокоуровневому субъекту.

Доступ по записи безопасен тогда и только тогда, когда уровень безопасности субъекта равен или меньше уровня безопасности объекта $f_L(s) \geq f_L(o)$ – т.н. правило NWD (no write down, нельзя писать вниз). В этом случае также реализуется безопасный «горизонтальный» поток или безопасный поток «снизу-вверх» от низкоуровневого субъекта в высокоуровневый объект.

В практической реализации модели Белла –Лападулы в операционных системах и СУБД применяется линейная решетка конечного набора уровней безопасности (обычно 3-4 уровня). При этом любая пара «субъект-объект» доступа сравнивается по параметру $f_L(x)$. В этом случае множество L можно рассматривать как некую порядковую шкалу безопасности сущностей компьютерной системы.

Вместе с тем использование линейной решетки с небольшим числом уровней безопасности приводит к существенному огрублению доступа, в т.ч. к избыточности прав доступа. Иначе говоря, по правилам NRU и NWD субъекту с определенным уровнем безопасности доступны по чтению и записи любые объекты с таким же уровнем безопасности, и, кроме того, только по чтению все субъекты с более низким, а по записи – все объекты с более высоким уровнем безопасности. Это вынуждает вносить в мандатную модель механизмы дискреционного разграничения доступа посредством дополнительного введения матрицы доступа $A[s,o]$. Строки матрицы доступа $A[s,o]$ соответствуют субъектам доступа (пользователям), столбцы объектам доступа, а в ячейках фиксируются разрешения доступа соответствующих субъектов к соответствующим объектам. В результате в рамках

мандатных полномочий пользователей для чтения $f_L(s) \geq f_L(o)$ и для записи $f_L(s) \geq f_L(o)$ (необходимое условие) доступ субъекта к объекту возможен только при наличии непосредственного разрешения в соответствующей ячейке матрицы доступа (достаточное условие).

Состояние компьютерной системы $V\{L(S), L(O), A[s, o]\}$ определяется совокупностью текущих значений уровней безопасности субъектов $f_L(s) \in L(S)$ и объектов доступа $f_L(o) \in L(O)$, значений ячеек матрицы доступа $A[s, o]$, а также совокупностью доступов, осуществляемых субъектами к объектам. Изменения значений $f_L(s)$, $f_L(o)$ и $A[s, o]$ трактуется как переход системы в новое состояние V^* , что, в свою очередь, обеспечивает новую совокупность доступов субъектов к объектам.

Д. Э. Белл и Л. Лападула доказали т.н. «основную теорему безопасности» (Basic Security Theorem), суть которой заключается в том, что, если изменения значений $f_L(s)$ и $f_L(o)$ приводят в новом состоянии к новым мандатным полномочиям определенных субъектов к определенным объектам, то адекватно должны изменяться соответствующие ячейки матрицы доступа $A[s, o]$, и наоборот. В теореме доказывается, что при таких условиях в любом произвольном состоянии системы V гарантированно отсутствуют доступы, нарушающие правила NRU и NWD, т.е. система функционирует безопасно в смысле критерия недопущения потоков «сверху-вниз», приводящих к нарушению конфиденциальности информации объектов доступа.

Трудно переоценить методологическую роль, которую сыграла модель Белла Лападулы в теории и практике защищенных компьютерных систем. Была математически доказана теоретическая безопасность компьютерных систем, в которых доступ осуществляется по мандатным правилам, и, что, может быть не менее важно в практическом плане, на основе модели обеспечивалась возможность воспроизведения в компьютерных системах, установленных для «бумажных» технологий нормативных «допусковых» (т.е. «мандатных») регламентаций работы с конфиденциальной информацией.

Вместе с тем, как часто бывает в отношении новых подходов и методов, а также из-за определенной абстрактности и схоластичности модели Белла Лападулы, были представлены многочисленные работы по ее критическому анализу [8, 9].

Прежде всего, следует отметить, что полный запрет всех информационных потоков «сверху-вниз» оправдан далеко не всегда, поскольку основывается на неявном предположении, что любой информационный элемент (слово, запись, символ, абзац, страница) документа, т.е. объекта доступа, является

конфиденциальным соответствующего уровня. Очевидно, что во многих случаях часть информации документа является конфиденциальной, а другая нет или конфиденциальной меньшего уровня. Ввиду этого на практике, сотруднику, не допущенному к документам определенного уровня конфиденциальности, может доводиться из таких документов только та часть информации, те выдержки, которые по уровню конфиденциальности соответствуют уровню допуска сотрудника.

Аналогично не вся информация, записываемая в какой-либо объект субъектом доступа, является конфиденциальной уровня безопасности субъекта. Сотрудник может вносить (записывать) данные в рабочую тетрадь или в [разрабатываемый] документ, уровень конфиденциальности которых ниже его уровня допуска, при условии того, что вносимые данные будут иметь соответствующий грифу документа уровень конфиденциальности.

Другим недостатком модели Белла Лападулы, который исследовался еще в работах Дж. МакЛина [8, 9], является отсутствие механизмов и процедур установления и изменения уровней безопасности субъектов и объектов доступа. Дж. МакЛином были введены понятия авторизованной функции перехода и уполномоченных субъектов (для изменения уровней безопасности субъектов или объектов доступа), что существенно снизило схоластичность исходной модели Белла Лападулы и обеспечило условия ее практической реализации в компьютерных системах.

Анализируя вслед за Дж. МакЛином процессы изменения уровней безопасности объектов доступа в мандатных системах, следует отметить еще один существенный недостаток базовой модели Белла-Лападулы, который заключается в отсутствии временного аспекта в понятии «доступ субъекта к объекту» [10]. Иначе говоря, процессы доступа субъектов к объектам рассматриваются как одномоментные («мгновенные») явления, переводящие систему в новое состояние. Таким образом, доступы «не делятся», и соответственно в промежутках между «мгновенно» (точнее вне временного аспекта) осуществленными доступами «ничего не происходит».

В результате системы управления доступом на основе модели Белла-Лападулы представляют собой системы с дискретным временем [10].

Будем считать, что в компьютерной системе существует дискретное время, в каждый момент которого t_i состояние системы V_i характеризуется определенной декомпозицией на множество субъектов S , помеченных соответствующими метками (уровнями) безопасности и осуществляющими доступы на множестве объектов O . В результате доступов формируются информационные потоки и, в т.ч. могут изменяться

уровни безопасности объектов, что переводит в момент времени t_{i+1} систему в новое состояние $V_{t_{i+1}}$. Соответственно уровни безопасности субъектов и объектов доступа в различные моменты времени будем индцировать верхними временными индексами – $f_L^{(t_i)}(s), f_L^{(t_i)}(o)$.

Как отмечалось выше, в рамках мандатного управления доступом в некоторых случаях субъекту s необходимо внести информацию (осуществить запись, т.е. доступ по записи) в объект o , уровень безопасности которого ниже его уровня безопасности – $f_L^{(t_i)}(s) > f_L^{(t_i)}(o)$. В этом случае в целях обеспечения критерия безопасности (недопущение потоков «сверху-вниз») субъект s сначала подает команду $reset(o)$, в результате которой уровень безопасности объекта o поднимается до максимального, и, соответственно, по правилам NRU и NWD становится для субъекта s доступным по записи. По завершению записи, т.е. в новом состоянии $V_{t_{i+1}}$, если уровень безопасности субъекта s не является максимальным, уровень безопасности объекта снижается до уровня записывающего субъекта $f_L^{(t_{i+1})}(o) = f_L^{(t_{i+1})}(s)$.

Для упрощения анализа будем считать систему статичной по декомпозиции на субъекты доступа. Иначе говоря, количество M субъектов доступа (s_1, s_2, \dots, s_M) и их декомпозиция на группы по уровням безопасности не изменяются во времени. Будем также считать систему статичной по количеству объектов доступа – $N^{(t_i)} = N_L^{(t_i)}$, но их декомпозиция на группы по уровням безопасности (грифам конфиденциальности), напротив, может изменяться при осуществлении высокоранговыми субъектами «записей вниз», по завершению которых низкоранговые объекты становятся высокоранговыми. Таким образом исходное количество низкоранговых объектов в мандатной системе управления доступом с возможностью «записей вниз» с течением времени сокращается.

Также для простоты будем предполагать, что в системе управления доступом два уровня безопасности – низкий l_1 и высокий l_2 ($l_1 < l_2$). Соответственно $N_{l_1}^{(t_0)}$ объектов доступа в начальный момент времени t_0 помечены нижним уровнем безопасности l_1 , а $N_{l_2}^{(t_0)}$ верхним уровнем безопасности l_2 , при этом $N_{l_1}^{(t_0)} + N_{l_2}^{(t_0)} = N$.

Определим понятие состояния деградации системы управления доступом как переход в состояние $V_{Degrade}$, при котором $N_{l_2}^{(Degrad)} = N, N_{l_1}^{(Degrad)} = 0$.

Также будем полагать, что уровни безопасности субъектов доступа при переходах системы из одного состояния в другое не меняются $f_L^{(t_i)}(s) = f_L^{(t_{i+1})}(s), i = 0, 1, 2, \dots$.

Кроме того, будем полагать, что субъект s с уровнем безопасности l_2 при осуществлении доступа

по записи может вносить в объект доступа о информацию как уровня l_2 , так и уровня l_1 .

Деградация мандатной системы управления доступом как результат простейшего потока однородных событий «записей вниз»

Переход объектов с уровня безопасности l_1 на уровень l_2 происходит в том случае, когда у субъектов с уровнем безопасности l_2 в какой-либо момент времени t_i возникает необходимость записи информации уровня l_1 в объект уровня безопасности $f_L^{(t_i)}(o) = l_1$ («запись вниз»).

Возникновение и осуществление такой потребности «записи вниз» будем трактовать как некое событие. Очевидно, такие события могут происходить в любой момент времени $t_0, t_1, t_2, \dots, t_i$, и в результате мы имеем поток однородных событий, результатом каждого из которых является уменьшение на единицу количества объектов уровня l_1 , что, собственно, и составляет тенденцию к деградации системы.

Если данный поток событий детерминированный, и соответствующее событие с вероятностью, равной 1, возникает в каждый следующий момент времени t_0, t_1, t_2, \dots , то деградация системы наступит в момент времени $t_i = t_{N_{l_1}^{(t_0)}}$, т.е. $i = N_{l_1}^{(t_0)}$.

Если поток событий случайный, то он может быть простейшим потоком [однородных] событий, который характеризуется свойствами ординарности, стационарности и отсутствия последействия.

В нашем случае ординарность будет означать, что в любой момент времени $t_0, t_1, t_2, \dots, t_i$ потребность записи информации уровня l_1 возникает и реализуется только у какого-либо одного субъекта s уровня l_2 в отношении какого-либо одного объекта o уровня l_1 . Возникновение и осуществление аналогичной потребности «записи вниз» у другого пользователя уровня l_2 или в отношении другого объекта уровня l_1 трактуется как следующий (другой) момент дискретного времени функционирования системы управления доступом.

Стационарность и отсутствие последействия будет означать, что вероятность наступления соответствующей потребности не зависит от момента времени t_i и от количества состоявшихся к этому времени k таких событий.

Важно отметить, что свойство отсутствия последействия также обусловлено указанным выше отсутствием временного аспекта доступов в исходной модели мандатного доступа Белла-Лападулы. Иначе говоря, в системе управления доступом обработка событий «записей вниз» происходит «мгновенно» (точнее вне временного аспекта) и поэтому не влияет на поступление (возникновение) и обработку последующих событий.

Простейший пуассоновский поток однородных событий характеризуется постоянной интенсивностью λ возникновения соответствующих событий, определяемой как среднее число событий в единицу времени, т.е. на интервале от t_{i-1} до t_i .

Очевидно, что при гипотезе об ординарности соответствующего потока событий в отмеченном выше смысле $0 < \lambda \leq 1$.

При пуассоновском потоке вероятность появления за i шагов точно k событий определяется известным выражением [11] :

$$P_{t_i}(k) = e^{-\lambda i} \frac{(\lambda i)^k}{k!}. \quad (1)$$

Для анализа процесса деградации удобнее рассмотреть вероятность того, что за i шагов, т.е. на промежутке времени от t_0 до t_i , произойдет не менее $N_{l_1}^{(t_0)}$ соответствующих событий, т.е. ($k \geq N_{l_1}^{(t_0)}$). Противоположное событие ($k < N_{l_1}^{(t_0)}$) является суммой событий, каждое из которых заключается в том, что на промежутке от t_0 до t_i произойдет только точно 0 событий, или только точно 1 событие, или только точно 2 события, или ... только точно $N_{l_1}^{(t_0)} - 1$ событие. Тогда для простейшего пуассоновского потока событий вероятность события $P_{t_i}(k \geq N_{l_1}^{(t_0)})$ определяется следующим соотношением:

$$P_{t_i}(k \geq N_{l_1}^{(t_0)}) = 1 - e^{-\lambda i} \sum_{m=0}^{N_{l_1}^{(t_0)}-1} \frac{(\lambda i)^m}{m!}. \quad (2)$$

На рис. 1. представлены графики вероятностей $P_{t_i}(k \geq N_{l_1}^{(t_0)})$, отражающие процесс деградации мандатной системы управления доступом при гипотезе о простейшем пуассоновском потоке событий «записей вниз» для $N_{l_1}^{(t_0)} = 10$, $N_{l_1}^{(t_0)} = 20$, $\lambda = 1$, $\lambda = 0,5$, $\lambda = 0,1$, соответственно.

Как видно из приведенных на рисунке графиков, процесс деградации при гипотезе о простейшем пуассоновском потоке отражает традиционный вид интегральных функций распределения вероятностей, характеризующий в данном случае то, что с увеличением интервала наблюдения (момента-шага времени t_i) вероятность превышения количества (k) произошедших событий «записей вниз» величины $N_{l_1}^{(t_0)}$ стремится к единице. Иначе говоря, в случае простейшего пуассоновского потока событий «записей вниз» деградация системы управления доступом в любом случае произойдет.

Когда (как скоро) наступит деградация – естественным образом зависит от двух параметров, исходного количества низкоуровневых объектов $N_{l_1}^{(t_0)}$ и интенсивности потока событий λ . Очевидно, что значения этих параметров определяются особенностями предметной области компьютерной системы, точнее говоря, особенностями информации (тематическими, технологическими, финансовыми, политическими и т.д.) низкоуровневых объектов и функциональными особенностями субъектов доступа (процессов пользователей). Определение параметра λ может осуществляться эмпирическим путем на основе анализа статистики возникновения событий «записей вниз».

Деградация мандатной системы управления доступом как результат нестационарного потока однородных событий «записей вниз»

Рассмотренный выше поток однородных событий «записей вниз» является стационарным. Вместе с тем, очевидно в определенных предметных областях у пользователей-субъектов доступа потребность «записей вниз» может изменяться с течением времени – уменьшаться или, наоборот, увеличиваться.

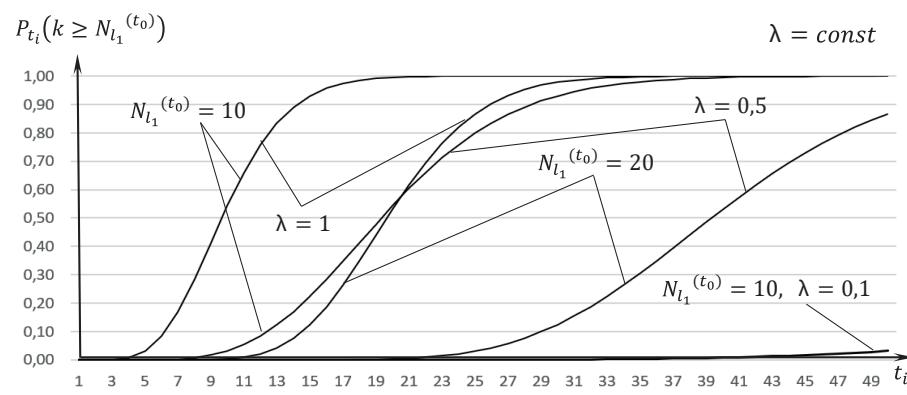


Рис. 1. Зависимость вероятности деградации мандатной системы управления доступом от времени при гипотезе о простейшем пуассоновском потоке событий «записей вниз».

$(N_{l_1}^{(t_0)})$ – количество низкоуровневых объектов в начальный момент времени; k – количество произошедших событий «записей вниз» к моменту-шагу времени t_i , т.е. количество низкоуровневых объектов, перешедших к моменту времени t_i в высокоуровневые; λ – интенсивность потока событий, т.е. среднее количество соответствующих событий в единицу времени).

В результате интенсивность (параметр λ) потока событий в таких системах не является константой и изменяется с течением времени.

Оставаясь в предположении об ординарности и отсутствии последействия потока событий «записей вниз» приходим к нестационарному пуассоновскому потоку событий, в котором вероятность деградации системы управления доступом с возможностью «записей вниз» представляется следующим соотношением

$$P_{t_i}(k \geq N_{l_1}^{(t_0)}) = 1 - e^{-\lambda(t_i)i} \sum_{m=0}^{N_{l_1}^{(t_0)}-1} \frac{(\lambda(t_i)i)^m}{m!}. \quad (3)$$

Характер зависимости интенсивности потока событий $\lambda(t_i)$ от времени может быть разным – линейным, периодическим, экспоненциальным и т.д.

При линейном характере интенсивности потока событий «записей вниз» является функций вида:

$$\lambda(t_i) = \lambda_0 \pm \beta i. \quad (4)$$

С учетом ординарности в отмеченном выше смысле потока событий «записи вниз» и ограничения значений параметра λ диапазоном $[0-1]$ будем полагать $\lambda_0 = 1$ при убывающем во времени характере $\lambda(t_i) = \lambda_0 - \beta i$. При возрастающем характере $\lambda(t_i) = \lambda_0 + \beta i$ положим $\lambda_0 = 0,1$.

На рис. 2 представлены графики вероятности деградации системы управления доступом при возрастающем характере интенсивности потока событий «записей вниз» во времени $\lambda(t_i) = \lambda_0 + \beta i$ и различных значениях параметра β , определяющем скорость возрастания $\lambda(t_i)$.

Из рисунка видно, что зависимость вероятности деградации $P_{t_i}(k \geq N_{l_1}^{(t_0)})$ от времени при возрастающей во времени интенсивности потока событий «записей вниз» $\lambda(t_i) = \lambda_0 + \beta i$ аналогична соответствующей

зависимости при стационарном потоке событий, только отличается «ускоренным» характером.

При убывающем характере интенсивности потока событий «записей вниз» после определенного момента времени ($i = \lambda_0 / \beta$) значения функции $\lambda(t_i) = \lambda_0 - \beta i$ становятся отрицательными и по смыслу параметра $\lambda(\lambda > 0)$ с этого момента приравниваются к нулю.

На рис. 3 представлены графики вероятности деградации мандатной системы управления доступом при убывающем характере интенсивности потока событий от времени $\lambda(t_i) = \lambda_0 - \beta i$ и различных значениях параметра β , ($\lambda_0 = 1$), вычисляемые по соотношению:

$$P_{t_i}(k \geq N_{l_1}^{(t_0)}) = 1 - e^{-i(\lambda_0 - \beta i)} \sum_{m=0}^{N_{l_1}^{(t_0)}-1} \frac{i(\lambda_0 - \beta i)^m}{m!}. \quad (5)$$

Как видно из рис. 3, вероятность деградации мандатной системы управления доступом при убывании интенсивности потока событий «записей вниз» во времени имеет существенно иной характер.

Сначала при увеличении интервала наблюдения вероятность деградации, как и в случае стационарного потока, также возрастает, причем при малых значениях параметра β практически до единицы (см. рис. 3), но далее при анализе для больших интервалов наблюдения (анализа) начинает уменьшаться, стремясь к нулю.

Такое странное на первый взгляд поведение объясняется тем, что вероятность $P_{t_i}(k \geq N_{l_1}^{(t_0)}) = 1 - P_{t_i}(k < N_{l_1}^{(t_0)})$ не характеризуется «накопительным» эффектом, а рассматривается в целом по промежутку времени от t_0 до t_i , на котором не должно произойти или только точно 0 событий «записей вниз», или только точно 1 событие, или ... только точно $N_{l_1}^{(t_0)} - 1$ событий. И соответственно, чем больше

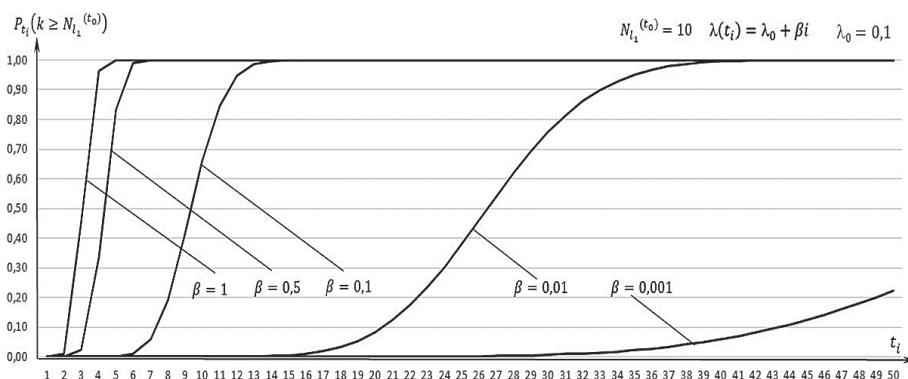


Рис. 2. Зависимость вероятности деградации мандатной системы управления доступом от времени при гипотезе о нестационарном пуассоновском потоке событий «записей вниз» с линейно возрастающей по времени интенсивностью.

($N_{l_1}^{(t_0)}$ – количество низкоуровневых объектов в начальный момент времени; k – количество произошедших событий «записей вниз» к моменту-шагу времени t_i , т.е. количество низкоуровневых объектов, перешедших к моменту времени t_i в высокоуровневые; $\lambda(t_i)$ – интенсивность потока событий, увеличивающаяся с течением времени со значением в нулевой момент времени $\lambda_0 = 0,1$ и со скоростью, определяемой параметром β).

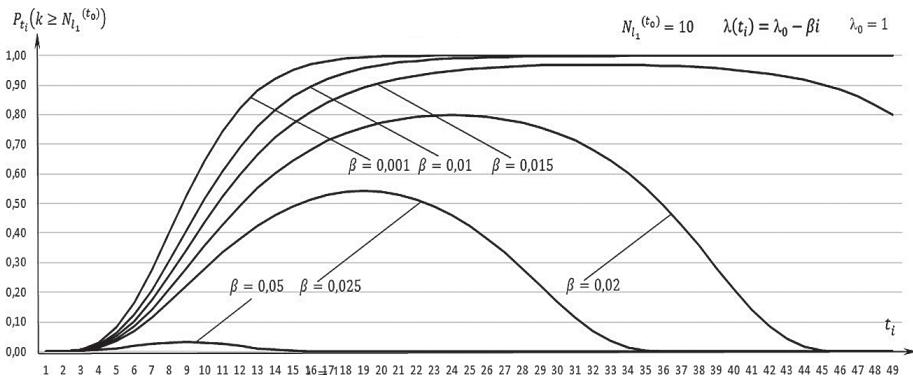


Рис. 3. Зависимость вероятности деградации мандатной системы управления доступом от времени при гипотезе о нестационарном пуассоновском потоке событий «записей вниз» с линейно убывающей по времени интенсивностью. ($N_{l_1}^{(t_0)}$ – количество низкоуровневых объектов в начальный момент времени; k – количество произошедших событий «записей вниз» к моменту-шагу времени t_i , т.е. количество низкоуровневых объектов, перешедших к моменту времени t_i в высокоровневые; $\lambda(t_i)$ – интенсивность потока событий, уменьшающаяся с течением времени со значением в нулевой момент времени $\lambda_0 = 1$ и со скоростью, определяемой параметром β).

период $(t_0 - t_i)$, т.е. чем больше t_i (при дискретном времени – i) и, соответственно, чем меньше $\lambda(t_i)$, – тем меньше вероятность совокупности отмеченных событий (только точно 0 событий, только точно 1 событие и т.д.) и соответственно суммы таких вероятностей.

Таким образом, если деградации не произошло в начальные периоды времени, когда интенсивность потока событий «записей вниз» была еще достаточно высокой (не нулевой), то в более поздние моменты времени, когда интенсивность потока событий становится практически нулевой, вероятность деградации также стремится к нулю. Данный эффект можно назвать эффектом «последнемаксимового затухания» пуассоновского процесса при убывающей интенсивности событий, который при увеличении интервала наблюдения проявляется тем быстрее, чем большим значением характеризуются скорость убывания интенсивности потока событий (параметр β).

Максимальное значение вероятности деградации характеризует экстремум (максимум) $P_{t_i}(k \geq N_{l_1}^{(t_0)})$ как функции от момента времени t_i . Значение момента времени t_i , при наблюдении на котором вероятность деградации будет максимальной, можно определить решением уравнения

$$\frac{dP_{t_i}(k \geq N_{l_1}^{(t_0)})}{di} = 0. \quad (6)$$

Для решения этого уравнения в выражении для $P_{t_i}(k \geq N_{l_1}^{(t_0)})$ по соотношению (5) обозначим $y(i) = i(\lambda_0 - \beta i)$, $N = N_{l_1}^{(t_0)}$ и произведем дифференцирование по i функции

$$f(i) = 1 - e^{-y(i)} \sum_{m=0}^{N_{l_1}^{(t_0)} - 1} \frac{(y(i))^m}{m!} (y(i))^m / m!.$$

В результате получаем

$$e^{-y(i)} \frac{de^{-y(i)}}{di} \left(\sum_{n=0}^{N-1} \frac{(y(i))^n}{n!} - \sum_{n=1}^{N-1} \frac{n(y(i))^{n-1}}{n!} \right) = 0. \quad (7)$$

Учитывая, что $e^{-y(i)} > 0$, для нахождения 1-го корня имеем

$$\lambda_0 - 2\beta i = 0,$$

откуда

$$i_{\text{экстремум1}} = \frac{\lambda_0}{2\beta}. \quad (8)$$

Второй и третий корни определяются по равенству 0 третьего сомножителя в соотношении (7):

$$\begin{aligned} \left(\sum_{n=0}^{N-1} \frac{(y(i))^n}{n!} - \sum_{n=1}^{N-1} \frac{n(y(i))^{n-1}}{n!} \right) &= \sum_{n=0}^{N-1} \frac{(y(i))^n}{n!} - \sum_{n=1}^{N-1} \frac{(y(i))^{n-1}}{(n-1)!} = \\ &= \sum_{n=0}^{N-1} \frac{(y(i))^n}{n!} - \sum_{m=0}^{N-2} \frac{(y(i))^m}{m!} = 0, \end{aligned}$$

где $j = n - 1$.

Преобразовывая, далее имеем

$$\sum_{n=0}^{N-1} \frac{(y(i))^n}{n!} - \sum_{m=0}^{N-2} \frac{(y(i))^m}{m!} = \frac{(y(i))^{N-1}}{(N-1)!} = 0,$$

откуда следует

$$i(\lambda_0 - \beta i) = 0.$$

В результате получаем³:

$$i_{\text{экстремум2}} = 0, i_{\text{экстремум3}} = \frac{\lambda_0}{\beta}.$$

Второй и третий корни не рассматриваем по смыслу отмеченных ранее ограничений на интервал значений интенсивности потока событий $0 < \lambda \leq 1$.

Таким образом, максимум вероятности деградации мандатной системы управления доступом с возможностью «записей вниз» приходится на момент времени $t_i = \frac{\lambda_0}{\beta}$ и не зависит от начального количества

3 Результаты по нахождению точек экстремума функции $P(t_i)$ ($k \geq N_{l_1}^{(t_0)}$) при убывающем характере интенсивности потока событий получены совместно с Караваевым А. С.

низкоуровневых объектов $N_{l_1}^{(t_0)}$, что соответствует численным данным на графиках $P_{t_i}(k \geq N_{l_1}^{(t_0)})$, представленным на рис. 3.

Значение вероятности деградации $P_{t_i}(k \geq N_{l_1}^{(t_0)})$ в точке максимума определяется соотношением

$$1 - e^{-\frac{\lambda_0}{2\beta}(\lambda_0 - \beta\lambda_0)} \sum_{m=0}^{N_{l_1}^{(t_0)}-1} \frac{\left(\frac{\lambda_0}{2\beta}(\lambda_0 - \beta\lambda_0)\right)^m}{m!}, \quad (9)$$

анализ которого показывает, что единичное значение $P_{t_i}(k \geq N_{l_1}^{(t_0)})$ в точке максимума достигается при нулевом значении скорости убывания интенсивности потока событий «записей вниз» ($\beta = 0$), т.е. при стационарном потоке событий.

Иначе говоря, при очень малых значениях β вероятность деградации мандатной системы управления доступом с возможностью «записей вниз» в момент времени $t_i = \frac{\lambda_0}{2\beta}$ может быть сколь угодно близкой к единице (но не равной ей).

Интересно отметить, что в других приложениях, характеризующихся сходными по смыслу процессами деградации, рассматривается экспоненциальный

характер зависимости $\lambda(t_i)$. В частности, в исследованиях старения и смертности биологических видов широко известно распределение Гомпертца-Мейххама [12], которое также применяется в исследованиях «старения» информации [13], в частности старения научной [14] и маркетинговой [15] информации, в анализе надежности и жизненного цикла сложных технических систем [16] и т.д.

В отмеченных предметных областях интенсивность потока событий рассматривается как функция вида

$$\lambda(t_i) = a + b e^{\lambda_0 t_i}, \quad (10)$$

что обеспечивает учет как постоянной во времени составляющей процессов деградации (параметр a), так и переменной с течением времени (параметры b и λ_0). При этом параметр λ_0 определяет «скорость» экспоненциального изменения интенсивности потока событий и может быть как положительным (интенсивность потока событий со временем возрастает), так и отрицательным (интенсивность потока событий со временем убывает).

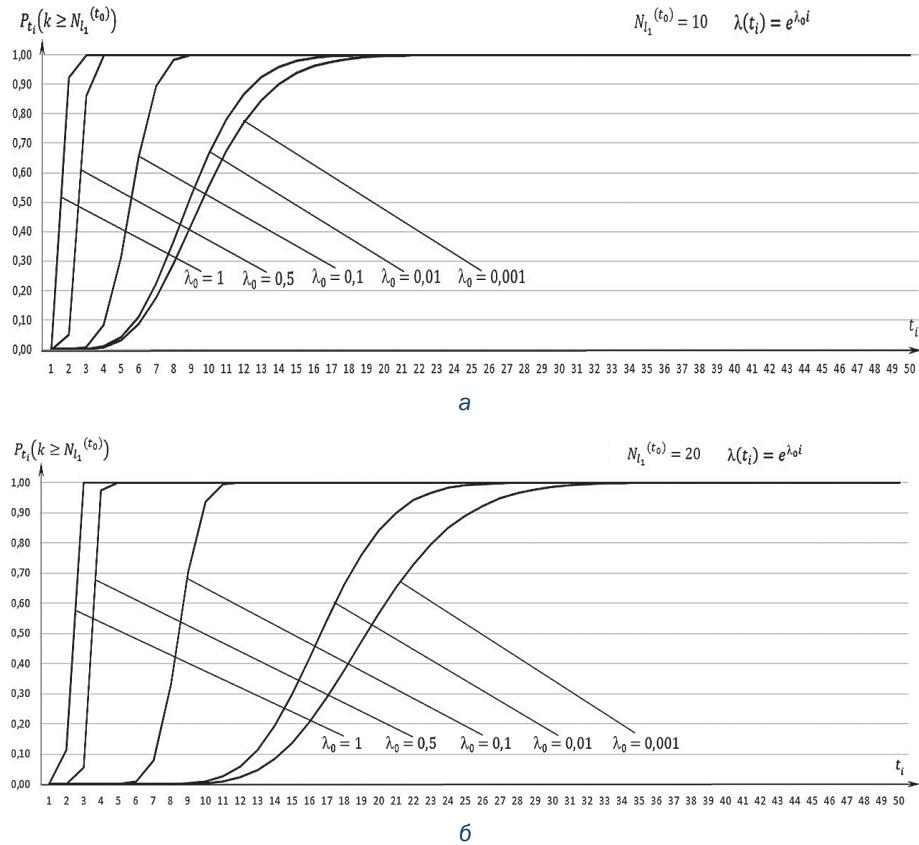


Рис. 4. Зависимость вероятности деградации мандатной системы управления доступом от времени при гипотезе о нестационарном пуассоновском потоке событий «записей вниз» с экспоненциально возрастающей по времени интенсивностью.

$(N_{l_1}^{(t_0)})$ – количество низкоуровневых объектов в начальный момент времени; k – количество произошедших событий «записей вниз» к моменту-шагу времени t_i , т.е. количество низкоуровневых объектов, перешедших к моменту времени t_i в высокогуровневые; $\lambda(t_i) = e^{\lambda_0 t_i}$ – интенсивность потока событий, экспоненциально возрастающая с течением времени со скоростью, определяемой параметром λ_0).

Рассмотрим сначала, как и при линейном характере функции $\lambda(t_i)$, деградацию мандатной системы управления доступом при экспоненциально возрастающей с течением времени интенсивностью потока событий «записей вниз». При этом для простоты положим $a = 0$, $b = 1$. Тогда $\lambda(t_i)$ будет характеризоваться простой экспоненциальной зависимостью от времени $\lambda(t_i) = e^{\lambda_0 i}$, $\lambda_0 \geq 0$. Соответственно зависимость вероятности деградации системы управления доступом от времени будет выражаться следующим соотношением:

$$P_{t_i}(k \geq N_{l_1}^{(t_0)}) = 1 - e^{-ie^{\lambda_0 i}} \sum_{m=0}^{N_{l_1}^{(t_0)} - 1} \frac{(ie^{\lambda_0 i})^m}{m!}. \quad (11)$$

На рис. 4 представлены графики вероятности деградации мандатной системы управления доступом при экспоненциально возрастающем характере интенсивности потока событий «запись вниз» во времени $\lambda(t_i) = e^{\lambda_0 i}$, различных значениях параметра λ_0 , определяющем скорость возрастания $\lambda(t_i)$, и при начальном количестве низкоуровневых объектов $N_{l_1}^{(t_0)} = 10$ (рис. 4а), $N_{l_1}^{(t_0)} = 20$ (рис. 4б).

Из рис. 4 видно, что и в случае с линейно возрастающей во времени интенсивностью, при экспоненциально возрастающей во времени интенсивности потока событий «записей вниз» $\lambda(t_i) = e^{\lambda_0 i}$ характер изменения со временем вероятности деградации системы управления доступом в целом аналогичен характеру при стационарном потоке событий и отличается только большей «ускоренностью» возрастания.

При экспоненциально убывающем характере интенсивности потока событий «записей вниз» вероятность деградации мандатной системы управления доступом определяется выражением

$$P_{t_i}(k \geq N_{l_1}^{(t_0)}) = 1 - e^{-ie^{-\lambda_0 i}} \sum_{m=0}^{N_{l_1}^{(t_0)} - 1} \frac{(ie^{-\lambda_0 i})^m}{m!}. \quad (12)$$

где λ_0 – параметр, определяющий скорость убывания интенсивности потока событий «записей вниз» во времени.

На рис. 5 представлены графики вероятности деградации мандатной системы управления доступом

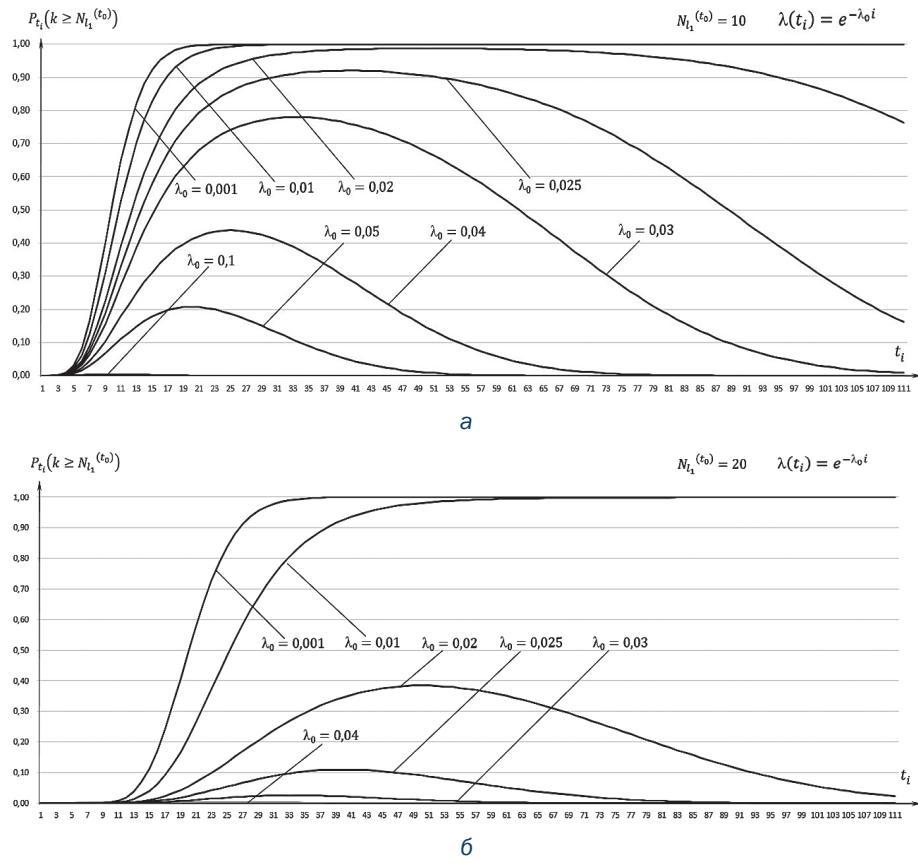


Рис. 5. Зависимость вероятности деградации мандатной системы управления доступом от времени при гипотезе о нестационарном пуссоновском потоке событий «записей вниз» с экспоненциально убывающей по времени интенсивностью.

$(N_{l_1}^{(t_0)})$ – количество низкоуровневых объектов в начальный момент времени; k – количество произошедших событий «записей вниз» к моменту-шагу времени t_i , т.е. количество низкоуровневых объектов, перешедших к моменту времени t_i в высокоровневые; $\lambda(t_i) = e^{\lambda_0 i}$ – интенсивность потока событий, экспоненциально возрастающая с течением времени со скоростью, определяемой параметром λ_0 .

при экспоненциально убывающем характере интенсивности потока событий «записей вниз» во времени $\lambda(t_i) = e^{-\lambda_0 i}$, различных значениях параметра λ_0 , определяющем скорость убывания $\lambda(t_i)$, и при начальном количестве низкоуровневых объектов $N_{l_1}^{(t_0)} = 10$ (рис. 5а), $N_{l_1}^{(t_0)} = 20$ (рис. 5б).

Из рис. 5 видно, что как и в случае с линейно убывающей интенсивностью потока событий «запись вниз», зависимость от времени вероятности деградации мандатной системы управления доступом характеризуется таким же эффектом «последнемаксимумного затухания», т.е. наличием максимума и дальнейшим убыванием к нулю при увеличении момента времени наблюдения-анализа t_i .

Производя аналогичным образом дифференцирование по i функции в правой части соотношения (12) и приравнивая результат дифференцирования к нулю, находим точку максимум вероятности деградации $P_{t_i}(k \geq N_{l_1}^{(t_0)})$:

$$t_{imax} = \frac{1}{\lambda_0},$$

что также соответствует численным данным на графиках $P_{t_i}(k \geq N_{l_1}^{(t_0)})$, представленным на рис. 5.

Заключение

Представленный анализ мандатных систем управления доступом с возможностью «записей вниз» показывает в большинстве случаев их «неизбежную» деградацию при тех или иных условиях и параметрах возникновения у пользователей соответствующих потребностей (в «записях вниз»). При этом, однако, при убывающих со временем у пользователей потребностях в «записях вниз» тенденция к деградации характеризуется эффектом «последнемаксимумного затухания», что может быть использовано в технологических процессах обработки информации или отражать такие процессы.

Тем не менее тенденция к деградации в виде уменьшения со временем количества низкоуровневых объектов из-за их перехода в высокоуровневые проявляется в любом случае.

В результате стремление к расширению функциональности мандатных систем обработки информации

через введение возможности «записей вниз» приводит, в свою очередь, к ограничению функциональности в виде тенденции к деградации, при которой низкоуровневые пользователи (с низким уровнем доступа) со временем не смогут получать доступ по чтению ко всем или к большинству объектов доступа. При этом следует оговориться, что данные выводы характеризуют системы управления доступом, в которых со временем новые низкоуровневые объекты доступа не создаются. В этом отношении порождение новых низкоуровневых объектов может снизить остроту проблемы деградации и соответствующее ограничение функциональности таких систем.

Принципиальным же направлением поиска теоретических и практических решений по устранению проблемы деградации в мандатных системах управления доступом с возможностью «записей вниз» и обеспечению их большей функциональности является разработка механизмов анализа конфиденциальности информации (классификации информации), записываемой пользователями в объекты доступа. При наличии таких доверенных и эффективных механизмов в случае, когда пользователь с высоким уровнем допуска записывает в низкоуровневый объект только низкоуровневую информацию, отпадает необходимость в команде reset и после записи объект остается низкоуровневым, что устраняет тенденцию к деградации.

Однако подобные механизмы на сегодняшний день эффективно и в полной мере реализуются только на основе содержательного анализа информации человеком-пользователем, в первую очередь при присваивании объекту доступа его уровня (метки) конфиденциальности. Тем не менее в DLP системах [17], которые играют в настоящее время важную роль в системах защиты информации, применяются или иные механизмы анализа (классификации) конфиденциальности информации, «ходящей» за периметр защищаемой системы. Очевидно, подобные «наработки» следует проанализировать на предмет возможности использования в мандатных системах управления доступом при санкционировании запросов «записей вниз».

Литература

1. Bell D. E., LaPadula L. J. Secure Computers Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976. – MTR-2997 Rev. 1.
2. Guo J. K. et al. Applicability of low water-mark mandatory access control security in linux-based advanced networked consumer electronics //First IEEE Consumer Communications and Networking Conference, 2004. CCNC 2004. – IEEE, 2004. – С. 364–369.
3. Landwher K. E. Formal Model Computer Security // Computer surveys, Vol 13, No 3, September 1981. pp. 247–278.
4. Bishop, M. Introduction to Computer Security / M. Bishop. – Addison- Wesley Professional, 2004. – 785 p.
5. Mohamed A., Auer D., Hofer D., Küng J. A systematic literature review for authorization and access control:definitions, strategies and models // International Journal of WebInformation Systems. Vol. 18 No. 2/3, 2022. pp. 156-180. DOI 10.1108/IJWIS-04-2022-0077.
6. Biba K. J. Integrity considerations for secure computer systems. ESD-TR- 76-372, ESD/AFSC, Hanscom AFB, Bedford, Mass., April 1977 (MITRE MTR-3153, NTIS AD A039324).

7. Weissman C. Security controls in the ADEPT-50 time sharing system. Proc. 1969 AFIPS Fall Jt Computer Conf., vol. 35, AFIPS Press, Arlington, Va., pp. 119–133.
8. McLean J. Security models and information flow. In Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy. IEEE Computer Society Press, 1990.
9. McLean J. The specification and modeling of computer security. Computer, 23(1): 9–16, January 1990.
10. Гайдамакин Н. А. Модель и метрики осведомленности в конфиденциальной информации. Часть 1. Потенциальная осведомленность // Прикладная дискретная математика. 2023. № 61. С. 86–103.
11. Кингман Дж. Пуассоновские процессы. — М.: МЦНМО, 2007. – 136 с.
12. Gavrilov L. A., Gavrilova N. S. The Biology of Life Span: A Quantitative Approach., New York: Harwood Academic Publishers, 1991.
13. Парамонов И. Ю. Модель учета ценности и старения информации при оценивании эффективности функционирования систем информационного обеспечения // Системы управления, связи и безопасности. 2016. № 1. С.238–334.
14. Климов Ю. Н. Исследование закономерностей старения научной информации // Машиностроение, методы исследования и моделирования. 2004. № 4. С. 40–44.
15. Чернявский А. Д. Моделирование скорости распространения маркетинговой информации с учётом изменения ценности информации во времени // Экономический анализ: теория и практика. 2009. № 7. С. 54–60.
16. Ташевский А. Г. Математические модели продолжительности жизненного цикла технических систем // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. 2014. № 1(190). С. 169–178.
17. Papadimitriou P., Garcia-Molina H. Data Leakage Detection // IEEE transactions on knowledge and data engineering, vol. 23, no. 1, January 2011. pp. 51-63.

ANALYSIS OF THE DEGRADATION OF ACCESS CONTROL SYSTEMS BASED ON MANDATED MODELS WITH THE ABILITY TO «WRITE DOWN»

Gaydamakin N. A.⁴

Keywords: mandatory access control principle, «write down», «write down» event flow, degradation of the access control system, «post-maximum attenuation» effect.

Purpose of the study: to conduct a theoretical analysis of the functioning of mandatory access control systems, in which, in order to expand the functional capabilities for processing information, access subjects are allowed to perform «write down».

Methods of research: application of the Poisson event flow apparatus for formalization and analysis of the functioning of mandatory access control systems with the possibility of "write down".

Result: The process of functioning of the mandatory access control system with the possibility of «write down» is considered as a Poisson flow of homogeneous events of occurrence and implementation by high-level access subjects (users with a high access level) of needs for recording information in low-level access objects (files, documents with a low confidentiality level). As a result of each such event after the completion of the «write down», in order to prevent possible further familiarization of low-level users with high-level information, the confidentiality level of the access object is increased to the access level of the corresponding (writing) subject. The concept of degradation of the access control system is introduced, which consists in the fact that with two levels of access and confidentiality (high and low), over time all access objects in terms of confidentiality become high-level, and accordingly inaccessible for «reading» for subjects (users) with a low access level.

The probability of the onset of degradation of the access control system in the case of stationarity and non-stationarity of the Poisson flow of "write down" events is analyzed. With decreasing intensity of "down write" events over time, an unusual at first glance nature of the change in the probability of degradation over time is considered, which can be called the «post-maximum attenuation» effect, consisting first in an increase in the probability of degradation over time with the achievement of a certain maximum value at a certain point in time, and then in a gradual decrease in the probability of degradation to zero. With a linear and exponential nature of the decrease in the intensity of the flow of «down write» events, relationships are obtained for the time point with the maximum probability of degradation, which is determined by the rate of decrease in the intensity of the flow of events.

References

1. Bell D. E., LaPadula L. J. Secure Computers Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976. – MTR-2997 Rev. 1.
2. Guo J. K. et al. Applicability of low water-mark mandatory access control security in linux-based advanced networked consumer electronics //First IEEE Consumer Communications and Networking Conference, 2004. CCNC 2004. – IEEE, 2004. – С. 364–369.

⁴ Nikolay A. Gaydamakin, Dr.Sc. of Technical Sciences, Professor, Professor of the Department of Algebra and Fundamental Informatics, Ural Federal University named after the first President of Russia B. N. Yeltsin, Yekaterinburg, Russia. E-mail: n.a.gaidamakin@urfu.ru

3. Landwher K. E. Formal Model Computer Security // Computer surveys, Vol 13, No 3, September 1981. pp. 247–278.
4. Bishop, M. Introduction to Computer Security / M. Bishop. – Addison-Wesley Professional, 2004. – 785 p.
5. Mohamed A., Auer D., Hofer D., Küng J. A systematic literature review for authorization and access control: definitions, strategies and models // International Journal of Web Information Systems. Vol. 18 No. 2/3, 2022. pp. 156-180. DOI 10.1108/IJWIS-04-2022-0077.
6. Biba K. J. Integrity considerations for secure computer systems. ESD-TR- 76-372, ESD/AFSC, Hanscom AFB, Bedford, Mass., April 1977 (MITRE MTR-3153, NTIS AD A039324).
7. Weissman C. Security controls in the ADEPT-50 time sharing system. Proc. 1969 AFIPS Fall Jt Computer Conf., vol. 35, AFIPS Press, Arlington, Va., pp. 119–133.
8. McLean J. Security models and information flow. In Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy. IEEE Computer Society Press, 1990.
9. McLean J. The specification and modeling of computer security. Computer, 23(1): 9–16, January 1990.
10. Gaydamakin N.A. Model' i metriki osvedomlennosti v konfidentsial'noy informatsii. Chast' 1. Potentsial'naya osvedomlennost' // Prikladnaya diskretnaya matematika. 2023. № 61. S. 86–103.
11. Kingman Dzh. Puassonovskiye protsessy. – M.: MTSNMO, 2007. – 136 s.
12. Gavrilov L. A., Gavrilova N. S. The Biology of Life Span: A Quantitative Approach., New York: Harwood Academic Publishe, 1991.
13. Paramonov I. Yu. Model' ucheta tsennosti i stareniya informatsii pri otsenivaniyu effektivnosti funktsionirovaniya sistem informatsionnogo obespecheniya // Sistemy upravleniya, svyazi i bezopasnosti. 2016. № 1. S. 238–334.
14. Klimov Yu. N. Issledovaniye zakonomernostey stareniya nauchnoy informatsii // Mashinostroyeniye, metody issledovaniya i modelirovaniya. 2004 №4. C. 40–44.
15. Chernyavskiy A. D. Modelirovaniye skorosti rasprostraneniya marketingovoy informatsii s uchotom izmeneniya tsennosti informatsii vo vremeni // Ekonomicheskiy analiz: teoriya i praktika. 2009. № 7. S. 54–60.
16. Tashevskiy A. G. Matematicheskiye modeli prodolzhitel'nosti zhiznennogo tsikla tekhnicheskikh sistem // Nauchno-tehnicheskiye vedomosti Cankt-Peterburgskogo gosu-darstvennogo politekhnicheskogo universiteta. 2014. № 1(190). C. 169–178.
17. Papadimitriou P., Garcia-Molina H. Data Leakage Detection // IEEE transactions on knowledge and data engineering, vol. 23, no. 1, January 2011. pp. 51-63.

