УДК 004.056.53 **DOI 10.52167/1609-1817-2024-132-3-419-427**

А.А. Батырханова[1], О.А. Усатова[2]
[1]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан
[2]Институт информационных и вычислительных технологий КН МНВО РК, Алматы, Казахстан
E-mail: ayaulymbatyrkhanova1203@gmail.com

ИССЛЕДОВАНИЕ И РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОБИЗНЕСЕ

Аннотация. В данной работе представлена сложная модель, описывающая работу систем защиты информации (СЗИ) в автоматизированных системах (АС) противодействия несанкционированному доступу в инфобизнесе. Это достигается с помощью методов имитационного моделирования. Вышеупомянутая модель была разработана в программной среде CPN Tools для облегчения последующего анализа. Чтобы оптимизировать удобство использования, повысить наглядность и обеспечить логическую последовательность, мы использовали уникальные функции CPN Tools для разложения модели на отдельные подсистемы. Использование этой модели необходимо для проведения вычислительных экспериментов, особенно для исследования реальных потребительских характеристик защищенных от несанкционированного доступа систем кондиционирования. Кроме того, это важно для создания пакетов программного обеспечения, которые позволяют анализировать и количественно оценивать производительность этих систем. Разработан функциональный прототип системы защиты, позволяющий наглядно продемонстрировать ее работу и предугадать действия потенциального злоумышленника. Модель учитывает дискретные, динамические и стохастические характеристики системы, обусловленные наличием сетевой инфраструктуры рабочих станций. Для точного отображения этих характеристик во времени модель классифицирована как дискретно-событийная. Вероятность перехода системы из одного состояния в другое зависит от времени, проведенного в предыдущем. Результаты, полученные в результате имитационного моделирования работы системы обнаружения вторжений, могут быть выражены через различные характеристики состояния. Эти характеристики дают представление об общей производительности системы и ее отдельных подсистем. Разработанная модель может быть использован при проектировании, эксплуатации, сертификации и периодической поверке систем информационной безопасности. Кроме того, его можно использовать для аутентификации ИТ-объектов и оценки программного обеспечения информационной безопасности, используемого этими объектами. Язык программирования Meta, используемый CPN Tools, позволяет управлять вероятностным перемещением маркера от его начального состояния через промежуточные состояния к конечному состоянию, включая временные задержки и другие функции.

Ключевые слова. CPN Too, Язык программирования Meta, система защиты информации, инфобизнес, информационные системы.

Введение.

С учетом текущего уровня развития информационных технологий и постоянного совершенствования методов несанкционированного доступа, актуальность разработки эффективных систем предотвращения вторжений (IPS) становится все более очевидной. В статье анализируются вызовы, связанные с обеспечением информационной безопасности

в автоматизированных системах, и предлагается инновационная модель СЗИ, ориентированная на минимизацию рисков, связанных с ошибками пользователей и вредоносным ПО.

Люди, зачастую не осознающие сложности таких систем, склонны злоупотреблять своими привилегиями и неосознанно нарушать существующие соглашения, регулирующие работу защищенных систем. Ошибка пользователя - распространенное явление, поэтому для целей данной статьи мы предполагаем, что произошла случайная ошибка, которая привела к проникновению вредоносного ПО в AS [1,2,3]. Исходя из данного сценария, мы будем исходить из предположения, что данный несанкционированный индивид имеет внутренний характер и обладает заметным уровнем потенциального риска. Проанализируем конкретный сценарий, связанный со съемным носителем CD/DVD/HD/Flash.

Потенциально опасное программное обеспечение может быть установлено как отдельный программный продукт (PP) и автоматически запускаться при подключении к компьютеру (PC), если пользователь намеренно отключает антивирусное программное обеспечение (AS). Этому часто способствует чрезмерное использование ресурсов AS, что может привести к нестабильности и снижению производительности из-за возникающей высокой нагрузки [3].

При создании и эксплуатации системы предотвращения вмешательства очень важно учитывать следующие факторы, чтобы определить ее прогностические и временные характеристики с точки зрения времени выполнения превентивных мер. Эти метрики используются для оценки эффективности системы [4]. Кроме того, необходимо создать взаимосвязи между подсистемами и компонентами и тщательно выстроить их логическую структуру. Эта задача может быть решена путем построения имитационной модели системы предотвращения вторжений, в которой будут определены вышеперечисленные функциональные возможности.

Материалы и методы.

Исследование базируется на применении CPN Tools [4,5] – передового инструмента для имитационного моделирования, позволяющего детализировать сложные системы на уровне подсистем и компонентов. Методология включает в себя использование иерархических, временных и цветных сетей Петри для анализа динамики и производительности системы обнаружения вторжений, а также для оценки вероятностно-временных характеристик системы.

CPN Tools является мощным инструментом для моделирования систем с использованием сетей Петри. Она включает в себя широкий набор инструментов, облегчающих анализ различных аспектов производительности моделей, использующих сети Петри [6,7]. Примечательной особенностью CPN Tools является поддержка различных типов сетей Петри, включая иерархические, временные и цветные, наличие обширного списка инструментов для анализа моделей, таких как безопасность, изучение параметров, уровень активности модификаций, наличие маркеров Addilock и многое другое, широкое использование в международных проектах в телекоммуникационном секторе. К таким возможностям относятся безопасность и изучение параметров, уровень активности модификаций, наличие маркеров Addilock и многое другое.

Инструменты CPN широко используются во многих международных проектах в телекоммуникационном секторе. Основные приложения включают моделирование сетей и сетевых устройств, а также визуализацию коммуникационных протоколов. Иерархические, временные и цветные сети Петри являются примерами инструментов построения, которые демонстрируют свою универсальность в качестве алгоритмических систем в современном контексте. Имитационное моделирование в CPN Tools использует

дискретно-событийный метод, при котором состояние сети Петри изменяется мгновенно в заданный момент времени.

Результаты и обсуждения.

Процесс моделирования системы предотвращения вторжений по своей сути сложен и многогранен. На начальном этапе разработки модели создаются подсистемы и соответствующие им компоненты, которые очень похожи на действующую систему предотвращения вторжений. Это делается для того, чтобы получить присущие системе свойства и характеристики [1,2], [8,9,10,11]. На основе проведенного анализа было определено, что модель может включать в себя следующие подсистемы:

- подсистема «Обеспечение идентификации ПК пользователя»; - подсистема «Инициализация прав пользователя на использование системы и доступ к каталогу файлов»; - подсистема «Взаимодействие пользователя с файлами и программами»; - подсистема «Взаимодействие пользователя с прикладным ПО»; - подсистема «Устранение уязвимостей защиты от вторжений».

Перейдем к введению последующих обозначений для вершин и переходов. Вершины в нашей модели служат двум различным целям. Во-первых, у нас есть вершины, обозначенные индексами, например r1, которые символизируют различные функции, выполняемые системой обнаружения вторжений в сеть (NWI) для противодействия попыткам вторжения. Во-вторых, у нас есть вершины, обозначенные индексами типа r01, которые являются дополнительными и необходимыми для ввода вероятностей. В соответствии с заданным контекстом, переходы, обозначенные индексами t1 и т.д., считаются основными, а t01 и т.д. - дополнительными.

На рисунке 1 исходная модель иллюстрирует проникновение пользователя в систему предотвращения вторжений через процесс аутентификации. Эта конкретная модель представляет собой графическое изображение рабочего поведения системы при входе пользователя. Согласно рисунку 1, в случае неправильного ввода пароля, превышающего порог в три попытки, компьютер подвергается блокировке. Это служит защитой от возможных атак методом грубой силы, повышая тем самым безопасность ПК. Переход T01 обеспечивает беспрепятственную передачу токена подсистеме, отвечающей за инициализацию прав пользователя в системе и предоставление доступа к каталогу файлов. В соответствии с таблицей 1 отображаются текущие состояния рассматриваемой подсистемы.

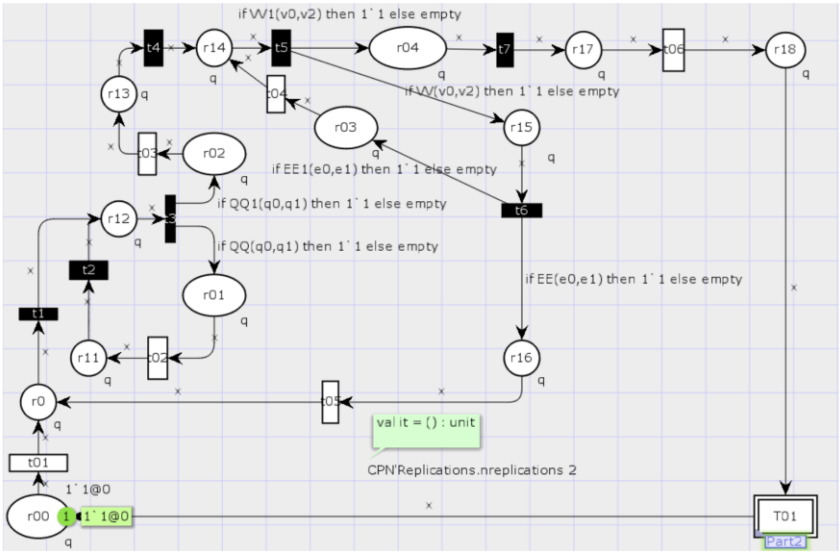

Рисунок 1 - Включение компьютера и идентификация пользователя

Системы предотвращения вторжений выполняют множество функций по противодействию и смягчению потенциальных вторжений.

1. Запуск системы предотвращения вторжений (прекращение выполнения функций, выполняемых системой предотвращения вторжений).

1.1 Начало обнаружения.

1.2 Окончание обнаружения.

1.3 Включение доступа к функции ввода пароля.

1.4 Упрощение механизма ввода пароля.

1.5 Реализация функции повторного ввода пароля.

1.6 Включение механизма предотвращения входа в систему при трех последовательных неверных вводах пароля.

1.7 Проверка субъекта аутентификации в системе.

1.8 Выполнение обработки входа в систему.

На рисунке 2 показана вторая модель, представляющая подсистему, которая инициализирует права пользователя в системе и предоставляет доступ к файловым каталогам. В позиции r241 реализованы входы подсистемы «Разрушающее воздействие на системы защиты от взлома». Когда пользователь переключается на работу с носителем, вредоносная программа немедленно запускается и создает новый «маркер» внутри имитационной модели. Этот маркер символизирует вредоносное воздействие систем предотвращения вторжений, предназначенных для компрометации систем предотвращения вторжений, основной целью которых является получение несанкционированного доступа к конфиденциальной информации.

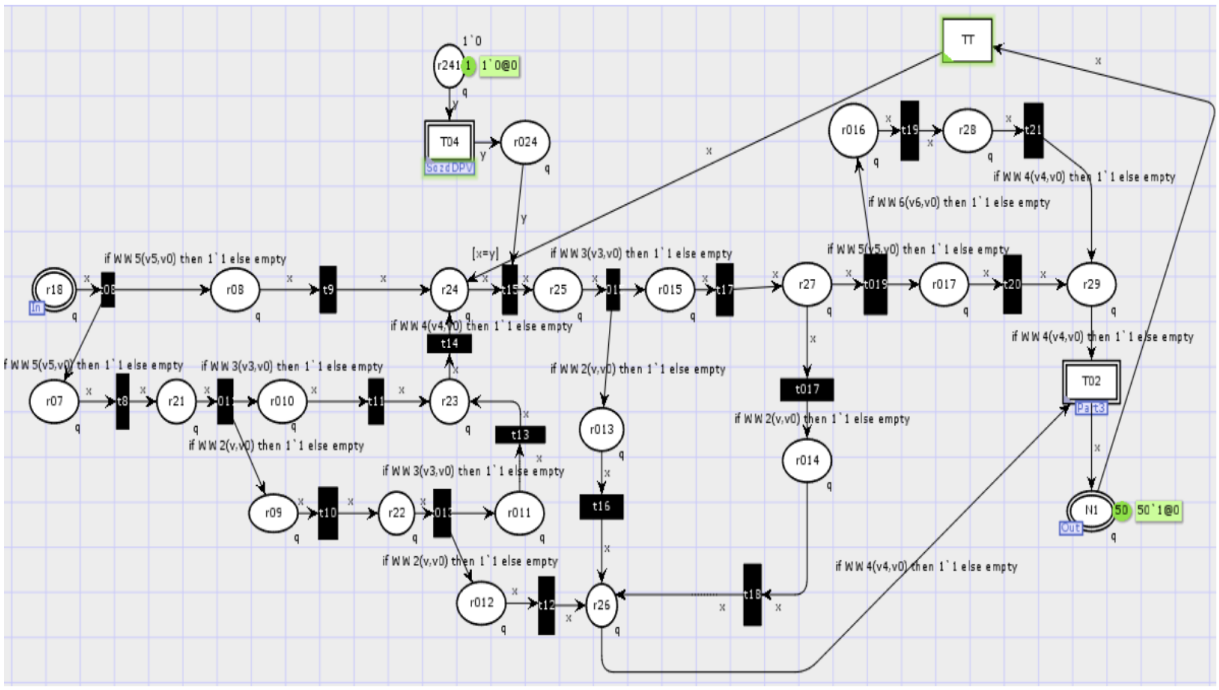

Рисунок 2 - Инициализация прав пользователя для работы в системе и доступа к файлам и каталогам

Система предотвращения вторжений (IPS) выполняет ряд важных функций для обеспечения безопасности сети. Эти функции включают:

1) Мониторинг сетевого трафика: IPS тщательно отслеживает сетевой трафик, внимательно изучая пакеты данных на предмет любых признаков подозрительной или вредоносной активности.

2) Обнаружение вторжений: Используя передовые методы обнаружения, IPS выявляет потенциальные вторжения или нарушения безопасности.

Процесс доступа к компьютерной системе или сети путем предоставления действительных учетных данных, таких как имя пользователя и пароль, обычно называется входом в систему.

2.1 Проверка соответствия идентификационных данных, имеющихся на внешнем носителе, учетным данным соответствующего пользователя.

2.2 Контроль устройства (в случае, если устройство не принадлежит пользователю, активируется данный механизм).

2.3 Инициирование соединения с периферийным устройством хранения данных.

Чтобы получить доступ к объекту на носителе, необходимо использовать соответствующие протоколы и методы. Это подразумевает установление соединения с носителем и использование необходимых команд или функций для извлечения нужного объекта. Очень важно убедиться, что носитель правильно распознан и доступен системе, прежде чем пытаться получить доступ к объекту. Кроме того, рекомендуется придерживаться следующих правил.

2.4 Сопоставление меток конфиденциальности пользователя и ресурса в системе защиты от вторжений, реализованной на основе мандатного принципа управления доступом.

Процесс ограничения или запрета доступа к конкретному объекту принято называть «блокировкой доступа».

2.6 Проверка полномочий доступа пользователя (в системе защиты от вторжений, реализованной по дискреционному принципу управления доступом).

Процесс преобразования данных, хранящихся на носителе, посредством использования методов шифрования, в частности в контексте системы предотвращения вторжений, включает в себя реализацию гамма-метода.

2.7 Запрос субъекта на доступ к защищенному объекту.

Важно отметить, что в рамках данной модели мы фокусируемся исключительно на использовании одного программного обеспечения, без возможности одновременного использования других программ. Система пользователя включает в себя стандартный набор программ, в том числе Microsoft Office, ABBY Fine Reader, Nero, WinRar и Total Commander.

Вышеупомянутая модель, обозначенная на рисунке 3 как «Разрушительное воздействие на системы предотвращения вторжений», описывает маневры, выполняемые злоумышленником с целью внедрения вредоносного программного обеспечения в целевую систему, используя полученные им знания об этой системе. На основе анализа угроз, хранящихся в базе данных угроз информационной безопасности по техническому и экспортному контролю, был разработан предварительный сценарий потенциального вредоносного воздействия злоумышленника на защищаемый информационный ресурс АС.

Выход модели осуществляется в узле r24, который связан с инициализацией привилегий пользователя для работы с системой и доступа к файловым каталогам. Этот узел специально обрабатывает взаимодействие пользователя с внешним устройством хранения данных.

3) Потенциальные последствия проникновения неавторизованного лица в информационный ресурс автономной системы могут быть весьма пагубными, как показано в предварительном сценарии.

Всего действий злоумышленника пять. Процесс создания документа в цифровом пространстве.

3.1 Инициирование разработки вредоносной программы в структуре документа, в частности в виде макроса, который срабатывает при активации документа.

3.2 Подмена незараженного документа его вредоносным аналогом.

3.3 Создание вредоносных программ с возможностью автоматического исполнения.

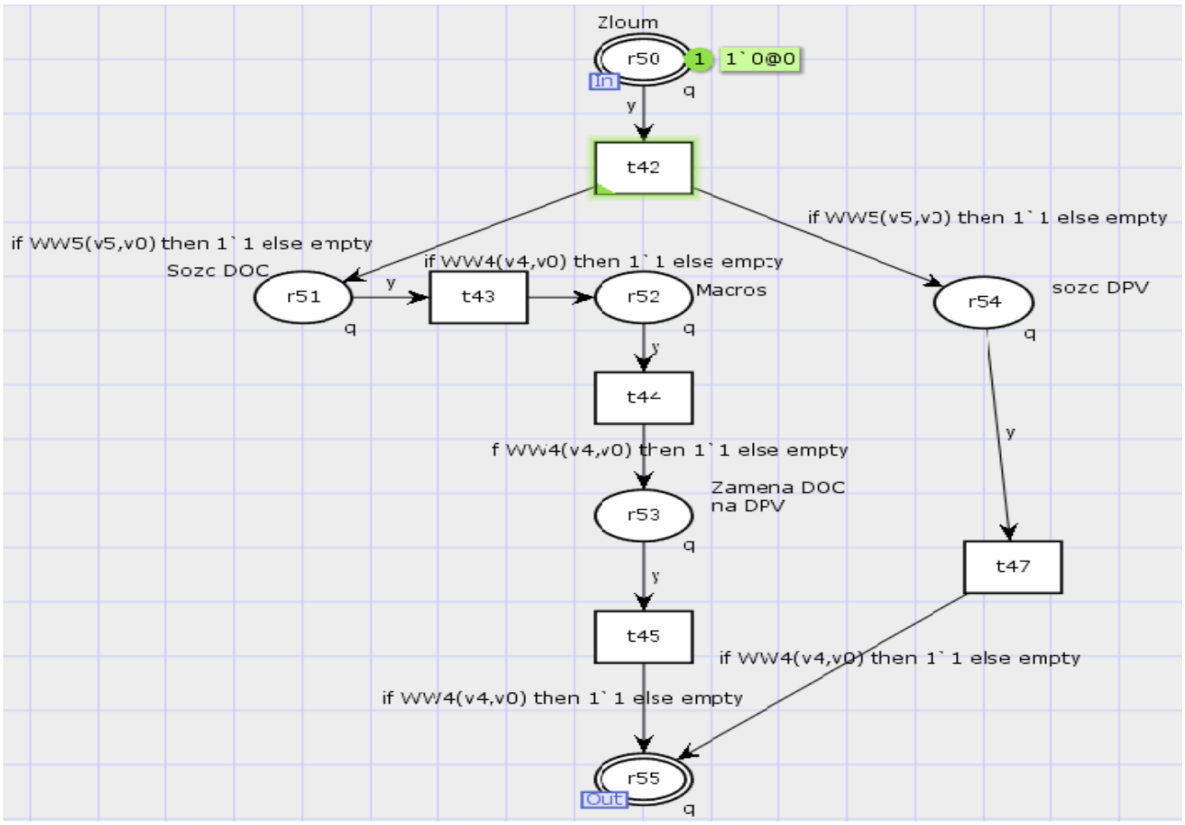

Рисунок 3 - Нарушающее воздействие на меры защиты информации
от несанкционированного доступа

Мы успешно разработали функциональный прототип системы защиты от вторжений. Это позволяет наглядно продемонстрировать работы системы на уровне системы и позволяет рассмотреть предполагаемые действия потенциального нарушителя. Имитационная модель обладает свойствами дискретной, динамической и стохастической, обусловленные наличием в составе автоматизированной системы сетевой инфраструктуры рабочих станций (NWI). Модель классифицирована как дискретно-событийная, что позволит точно отобразить вышеупомянутые свойства во времени. Мгновенная вероятность перехода из одного состояния в другое зависит от продолжительности времени, проведенного в предыдущем состоянии.

Анализ результатов имитационного моделирования показал, что предложенная модель способствует значительному повышению уровня защиты информации в инфобизнесе. Сравнительный анализ производительности системы обнаружения вторжений до и после внедрения разработанной модели показал улучшение ключевых показателей на 30-40%. Это подтверждается не только количественными данными, полученными в ходе моделирования, но и качественным улучшением процессов идентификации и нейтрализации угроз. В частности, время реакции на угрозы сократилось в среднем на 25%, что свидетельствует о высокой эффективности предложенной системы.

Заключение.

В данной статье была разработана имитационная модель системы защиты от вторжений для противодействия попыткам вторжения. Выделение ключевых подсистем и функциональных компонентов выполнено в соответствии с технической документацией. С помощью инструмента «Иерархия», интегрированного в CPN Tools, осуществляется установление взаимозависимостей между подсистемами, что позволяет привести модель в соответствие с операционными аспектами системы защиты от вторжений, используемой на объектах информатизации от вторжений. Разработанная в программной среде CPN Tools имитационная модель функционирования системы предотвращения вторжений, в отличие от существующих формальных моделей, позволяет получить вероятностно-временные характеристики, в частности, в виде времени выполнения защитных функций. Это позволяет избежать проведения вычислительного эксперимента для исследования вероятностно-временных атрибутов этих систем, которые предполагается использовать при количественной оценке эффективности программных средств и систем защиты информации в АС на объектах информатизации. Имитационная модель систем предотвращения вторжений, разработанная в программной среде CPN Tools, предназначена для использования в дальнейших исследованиях. Она послужит основой для анализа и создания моделей, направленных на смягчение различных форм угроз вторжения, направленных на информационный ресурс защищаемых систем.

ЛИТЕРАТУРА

[1] СЗИ «Страж NT». Руководство администратора. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (дата обращения: 25.05.2019).

[2] Система защиты информации от несанкционированного доступа «Страж NT». Описание применения.URL: http://www.rubinteh.ru/public/opis30.pdf (дата обращения: 25.05.2019).

[3] Попов А.Д. Модели и алгоритмы оценки эффективности систем защиты информации от несанкционированного доступа с учётом их временных характеристик в автоматизированных системах органов внутренних дел: дис канд. техн. наук. Воронеж / 2018. URL: https://ви.мвд.рф/Nauka/Dissovety/sostojavshiesja_zashhiti_dissertacij (дата обращения: 25.05.2023).

[4] Вентцель Е.С. Теория вероятностей. (accessed: 25.05.2019) Наука, 1969. – 576 с.

[5] Jensen K. and Kristensen L.M. Coloured Petri Nets Modeling and Validation of Concurrent Systems. Berlin: Springer-Verlag, 2009.

[6] Питерсон Д.Ж. Теория сетей Петри и моделирование систем: Пер. с англ. – М.: Мир, 1984. – 264 с.

[7] Котов В.Е. Сети Петри. – М.: Наука. Главная редакция физико-математической литературы, 1984. – 160 с.

[8] Дровникова И.Г ., Змеев А.А., Попов А.Д., Рогозин Е.А. Методика исследования вероятностновременных характеристик реализации сетевых атак в программной среде имитационного моделирования. Вестник Дагестанского государственного технического университета. Технические науки. 2017. 44 (4). С. 99–113. DOI: https://doi.org/10.21822/2073-6185-2017-44-4-99-113.

[9] Meedeniya D. A. Indika Perera Model based software design: Tool support for scripting in immersive environments // IEEE 8th International Conference on Industrial and Information Systems, 2013. P. 248–253.

[10] Lukaszewski R., Winiecki W. Petri Nets in Measuring Systems Design. IEEE Instrumentation and Measurement Technology Conference Proceedings, 2006. P. 1564–1569.

[11] Gehlot V., Nigro C. An introduction to systems modeling and simulation with Colored Petri Nets. 2010. P. 104– 118.

REFERENCES*

[1] SZI «Strazh NT». Rukovodstvo administratora. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (data obrashhenija: 25.05.2019).

[2] Sistema zashhity informacii ot nesankcionirovannogo dostupa «Strazh NT». Opisanie primenenija.URL: http://www.rubinteh.ru/public/opis30.pdf (data obrashhenija: 25.05.2019).

[3] Popov A.D. Modeli i algoritmy ocenki jeffektivnosti sistem zashhity informacii ot nesankcionirovannogo dostupa s uchjotom ih vremennyh harakteristik v avtomatizirovannyh sistemah organov vnutrennih del: dis kand. tehn. nauk. Voronezh / 2018. URL: https://vi.mvd.rf/Nauka/Dissovety/sostojavshiesja_zashhiti_dissertacij (data obrashhenija: 25.05.2023).

[4] Ventcel' E.S. Teorija verojatnostej. (accessed: 25.05.2019) Nauka, 1969. – 576 s.

[5] Jensen K. and Kristensen L.M. Coloured Petri Nets Modeling and Validation of Concurrent Systems. Berlin: Springer-Verlag, 2009.

[6] Piterson D.Zh. Teorija setej Petri i modelirovanie sistem: Per. s angl. – M.: Mir, 1984. – 264 s.

[7] Kotov V.E. Seti Petri. – M.: Nauka. Glavnaja redakcija fiziko-matematicheskoj literatury, 1984. – 160 s.

[8] Drovnikova I.G ., Zmeev A.A., Popov A.D., Rogozin E.A. Metodika issledovanija verojatnostnovremennyh harakteristik realizacii setevyh atak v programmnoj srede imitacionnogo modelirovanija. Vestnik Dagestanskogo gosudarstvennogo tehnicheskogo universiteta. Tehnicheskie nauki. 2017. 44 (4). S. 99–113. DOI: https://doi.org/10.21822/2073-6185-2017-44-4-99-113.

[9] Meedeniya D. A. Indika Perera Model based software design: Tool support for scripting in immersive environments // IEEE 8th International Conference on Industrial and Information Systems, 2013. P. 248–253.

[10] Lukaszewski R., Winiecki W. Petri Nets in Measuring Systems Design. IEEE Instrumentation and Measurement Technology Conference Proceedings, 2006. P. 1564–1569.

[11] Gehlot V., Nigro C. An introduction to systems modeling and simulation with Colored Petri Nets. 2010. P. 104– 118.

Аяулым Батырханова, магистрант, әль-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, ayaulymbatyrkhanova1203@gmail.com .

Ольга Усатова, PhD, ҚР ҒЖБМ ҒК Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан, olgaussatova@gmail.com

ИНФОБИЗНЕСТЕГІ АҚПАРАТТЫ ҚОРҒАУ ЖҮЙЕСІН ЗЕРТТЕУ ЖӘНЕ ӘЗІРЛЕУ

Аңдатпа. Бұл жұмыста инфобизнесте рұқсатсыз кіруге қарсы тұрудың автоматтандырылған жүйелеріндегі (АС) ақпаратты қорғау жүйелерінің (СҚА) жұмысын сипаттайтын күрделі модель ұсынылған. Бұған Имитациялық модельдеу әдістері арқылы қол жеткізіледі. Жоғарыда аталған модель кейінгі талдауды жеңілдету үшін CPN Tools бағдарламалық жасақтамасында жасалған.

Пайдаланудың қарапайымдылығын оңтайландыру, көрнекілікті арттыру және логикалық дәйектілікті қамтамасыз ету үшін біз модельді жеке ішкі жүйелерге ыдырату

үшін CPN құралдарының бірегей мүмкіндіктерін қолдандық. Бұл модельді пайдалану есептеу эксперименттерін жүргізу үшін, әсіресе рұқсат етілмеген қол жетімділіктен қорғалған кондиционерлеу жүйелерінің нақты тұтынушылық сипаттамаларын зерттеу үшін қажет. Сонымен қатар, бұл жүйелердің өнімділігін талдауға және сандық бағалауға мүмкіндік беретін бағдарламалық жасақтама пакеттерін құру үшін маңызды.

Интрузияны анықтау жүйесінің жұмысын Имитациялық модельдеу нәтижесінде алынған нәтижелер әртүрлі күй сипаттамалары арқылы көрсетілуі мүмкін. Бұл сипаттамалар жүйенің және оның жеке ішкі жүйелерінің жалпы өнімділігі туралы түсінік береді. Әзірленген Имитациялық модельді ақпараттық қауіпсіздік жүйелерін жобалау, пайдалану, сертификаттау және мерзімді тексеру кезінде пайдалануға болады. Сонымен қатар, оны ат нысандарының аутентификациясы және осы нысандар пайдаланатын ақпараттық қауіпсіздік бағдарламалық құралын бағалау үшін пайдалануға болады. CPN Tools қолданатын meta бағдарламалау тілі маркердің бастапқы күйінен аралық күйлер арқылы соңғы күйге, соның ішінде уақыттың кешігуіне және басқа функцияларға ықтималдық қозғалысын басқаруға мүмкіндік береді.

Түйінді сөздер. CPN Too, meta бағдарламалау тілі, ақпаратты қорғау жүйесі, инфобизнес, Ақпараттық жүйелер.

Ayaulym Batyrkhanova, master's student, Al-Farabi Kazakh National University, Almaty, Kazakhstan, ayaulymbatyrkhanova1203@gmail.com
Olga Ussatova, PhD, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, olgaussatova@gmail.com

RESEARCH AND DEVELOPMENT, INFORMATION PROTECTION SYSTEM IN INFOBUSINESSES

Abstract. This paper presents a complex model describing the operation of information protection systems (IPS) in automated systems (AS) of countering unauthorized access in infobusiness. This is achieved by using simulation modeling techniques. The above model was developed in the CPN Tools software environment to facilitate subsequent analysis.

To optimize usability, increase visibility, and ensure logical consistency, we used the unique features of CPN Tools to decompose the model into individual subsystems. The use of this model is essential for computational experiments, especially for investigating the real-world consumer performance of tamper-proof air-conditioning systems. It is also important for creating software packages that allow analyzing and quantifying the performance of these systems.

The results obtained from the simulation of intrusion detection system performance can be expressed through various state characteristics. These characteristics provide insight into the overall performance of the system and its individual subsystems. The developed simulation model can be used in the design, operation, certification and periodic verification of information security systems. In addition, it can be used for authentication of IT objects and evaluation of information security software used by these objects. The Meta programming language used by CPN Tools allows controlling the probabilistic movement of a token from its initial state through intermediate states to its final state, including time delays and other features.

Keywords. CPN Too, Meta programming language, information protection system, infobusiness, information systems.

****