УДК: 004.942
DOI: 10.26102/2310-6018/2021.35.4.010

Моделирование процессов функционирования автоматизированных систем при проведении мероприятий по оценке защищенности

И.Д. Королев, Д.И. Маркин, Е.С. Литвинов

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко Министерство обороны Российской Федерации, Краснодар, Российская Федерация

Резюме. Актуальность исследования обусловлена необходимостью минимизации негативного влияния на целостность и конфиденциальность данных, обрабатываемых автоматизированной системой, а также на состояние компонентов системы в ходе осуществления тестирования на проникновение в рамках мероприятия контроля защищенности. В связи с этим данная статья направлена на выявление методики создания и применения виртуальных макетов систем для их последующего использования в рамках тестирования. Ведущим подходом к исследованию данной проблемы является моделирование реальных процессов функционирования пользователей системы, злоумышленников и должностных лиц, ответственных за обеспечение безопасности информации, обрабатываемой в системе на основе теории массового обслуживания, позволяющее комплексно рассмотреть функционирование автоматизированных систем в терминах обработки пользовательских запросов и запросов злоумышленника. В статье представлена абстрактная модель функционирования автоматизированных систем, позволяющая осуществить оценку защищенности системы за счет анализа значений вероятности обработки системой запросов пользователей на доступ к информационным ресурсам и запросов злоумышленников, направленных на нарушение конфиденциальности, целостности и доступности компонентов системы и обрабатываемых информационных ресурсов. Материалы статьи представляют практическую ценность для создания виртуального стенда для тестирования на проникновение, имитирующего функционирование автоматизированной системы и позволяющего минимизировать влияние на реальную систему.

***Ключевые слова*:** обеспечение безопасности информации, автоматизированная система, система защиты информации, контроль защищенности информации, активная проверка, система массового обслуживания, эмуляция.

Для цитирования: Королев И.Д., Маркин Д.И., Литвинов Е.С. Моделирование процессов функционирования автоматизированных систем. *Моделирование, оптимизация и информационные технологии.* 2021;9(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1001
DOI: 10.26102/2310-6018/2021.35.4.010

Modeling of automated system's functioning processes during security assessment activities

I.D. Korolev, D.I. Markin, E.S. Litvinov

Krasnodar higher military orders of Zhukov and the October Revolution Red banner school named after general of the army S.M. Shtemenko Ministry of Defense, Krasnodar, Russian Federation

Abstract: The study is relevant due to the need for minimization of the negative impact on the integrity and confidentiality of data processed by the automated system, as well as on the state of the system

components during penetration testing as part of the security control measure. In this regard, this article is aimed to identify methods for creating and using virtual system layouts for their subsequent use in testing. The leading research approach is the modeling of real-world processes of system users functioning: malicious users, officials, responsible for ensuring the security of information processed in the system based on the queuing theory, which makes it possible to comprehensively consider the functioning of automated systems in terms of processing user and attacker requests. The article presents an abstract model of the automated systems functioning. It makes it possible to assess the system security by analyzing the values of the probability that the system will process user requests for access to information resources and inquiry from intruders aimed at violating the confidentiality, integrity, and availability of system components and processed information resources. The article materials are of practical value for creating a virtual test bench for penetration testing, simulating the functioning of an automated circuit, and minimizing the impact on a real system.

Keywords: information security, automated system, information security system, information security control, active security check, queuing system, emulation.

For citation: Korolev I.D., Markin D.I., Litvinov E.S. Modeling of automated system's functioning processes. *Modeling, Optimization and Information Technology*. 2021;9(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=1001 DOI: 10.26102/2310-6018/2021.35.4.010 (In Russ).

Введение

Актуальность проблемы обеспечения безопасности информации при ее автоматизированной обработке, передаче и хранении в настоящее время неоспорима, поскольку, с одной стороны, наблюдается непрерывный рост сферы применения автоматизированных систем, комплексов средств автоматизации и информационных систем в тех или иных отраслях деятельности коммерческих и государственных структур, а с другой – возрастает количество, разнообразие и сложность компьютерных атак, направленных на нарушение свойств безопасности информации, обрабатываемой в подобных системах.

Особое внимание при этом стоит уделить объектам критической информационной инфраструктуры [1], автоматизированным системам, осуществляющим обработку сведений, составляющих государственную тайну [2], а также информационным системам персональных данных. Нарушение функционирования подобных объектов и безопасности обрабатываемой в них информации ведет к наиболее значительным последствиям как для отдельных граждан, так и для определенных коммерческих и государственных структур и государства в целом.

Наиболее уязвимыми компонентами и информационных [2], и автоматизированных [3] систем являются программные и аппаратные компоненты, содержащие уязвимости, то есть ошибки, допущенные при их проектировании, разработке и конфигурации, обусловливающие возможность реализации угроз безопасности обрабатываемой соответствующей системы[2].

В качестве иллюстрации роста компьютерных угроз целесообразно привести статистику IV квартала 2020 года, собранную организацией Positive Technology [4]. Согласно статистическим данным, наблюдается тенденция к увеличению доли хакинга в атаках на организации: 8 из 10 атак в IV квартале носили целенаправленный характер, около 40 % всех выявленных за указанный период компьютерных атак, направлены на предприятия промышленности, государственные и медицинские учреждения.

Для снижения риска реализации угроз безопасности информации осуществляются мероприятия по защите информации различных типов. Например, согласно [1], при контроле в целях проверки соблюдения субъектами критической информационной инфраструктуры требований законодательства осуществляются

проверки, подразумевающих как изучение руководящих документов, разработанных в рамках реализации организационных мер обеспечения безопасности информации, так и анализ совокупности аппаратных и программных средств вычислительной техники на предмет наличия в них уязвимостей, а согласно [5], одним из этапов создания системы защиты информации, обрабатываемой в автоматизированной системе, проводимых до ввода соответствующего объекта в эксплуатацию, является аттестация системы защиты на соответствие требованиям безопасности информации, содержащая оценку соответствия системы ЗИ требованиям безопасности информации в реальных условиях эксплуатации путем анализа организационных и технических мер защиты информации.

Мероприятия, проводимые в рамках оценки технических мер защиты информации, подразумевают под собой, в том числе, процесс выявления уязвимостей компонентов системы, который, согласно [6], строится посредством выполнения пассивных и активных проверок наличия уязвимостей. Пассивная проверка осуществляется путем сбора специализированными программными и аппаратными средствами определенных параметров системы с минимальным влиянием на проверяемую систему и их сравнения с эталонными значениями.

Наиболее существенным недостатком пассивной проверки является тот факт, что проверка не учитывает комплексный характер поведения злоумышленника и не охватывает весь спектр непрерывно обновляющихся специализированных средств, техник и методов проведения компьютерных атак. Для повышения достоверности проверок и учета вышеописанного поведения злоумышленника проводятся активные проверки (тестирование на проникновение), заключающиеся в моделировании действий потенциального нарушителя и анализе последствий реализованных атак по отношению к системе.

Основным недостатком активной проверки является степень ее влияния на проверяемую систему: в ходе проверки высока вероятность вывода компонентов системы из строя или компрометации обрабатываемой в системе информации. Как правило, данную вероятность снижают за счет вывода системы из эксплуатации на момент проверки, однако при этом снижается точность, поскольку при выводе из эксплуатации невозможно протестировать атаки, основанные на отслеживании действий пользователей системы и генерируемого ими трафика.

Главной целью проводимого исследования процессов оценки защищенности автоматизированных систем является снижение вероятного негативного влияния на функционирование системы при уровне точности оценки, достигаемом путем активных проверок. В качестве задачи исследования, соответственно, выступает разработка подхода к процессу оценки защищенности, позволяющего повысить его точность за счет тестирования на проникновение без негативного влияния на систему.

Материалы и методы

Одним из решений данного противоречия, позволяющим снизить степень влияния на систему при ее проверке, является проведение экспериментального исследования проверяемой системы, а именно эмуляцию, при которой реальный процесс выполняется в модели вычислительной среды, то есть для работы реального процесса создаются синтетические условия [7].

В рамках данной работы построение модели функционирования автоматизированной системы реализовано на основе теории систем массового обслуживания, поскольку этот математический аппарат позволяет описать временные и вероятностные характеристики процессов обмена и обработки информации с учетом осуществления различных видов атак. В качестве основы модели выступает

одноканальная система массового обслуживания с отказами. В общем случае подобная система состоит из входящего простейшего потока заявок, очереди заявок, канала обслуживания и исходящего потока заявок. Обработка заявок осуществляется в порядке их помещения в очередь. Если при поступлении заявки очередь полна – заявка отбрасывается. Оценка функционирования системы при этом строится на анализе относительной пропускной способности системы, то есть отношения среднего числа заявок, которое может обслужить система за единицу времени, к среднему числу заявок, поступивших в систему за это время. Данное соотношение выражается следующим образом [8]:

$$q = \frac{\lambda'}{\lambda}, \quad (1)$$

где:

q – относительная пропускная способность;

λ' – интенсивность входящего потока заявок, то есть среднее число заявок, поступающих на вход системы в единицу времени;

λ – интенсивность исходящего потока заявок, то есть среднее число заявок, обрабатываемых системой в единицу времени.

Поскольку вероятность обработки входящей заявки, согласно [9], есть отношение количества обслуженных требований к количеству поступивших требований, то возможно выразить относительную пропускную способность системы через вероятность того, что заявка будет обслужена, то есть:

$$q = \frac{\lambda'}{\lambda} = \frac{\lambda' \times T}{\lambda \times T} = \frac{N_s}{N} = P_{serv}, \quad (2)$$

где:

T – общее время работы системы;

N_s – общее количество обработанных заявок;

N – общее количество поступивших заявок;

P_{serv} – вероятность обработки входящей заявки.

Соответственно, определив вероятность обслуживания заявки в рассматриваемой системе, можно сделать вывод о состоянии ее функционирования.

Структура модели автоматизированной системы на основе системы массового обслуживания представлена на Рисунке 1 и содержит следующие компоненты:

1. Пользователь. Источник санкционированных заявок, обрабатываемых системой. Имитирует действия пользователей автоматизированной системы.

2. Нарушитель. Совокупность источников несанкционированных заявок, направленных на нарушение конфиденциальности, целостности и доступности информации, обрабатываемой в системе. Позволяет описать и оценить степень воздействия злоумышленника на свойства безопасности информации.

3. Автоматизированная система (АС). Последовательность очередей заявок и каналов обслуживания, соответствующих определенным компонентам автоматизированной системы.

4. Блок оценки защищенности. Предназначен для оценки защищенности и состояния функционирования системы за счет анализа интенсивностей потока обработанных заявок пользователя и потока обработанных заявок нарушителя.

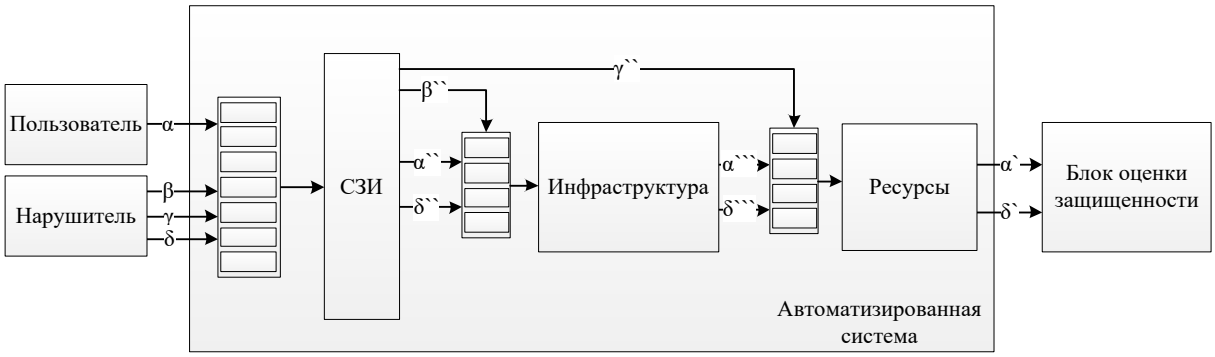

Рисунок 1 – Структура модели автоматизированной системы
Figure 1 – Structure of automated system model

Блок «Автоматизированная система», в свою очередь, состоит из блоков «СЗИ» (система защиты информации), «Инфраструктура» и «Ресурсы», а также очередей заявок перед каждым блоком.

Блок «СЗИ» представляет собой канал обслуживания, который на основании внутренних проверок либо обрабатывает поступившую заявку, приняв ее за санкционированную, либо блокирует ее в противном случае. Более подробно функционирование данного блока описано ниже.

Блок «Инфраструктура» может быть интерпретирован как совокупность программных и аппаратных компонентов автоматизированной системы ω_i (средств вычислительной техники, сетевого оборудования и установленного на них программного обеспечения), необходимых для корректной обработки всех пользовательских заявок. Представим данную совокупность компонентов следующим образом:

$$I = \{\omega_1, \omega_2, ..., \omega_v\} \quad (3)$$

Соответственно, совокупность компонентов, необходимая для обработки заявки x, выражается следующим образом:

$$I(x) = \{\omega_i \in I \,|\, \omega_i \text{ необходим для обработки } x\}, I(x) \subseteq I \quad (4)$$

Обработка заявки в блоке «Инфраструктура» представляет собой процесс передачи заявки x, обработанной блоком «СЗИ», к месту хранения информационных ресурсов с помощью аппаратных и программных компонентов автоматизированной системы.

Блок «Ресурсы» представляет собой совокупность информационных ресурсов ψ_j, запрос, на доступ к которым осуществляет пользователь путем формирования заявок. Представим данную совокупность следующим образом:

$$R = \{\psi_1, \psi_2, ..., \psi_w\} \quad (5)$$

Аналогично, совокупность информационных ресурсов, к которым осуществляется доступ в ходе обработки заявки, выражается следующим образом:

$$R(x) = \{\psi_j \in R \,|\, \psi_j \text{ необходим для обработки } x\}, R(x) \subseteq R \quad (6)$$

Обработка заявки в блоке «Ресурсы» осуществляется аналогично блоку «Инфраструктура»: в случае, если целостность информационных ресурсов не нарушена, интенсивность выходного потока заявок не изменяется.

Пусть максимальный объем очередей блоков «СЗИ», «Инфраструктура» и «Ресурсы» составляет τ, σ и μ элементов соответственно. Каждая заявка обладает

временной меткой $t(x)$, определяемой временем, прошедшим от начала функционирования модели до генерации запроса x. Таким образом, количество заявок, находящихся в очереди к каждому из блоков в момент времени $t(x)$, возможно задать как $\tau(t(x)), \sigma(t(x))$ и $\mu(t(x))$ соответственно.

Для повышения наглядности дальнейших вычислений введем следующие временные показатели:

$t_1(x)$ – временная метка генерации x и поступления заявки на вход блока «СЗИ»;

$t_2(x)$ – временная метка поступления x на вход блока «Инфраструктура»

$$t_2(x) = t_1(x) + t_{def} \times (\tau(t_1(x)) + 1), \quad (7)$$

где

t_{def} – время обработки запроса блоком «СЗИ»;

$t_3(x)$ – временная метка поступления запроса x на вход блока «Ресурсы»

$$t_3(x) = t_2(x) + t_{it} \times (\sigma(t_2(x)) + 1), \quad (8)$$

где t_{it} – время обработки запроса блоком «Ресурсы».

В случае если заявка – санкционированная либо направлена на нарушение конфиденциальности информации, она обрабатывается по вышеописанному алгоритму, вероятность ее обработки зависит от заполненности очередей и состояния функционирования соответствующих блоков.

Заявка, направленная на нарушение доступности информации, при попадании в блок «Инфраструктура» выводит его из строя на определенное время, необходимое для восстановления (замены) соответствующего компонента.

При обработке блоком «Ресурсы» заявки, направленной на нарушение целостности, осуществляется изменение (модификация) соответствующих ресурсов, что приводит к снижению вероятности обработки заявок пользователя.

Целесообразно подробнее рассмотреть разновидности потоков входящих заявок, в рамках моделирования процессов функционирования автоматизированной системы подразделяющиеся на:

1. Поток заявок пользователя α на доступ к ресурсам АС.
2. Поток заявок β на нарушение доступности информационных ресурсов АС.
3. Поток заявок γ на нарушение целостности информационных ресурсов АС.
4. Поток заявок нарушителя δ на доступ к ресурсам АС.

Поток заявок пользователя на доступ к ресурсам рассматривается как поток повторяющихся процедур, осуществляемых пользователем с помощью компонентов АС, с целью выполнения поставленной задачи. В случае если автоматизированная система работает в штатном режиме – интенсивность потока заявок α не превышает потока выполненных (корректно обработанных) автоматизированной системой заявок α'. Совокупность всех видов санкционированных заявок представима в следующем виде:

$$\mathrm{A} = \{\alpha_1, \alpha_2, ..., \alpha_q\} \quad (9)$$

Под заявкой на нарушение доступности компонентов АС будем понимать последовательность действий нарушителя, приводящую к нарушению доступности ресурсов АС за счет нарушения функционирования компонентов АС. Примером подобной заявки может выступать отправка нарушителем специфически сконфигурированного сетевого пакета, при получении которого сервер, входящий в

состав АС и хранящий информационные ресурсы, выходит из строя и перестает функционировать. Совокупность всех видов заявок на нарушение доступности представима в следующем виде:

$$\mathrm{B} = \{\beta_1, \beta_2, ..., \beta_g\} \quad (10)$$

В качестве заявки на нарушение целостности информационных ресурсов рассматривается последовательность действий нарушителя, подразумевающая несанкционированный доступ к информационным ресурсам, а также их изменение. В качестве примера заявки на нарушение целостности может выступать подмена (модификация) информационных ресурсов, к которым имеет доступ конкретный пользователь. Совокупность всех видов заявок на нарушение целостности представима в виде следующего множества:

$$\Gamma = \{\gamma_1, \gamma_2, ..., \gamma_h\} \quad (11)$$

Несанкционированные заявки нарушителя на доступ к ресурсам автоматизированной системы представляют собой последовательности действий нарушителя, не влияющие на функционирование системы и целостность ресурсов, однако приводящие к получению несанкционированного доступа нарушителя к информационным ресурсам системы. Совокупность всех видов заявок на нарушение доступности представима в следующем виде:

$$\Delta = \{\delta_1, \delta_2, ..., \delta_u\} \quad (12)$$

Защищенность системы в данном случае оценивается через способность системы корректно обрабатывать пользовательские заявки и блокировать заявки злоумышленника, что с учетом (2) можно выразить следующим образом:

$$S(x, y) = k_c \times P_{serv}(x) + 1 - k_a \times P_{serv}(y),\ S(x, y) \in [0, 2], \quad (13)$$

где:

$P_{serv}(x)$ – вероятность обработки санкционированной заявки;

$P_{serv}(y)$ – вероятность обработки несанкционированной заявки на доступ;

k_c и k_a – задаваемые вручную показатели, определяющие, какой вид угроз наиболее критичен для моделируемой системы, $0,5 \le k_c, k_a \le 1$. В случае, если для системы более критично нарушение конфиденциальности, задают $k_c < k_a$. В этом случае показатель защищенности при нарушении конфиденциальности $(P_{serv}(y) \to 1)$ оказывается выше аналогичного показателя при нарушении целостности и доступности $(P_{serv}(x) \to 0)$.

Рассмотрим подробнее общую вероятность обработки входящей заявки x каналом обслуживания «АС» $P_{serv}(x)$. Поскольку заявка будет обработана всей системой только в случае обработки заявки каждым из вышеперечисленных блоков, то:

$$P_{serv}(x) = P_{serv}^{def}(x) \times P_{serv}^{it}(x) \times P_{serv}^{res}(x), \quad (14)$$

где:

$P_{serv}^{def}(x)$ – вероятность обработки входящей заявки x блоком «СЗИ»;

$P_{serv}^{it}(x)$ – вероятность обработки входящей заявки x блоком «Инфраструктура»;

$P_{serv}^{res}(x)$ – вероятность обработки входящей заявки x блоком «Ресурсы».

Заявка x будет обработана блоком «СЗИ» в случае, если в момент подачи заявки на вход соответствующая очередь заявок не будет полна, а также если система защиты распознает заявку как санкционированную, то есть вероятность обработки заявки x в блоке СЗИ может быть представлена следующим образом:

$$P_{serv}^{def}(x) = \left(1 - P_{\tau}\left(t(x)\right)\right) \times P_{rec}^{k}(x), \tag{15}$$

где:

$P_{\tau}\left(t(x)\right)$ – вероятность того, что в момент времени $t(x)$ очередь блока «СЗИ» полна, то есть количество заявок, находящихся в очереди блока «СЗИ», достигнет максимального значения;

$P_{rec}^{k}(x)$ – показатель распознавания заявки как санкционированной, представимый в виде:

$$P_{rec}^{k}(x) = \begin{cases} 1, \text{при } P_{\alpha}(x) \geq k, \\ 0, \text{при } P_{\alpha}(x) < k; \end{cases} \tag{16}$$

$P_{\alpha}(x)$ – вероятность того, что заявка x является санкционированной;

k – коэффициент распознавания санкционированных заявок, $0 \leq k \leq 1$.

Значение k задается в зависимости от выбора СЗИ и корректности конфигурации отдельных средств защиты. Корректно сконфигурированные средства защиты информации блокируют все виды несанкционированных заявок, однако существует вероятность как ложноположительных, так и ложноотрицательных срабатываний: ситуаций, в которых система защиты информации пропускает несанкционированные заявки либо блокирует санкционированные заявки. В рамках построения модели целесообразно обусловливать подобные ситуации корректностью выбора коэффициента k, а также соответствующих ему значений границ ложноположительных и ложноотрицательных срабатываний a и b соответственно.

Заявка x будет обработана блоком «Инфраструктура» в том случае, если в момент подачи заявки на вход соответствующая очередь заявок не будет полна, а также, если доступность всех компонентов, необходимых для обработки заявки x, не нарушена. Поскольку данные события являются независимыми, то, согласно [10], вероятность обработки запроса блоком «Инфраструктура» выражается следующим образом:

$$P_{serv}^{it}(x) = \left(1 - P_{\sigma}\left(t_2(x)\right)\right) \times P_{online}^{it}\left(t_2(x)\right) \tag{17}$$

где:

$P_{\sigma}\left(t_2(x)\right)$ – вероятность того, что на момент поступления x на вход блока «Инфраструктура» соответствующая очередь заявок будет полна;

$P_{online}^{it}\left(t_2(x)\right)$ – вероятность того, что на момент поступления x на вход блока «Инфраструктура» его доступность не нарушена.

В свою очередь, доступность блока «Инфраструктура» не будет нарушена, если в соответствующий момент времени не будет нарушена доступность тех его компонентов, которые необходимы для обработки соответствующей заявки, то есть:

$$P_{online}^{it}\left(t(x)\right) = \prod_{i=1}^{v}\left(P_{online}^{\omega_i}\left(t(x)\right)\right)^{m_{\omega_i}}, \tag{18}$$

где

$P_{online}^{it}\left(t\left(x\right)\right)$ – вероятность того, что в момент $t\left(x\right)$ не нарушена доступность компонента $\omega_i \in I$;

m_{ω_i} – коэффициент принадлежности компонента ω_i к обработке заявки x,

$$m_{\omega_i} = \begin{cases} 1, \text{если } \omega_i \in I\left(x\right), \\ 0, \text{если } \omega_i \notin I\left(x\right). \end{cases} \quad (19)$$

Доступность компонента $\omega_i \in I$ не будет нарушена в том случае, если не поступит ни одной заявки $\beta_j \in \mathrm{B}$, удовлетворяющей следующим условиям:

1. Заявка $\beta_j \in \mathrm{B}$ возникнет в такой момент времени, что при поступлении заявки x на вход блока «Инфраструктура» и ее обработке компонент ω_i будет выведен из строя и не восстановлен.
2. На момент поступления β_j на вход блока «СЗИ» соответствующая очередь не будет полна.
3. Вероятность распознавания β_j превышает значение коэффициента k.
4. На момент поступления β_j на вход блока «Инфраструктура» соответствующая очередь не будет полна.
5. Заявка β_j выводит из строя компонент ω_i с некоторой вероятностью.

Компонент системы не сможет обработать заявку x, если на временном промежутке длины t_{it} на вход блока «Инфраструктура» поступила заявка на нарушение доступности компонента ω_i. Поскольку потоки заявок, рассматриваемых в рамках данной работы, являются стационарными, то вероятность возникновения заявки во временном промежутке $\left[a,b\right]$ зависит только от его длины.

Поскольку в рамках разработки модели рассматриваются простейшие потоки заявок, то, согласно [8], вероятность того, что на временном отрезке T будет сгенерировано ровно k заявок из простейшего потока с интенсивностью β, выражается формулой Пуассона:

$$P_k = \frac{\left(\beta T\right)^k}{k!} e^{-\beta T}, k = 0,1,\ldots \quad (20)$$

Заявки генерируются с равной вероятностью, то есть вероятность выбора заявки на нарушение доступности вида β_j может быть выражена как $\frac{1}{g}$.

Таким образом, вероятность того, что на временном промежутке длины t_{it} возникнет конкретная заявка $\beta_j \in \mathrm{B}$, направленная на нарушение доступности компонента ω_i, с учетом $k = 1$ принимает вид:

$$p_{it}\left(\beta_j\right) = \frac{1}{g} \beta t_{it} e^{-\beta t_{it}} \quad (21)$$

На основании вышеизложенного, вероятность того, что компонент ω_i доступен в момент времени $t\left(x\right)$ можно представить в виде:

$$P_{online}^{\omega_i}\left(t\left(x\right)\right)=\prod_{i=1}^{g}\left(1-p_{it}\left(\beta_j\right)\times P_{serv}^{def}\left(\beta_j\right)\times\left(1-P_{\sigma}\left(t_2\left(\beta_j\right)\right)\right)\times P_{dos}^{\omega_i}\left(\beta_j\right)\right) \quad (22)$$

где $P_{dos}^{\omega_i}\left(\beta_j\right)$ – вероятность того, что заявка β_j выведет из строя компонент ω_i.

Соответственно, вероятность обработки заявки x блоком «Инфраструктура» выражается следующим образом:

$$P_{serv}^{it}\left(x\right)=\left(1-P_{\sigma}\left(t_2\left(x\right)\right)\right)\times$$

$$\times\prod_{i=1}^{v}\left(\prod_{j=1}^{g}\left(1-p_{it}\left(\beta_j\right)\times P_{serv}^{def}\left(\beta_j\right)\times\left(1-P_{\sigma}\left(t_2\left(\beta_j\right)\right)\right)\times P_{dos}^{\omega_i}\left(\beta_j\right)\right)\right)^{m_{\omega_i}} \quad (23)$$

Аналогично выведем вероятность обработки заявки x блоком «Ресурсы»:

$$P_{serv}^{res}\left(x\right)=\left(1-P_{\mu}\left(t_3\left(x\right)\right)\right)\times$$

$$\times\prod_{l=1}^{w}\left(\prod_{r=1}^{h}\left(1-p_{res}\left(\gamma_r\right)\times P_{serv}^{def}\left(\gamma_r\right)\times P_{serv}^{it}\left(\gamma_r\right)\times\left(1-P_{\mu}\left(t_3\left(\gamma_r\right)\right)\right)\times P_{\text{int}}^{\psi_l}\left(\gamma_r\right)\right)\right)^{n_{\psi l}} \quad (24)$$

где:

$p_{res}\left(\gamma_r\right)$ – вероятность генерации γ_r во временном промежутке длины t_{res};

$P_{\mu}\left(t\left(x\right)\right)$ – вероятность того, что в момент времени $t\left(x\right)$ очередь блока «Ресурсы» будет полна;

$P_{int}^{\psi_l}\left(\gamma_r\right)$ – вероятность того, что заявка γ_r нарушит целостность информационного ресурса ψ_l,

n_{ψ_l} – коэффициент принадлежности ресурса ψ_l к обработке заявки x:

$$n_{\psi_l}=\begin{cases}1, \text{если}\ \psi_l\in R\left(x\right),\\ 0, \text{если}\ \psi_l\notin R\left(x\right).\end{cases} \quad (25)$$

Результаты

В результате исследования создана теоретическая модель, позволяющая сопоставить функционирование автоматизированной системы с обработкой заявок одноканальной системой массового обслуживания с отказами и ограниченной очередью. Эффект от действий злоумышленника представлен в виде снижения интенсивности обработки заявок пользователей и повышения интенсивности обработки заявок на нарушение доступа. Функционирование системы защиты в данной модели представлено в виде условного оператора, отбрасывающего или пропускающего заявки в соответствии с коэффициентом распознавания k, абстрактно описывающим корректность и эффективность средств защиты. Объединив формулы 14, 15, 22 и 23, возможно аналитически описать вероятность обработки заявки с учетом функционирования средств защиты и действий злоумышленника, а при раскрытии формулы 13 за счет описания вероятностных показателей обработки заявок $P_{serv}\left(x\right), P_{serv}\left(y\right)$ формируется общая формула, позволяющая оценить защищенность системы, с точки зрения ее способности обеспечивать поставленные задачи, блокировать те или иные действия злоумышленника и осуществлять восстановление поврежденных компонентов.

Заключение

В рамках данной работы рассмотрена модель функционирования автоматизированной системы, в основе которой лежит система массового обслуживания. Модель позволяет оценивать защищенность информации с учетом как злоумышленника, так и защищающегося, интерпретируя функционирование системы и действия злоумышленника как заявки, поступающие на вход системы массового обслуживания и подлежащие обработке.

Дальнейшие исследования, посвященные вопросам повышения точности контроля защищенности автоматизированной системы при снижении риска нарушения ее функционирования, могут быть посвящены как конкретизации вышеописанной модели и разработке конкретных методик и алгоритмов создания и оперативного развертывания программных и аппаратно-программных комплексов, воссоздающих инфраструктуру и процессы функционирования контролируемой системы, так и внедрению в существующую модель математического аппарата, позволяющего наиболее точно сымитировать поведение потенциального нарушителя информационной безопасности

СПИСОК ИСТОЧНИКОВ

1. Федеральный закон РФ от 26.07.2017 № 187-ФЗ «О безопасности критической инфраструктуры Российской Федерации». 2017.
2. Указ президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». 2016.
3. Защита информации. Основные термины и определения: ГОСТ Р 50922-20061, 2008.
4. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения: ГОСТ 34.003-90. 1992.
5. Актуальные киберугрозы: IV квартал 2020 года. *Positive technology*. Доступно по: https://ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q4/ (дата обращения: 25.04.2021).
6. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: ГОСТ Р 51583-2014, 2014.
7. Коноваленко С.А., Королев И.Д. Выявление уязвимостей информационных систем. *Инновации в науке*. 2016;9(58):12-20.
8. Порохненко Ю.С., Полежаев П.Н. Сравнительный анализ эмуляторов компьютерных сетей. *Университетский комплекс как региональный центр образования, науки и культуры.* 2017;3(18):3194-3199.
9. Самаров К.Л. *Математика. Учебно-методическое пособие по разделу «Элементы теории массового обслуживания»*. Новосибирск: ООО «Резольвента»; 2009. 19 с.
10. Томашевский В.Н., Жданова Е.Г. *Имитационное моделирование в среде GPSS*. М.: Бестселлер; 2003. 219 с.
11. Гмурман В.Е. *Теория вероятностей и математическая статистика*. М.: «Высшая школа»; 2003. 479 с.

REFERENCES

1. The Federal Law of July 27, 2017 No. 187-FZ On the Safety of Critical Information infrastructure of Russian Federation. 2017. (In Russ.)
2. Decree of the President of the Russian Federation of December 5, 2016 No.646 On the approval of the Doctrine of information security of the Russian Federation. 2016. (In Russ.)

3. Protection of information. Basic terms and definitions: GOST R 50922-20061. 2008. (In Russ.)
4. Information technology. Set of standards for automated systems. Automated systems. Terms and definitions: GOST 34.003-90, 1992. (In Russ.)
5. *Cybersecurity Threatscape* 2020 Q4. Available from: https://ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q4/ (date of access: 25.04.2021). (In Russ.)
6. Information protection. Sequence of protected operational system formation. General provisions: GOST R 51583-2014, 2014. (In Russ.)
7. Konovalenko S.A., Korolev I.D. Information system's vulnerabilies detection. *Innovation in science*. 2016;9(58):12-20. (In Russ.)
8. Porokhnenko Y.S., Polezhaev P.N. Comparative analysis of computer network emulators. *The university complex as a regional center of education, science and culture*. 2017;3(18):3194-3199. (In Russ.)
9. Samarov K.L. *Study guide for the section «Elements of queuing theory»*. Novosibirsk: OOO «Rezolventa»; 2009. 19 p. (In Russ.)
10. Tomashevsky V.N., Zhdanova E.G. *Simulation in the GPSS environment*. M.: «Bestseller»; 2003. 219 p. (In Russ.)
11. Gmurman V.E., *Theory of Probability and Mathematical Statistics*. M.: «Vyshhaya shkola»; 2003. 479 p. (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Королёв Игорь Дмитриевич, доктор технических наук, профессор Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища им. С.М. Штеменко, Краснодар, Российская Федерация
e-mail: *pi_korolev@mail.ru*
ORCID: 0000-0003-3102-4323

Korolev Igor Dmitrievich, doctor of technical sciences, professor of Krasnodar Higher Military School, Krasnodar, Russian Federation

Маркин Денис Игоревич, адъюнкт Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища им. С.М. Штеменко, Краснодар, Российская Федерация
e-mail: *denismark94@gmail.com*
ORCID:0000-0002-1616-7329

Markin Denis Igorevich, post-graduate student of Krasnodar Higher Military School, Krasnodar, Russian Federation

Литвинов Евгений Сергеевич, адъюнкт Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища им. С.М. Штеменко, Краснодар, Российская Федерация
e-mail: *litvinoves@rambler.ru*
ORCID:0000-0009-1146-7370

Litvinov Evgeny Sergeevich, post-graduate student of Krasnodar Higher Military School, Krasnodar, Russian Federation

Статья поступила в редакцию 11.06.2021; одобрена после рецензирования 05.10.2021; принята к публикации 21.10.2021.

The article was submitted 11.06.2021; approved after reviewing 05.10.2021; accepted for publication 21.10.2021.