АНАЛИТИЧЕСКАЯ ОЦЕНКА ОПЕРАЦИОННЫХ ХАРАКТЕРИСТИК СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

И.А. Хвостов, *канд. техн. наук*
В.В. Денисенко, *старший преподаватель*
К.С. Евтеева, *магистр*
М.А. Зайцева, *магистр*
А.А. Скрыпников, *бакалавр*
Воронежский государственный университет инженерных технологий
(Россия, г. Воронеж)

DOI:10.24411/2500-1000-2019-11533

Аннотация. *Статья описывает проблему оценки операционных характеристик системы защиты информации. В процессе работы администратор безопасности автоматизированной системы (АС) выполняет операции по эксплуатации системы защиты информации (СЗИ). При этом в основе взаимодействия «человек – машина» лежит интерфейс программы защиты. Важнейшей характеристикой СЗИ для ее основного пользователя - администратора безопасности является «удобством использования». Данный показатель оцениваться вероятностными, временными и операционными показателями.*

Ключевые слова: *защита информации, автоматизированная система, система защиты информации, несанкционированный доступ, информационная безопасность, ФСТЭК России.*

В процессе обеспечения безопасности информации (БИ) одним из важнейших мероприятий является установка и настройка систем защиты информации (СЗИ). Установившейся практикой применения СЗИ является их использование в виде отдельной программной системы, разрабатываемой отдельно от АС, и ее добавление в состав общесистемного программного обеспечения на этапе технической реализации защищаемой системы. Использование СЗИ решает проблему обеспечения БИ, но также приводит к ряду негативных последствий [1]. Наряду со снижением общего уровня надежности АС, дополнительного использования памяти и производительности на выполнение защитных функций, возникает необходимость взаимодействия пользователей АС с СЗИ, приводящая к снижению характеристики качества «удобство использования».

Проведенный анализ работы СЗИ позволяет сделать вывод о наличии двух категорий пользователей: администратор безопасности и пользователь. Пользователь при взаимодействии с СЗИ, введя идентификационную и аутентификационную информацию, использует основные функции защиты в незаметном для себя прозрачном режиме. Роль администратора безопасности – установка, настройка и эксплуатация системы защиты [2, 3]. И, следовательно, администратор безопасности решающее и управляющее звено системы, существенно влияющее на эффективность защиты. Учет эргатических процессов администрирования позволяет обеспечить адекватность настроек СЗИ текущим требованиям политики безопасности, обеспечить отсутствие ошибок в работе администратора и пользователей, а также позволяет прогнозировать качество работы системы с достаточной степенью точности.

Главной сложностью при анализе эргатических процессов является выбор показателей, характеризующих возможности и способности человека при администрировании СЗИ. Конструирование показателя, характеризующего качество администрирования СЗИ, с одной стороны, учитывающего способности индивидуума, а с другой стороны, учитывающего статистику поступления заявок на выполнение

стандартных функций администрирования, является сложной научной задачей. Эрготехнические процессы обычно характеризуются следующими показателями: вероятностными, временными и операционными [4]. Первый вид показателей: вероятность выполнения операции в данный момент, занятость администратора в данный момент, наличие очереди. Второй вид показателей: среднее время занятости администратора, полная загруженность оператора, выполнение типовой операции, пребывание операции в очереди. Операционные показатели: среднее число выполненных операций, операций выполняемых одновременно, операций, выполняемых в очереди.

При решении вопросов организации работы СЗИ в составе АС различного назначения наиболее важными являются операционные показатели системы защиты как основы для формирования организационной структуры подразделения ответственного за защиту информации, «Плана мероприятий по защите информации», «Плана внутренних проверок» и др.

Опыт эксплуатации СЗИ, а также анализ руководящих документов [1-7], позволяет выделить следующие типовые операции, выполняемые администратором:

1. Настройка системы (задание субъектов и объектов доступа, задание правил аутентификации пользователей, формирование матрицы доступа и т.п.).

2. Непрерывный контроль за функционированием АС (контроль правильности настройки СЗИ, выполнения правил защиты информации пользователями, выполнения правил политики безопасности информации при подключении к сетям общего доступа и т.п.);

3. Реагирование на инциденты в области БИ в соответствии с установленной политикой и «Обязанностями администратора безопасности».

4. Анализ отчетов о работе СЗИ (по журналу регистрации системы).

Каждая типовая технологическая операция, выполняемая оператором, характеризуется:

1. Частотой. Сколько раз администратор безопасности выполняет типовую технологическую операцию. Чем выше показатель частоты типовой технологической операции, тем более важными становятся ее операционные характеристики.

2. Составом. Типовой сценария взаимодействия администратора безопасности с СЗИ при выполнении типовой технологической операции и разложение ее на элементарные действия администратора.

3. Операционным показателем «Сложность». Комплексный показатель, который формируется на основе балльной оценки элементарных действий администратора безопасности.

Частота выполнения типовых технологических операций определяется реализуемой в организации политикой безопасности информации и характеристиками потока реализации угроз БИ. Оценке этого показателя посвящен ряд исследований [3, 4]. Поэтому данный показатель в настоящей статье не рассматривается.

Проведем анализ методов оценки показателя «Сложность».

Теоретический анализ операционных показателей СЗИ возможно выполнить с использованием закона Хика [3]. Он позволяет количественно оценивать время необходимое для принятия решения при выборе одного из нескольких вариантов. Перед перемещением курсора к окну или кнопке, а также при совершении любого другого действия из набора множества вариантов, администратор должен сделать выбор этого объекта или действия. Закон Хика утверждает, что когда необходимо сделать выбор из n вариантов, время на выбор одного из них будет пропорционально логарифму по основанию 2 от числа вариантов плюс 1, при условии, что все варианты являются равновероятными.

Математическое выражения оценки времени принятия решения в соответствии с законом Хика следующее:

$$T_o(мс) = a + b\log_2(n+1), \qquad (1)$$

где a и b – константы, которые описывают индивидуальные особенности восприятия, такие как задержка перед выполнением задания и индивидуальный коэффициент скорости принятия решения;

n – количество равнозначных альтернативных вариантов, из которых нужно выбрать.

После проведенного анализа, перемещение курсора к окну или к кнопке, а также при совершении любого другого действия, время затрачиваемое на типовую технологическую операцию может быть оценено законом Фитса:

$$T_{\partial}(мс) = a + b\log_2(D/W+1), \quad (2)$$

где T – среднее время, затрачиваемое на совершение действия;

a – время запуска/остановки устройства;

b – величина, зависящая от типичной скорости устройства;

D – дистанция от точки старта до центра объекта;

W – ширина объекта, измеренная вдоль оси движения.

Недостатком аналитических методов анализа и оценки операционных характеристик СЗИ с использованием математических выражений (1) и (2) является ориентировочный и усредненный характер оценки. Также, закон Фитса имеет ряд ограничений и допущений, ограничивающих его применимость при практических расчетах [5].

Наиболее распространенной методикой оценки операционных характеристик программных систем является применение технологии eye-tracking (технологии отслеживания движения взгляда). Данная технология нашла широкое применение для проведения оценки эффективности печатной рекламы, рекламных видеоклипов и др. Также технология eye-tracking может применяться при оценке времени фиксации взгляда на элементах интерфейса СЗИ. Использование такого оборудования как «Tobii eye tracker 4C» при помощи лучей ближнего инфракрасного спектра позволяет зафиксировать движение глаз во время просмотра интерфейса программы. Отметить последовательность перемещения взгляда, длительность фиксации на определенном месте интерфейса программы.

Применяя данную технику, оценивается возможность рационального размещения элементов интерфейса программы. Также возможно построить тепловую карту распределения внимания по интерфейсу программы.

Основным недостатком технологии eye-tracking является ориентация на качественный анализ операционных характеристик и трудность получения количественных оценок операционных характеристик СЗИ. Поэтому при проведении экспериментальной оценки целесообразно применить второй, наиболее широко применяемый метод mouse-tracking.

Mouse-tracking (отслеживание мыши также известное как отслеживание курсора) инструмент позволяющий отслеживать движение мыши администратором безопасности и сделанные им клики. Использование этого инструмента позволяет построить последовательность передвижения курсора по интерфейсу и карту кликов, показывающую по каким элементам интерфейса СЗИ чаще кликали. Также, программы реализующие технологии отслеживания мыши позволяют экспериментально определить операционные характеристики программы, такие как время выполнения всей операции и время задержки курсора на элементе интерфейса программы (окне, кнопке и т.п.).

В качестве инструмента, реализующего технологию mouse-tracking целесообразно использовать программу «IOGraph V1.0.1».

Заключение. Применение специального программного и аппаратного обеспечения, реализующего технологии отслеживания движения взгляда и технологии записи перемещения курсора позволило бы экспериментально оценить показатель качества «удобство использования» СЗИ – «сложность», характеризующий среднее требуемое время выполнения типовых технологических операций администратором. Отдельно необходимо упомянуть о возможности использовать значения «сложности» при построении сетевых планов выполнения работ по эксплуатации и обслуживанию АС в защищенном исполнении, расчетам при обосновании структуры и численности подразделений ответственных за защиту информации, а также при проведении расчетов по оценке своевременности выполнения работ в соответствии с методиками.

Библиографический список

1. *ФСТЭК РФ.* Приказ ФСТЭК России от 14 марта 2014 г. N 31. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды: [Электронный ресурс]. – URL: https://fstec.ru/component/attachments/download/ (дата обращения: 21.12.2018).
2. *Хвостов В.А.* Разработка моделей и алгоритмов обоснования требований к программным средствам защиты информации от несанкционированного доступа: дис. канд. техн. наук: 05.13.19. – Воронеж: Воронежский государственный технический университет, 2008. – 137 с.
3. *Скрыпников А.В.* Нормирование требований к характеристикам программных систем защиты информации / А.В. Скрыпников, В.А. Хвостов, Е.В. Чернышова, В.В. Самцов, М.А. Абасов // Вестник Воронежского государственного университета инженерных технологий. – 2018. – Т. 80. № 4 (78). – С. 96-110.
4. *Хвостов В.А.* Методы и средства повышения защищенности автоматизированных систем: монография / В.А. Хвостов [и др.]. – Воронеж: Воронежский институт МВД России, 2013. – 108 с.
5. *Хвостов В. А.* Модель оценки эргатотехнических характеристик систем защиты информации автоматизированных средств управления экологически опасными объектами от несанкционированного доступа / В.А. Хвостов [и др.] // Теоретические основы проектирования технологических систем и оборудования автоматизированных производств: межвуз. сб. науч. тр. – Воронеж: ВГТА, 2007. –Часть 2. Вып. 5. – С. 160-169.
6. *Скрыпников А.В.* Защита данных при передаче по беспроводным каналам связи / А.В. Скрыпников, В.В. Денисенко, К.С. Евтеева // International Journal of Humanities and Natural Sciences, Vol. 8-2, 2019, – С. 35-38
7. *Абрамов Г.В.* Моделирование пакетной передачи сети при условии гарантированной доставки / Г.В. Абрамов, В.В. Денисенко // Математические методы в технике и технологиях – ММТТ. – 2014. – № 4 (63). – С. 211-213.

ANALYTICAL EVALUATION OF THE OPERATIONAL CHARACTERISTICS OF INFORMATION PROTECTION SYSTEMS

I.A. Khvostov, *Candidate of Technical Science*
V.V. Denisenko, *Senior Lecturer*
K.S. Evteeva, *Graduate Student*
M.A. Zaitseva, *Graduate Student*
A.A. Skrypnikov, *Student*
Voronezh State University of Engineering Technology
(Russia, Voronezh)

Abstract*. The article describes an analysis of the problem of evaluating the operational characteristics of an information security system. In the work process the security administrator of the automated system (AS) performs operations on the operation of the information security system (ISS). Moreover, the basis of the “man-machine” interaction is the interface of the protection program. The most important characteristic of SIS for its main user, the security administrator, is "ease of use". This indicator is assessed by probabilistic, temporary and operational indicators.*

Keywords*: information security; automated system; information security system; system effectiveness; unauthorized access; information security; FSTEC.*