УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-19-24

ПРЕИМУЩЕСТВА МОДЕЛИРОВАНИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Анастасия Сергеевна Голдобина
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, кафедра информационной безопасности, тел. (923)220-80-89,e-mail: nastya-gold09@mail.ru

Игорь Николаевич Карманов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой физики, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

Полина Александровна Звягинцева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

Статья представляет значимость моделирования при внедрении разработанной системы на предприятие, помогая избежать существенных экономических потерь, и обеспечивая защиту информации при работе средств обнаружения вторжений, в информационных системах.

Ключевые слова: модель процессов управления, показатели эффективности, эффективности смоделированных процессов.

ADVANTAGES OF SECURITY MANAGEMENT PROCESS MODELING OF STATE INFORMATION SYSTEMS

Anastasia S. Goldobina
Siberian State University of Geosystems and Technologies, 10 Plakhotnogo St., Novosibirsk, 630108, Russia, Student, Department of Information Security, phone: (923)220-80-89, e-mail: nastya-gold09@mail.ru

Igor N. Karmanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of Department of Phisics, phone: (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

Polina A. Zviagintceva
Siberian State University of Geosystems and Technologies, 10 Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone:(383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

The article demonstrates the importance of modeling in the implementation of the developed system at the enterprise, helping to avoid significant economic losses, and providing protection of

information during the work of intrusion detection in information systems built with using optical equipment.

Key words: management processes model, efficiency indicators, efficiency of simulated processes.

Государственные информационные системы (ГИС) все чаще строятся на базе автоматизированных систем. Актуальность защиты информации в них обусловлена существенными изменениями в законодательстве Российской Федерации. ФСТЭК России рекомендует использовать моделирование процессов управления защитой информации в качестве предпроектного обследования для выявления недочетов до ввода ГИС в эксплуатацию.

Целью работы является обоснование проведения оценки эффективности для модели процессов управления защитой информации ГИС с использованием имитационной модели [1–3].

Существует три вида программ для имитационного моделирования:

– инструментарий имитационного моделирования, основанного на потоковых диаграммах;

– инструментарий динамического моделирования;

– инструментарий дискретно-событийного имитационного моделирования.

Для создания модели системы управления защитой информации необходимы функции последнего вида программ, которые позволяют пользователю выполнять наблюдение за движением в системе потоковых объектов, т.к. эти инструменты дают возможность моделировать потоки объектов. Наиболее распространенными системами имитационного моделирования являются следующие программы: AnyLogic, Arena, Simulink.

В работе было проанализировано 2 существующих способа построения модели. Первый способ управления параметрами объекта состоит в создании пропорциональных входного и выходного параметров в системе. При изменении выходного параметра система выдаст ошибку. Также устанавливаются пороговые сигналы системы, определяющие значения положительной и отрицательной величины отклонения от номинальной величины выходного параметра системы. Второй способ удаленного управления аппаратурой состоит в формировании на ПУ команд в виде управляющих сигналов и их передачи по линиям связи устройству приема команд и адресной выдачи управляющих сигналов.

В анализируемых работах были выявлены недостатки, снижающие функциональные возможности трехуровневого управления группами программных средств при использовании технического решения как в качестве способа, так и в качестве процессов трехуровневого управления программными средствами различного назначения.

Перечисленные отличительные признаки, позволяют расширить функциональные возможности системы трехуровневого алгоритма управления подсистемой обнаружения вторжений. Это реализуется за счет обеспечения выполнения функций управления в отделе мониторинга и безопасности и доопределе-

ния данных об объектах воздействия на пунктах управления АРМ в трехуровневой системе управления путем опроса системы, измерения состояния системы, удаленного измерения состояния системы, вычисления запущенных процессов и выбора объектов по характеристикам.

Трехуровневую модель процессов управления, возможно построить двумя способами:

– решение аналитической задачи;
– моделирование AnyLogic.

Для приема и обработки событий безопасности в защищаемой ГИС необходимо трехуровневое моделирование процессов управления системой защиты информации с использованием программного обеспечения AnyLogic для более точных расчетов.

Для построения имитационной модели процессов управления формализуются задачи под объект, что подразумевает описание процесса управления системой защиты информации с учетом приказа ФСТЭК России №17 на трех уровнях:

– третий – отдел мониторинга и безопасности;
– второй – сервера, на которых собранные данные автоматизируются;
– первый – автоматизированной рабочее место (далее – АРМ).

Формальная запись действия ${}^{j}D_i$ алгоритма означает i-е действие на j-м уровне моделирования. Алгоритм процессов управления выглядит следующим образом:

${}^{3}D_1$ – моделирование процесса создания команд на сбор данных об имеющихся в организации группах программных средств, объектах воздействия, условиях обстановки для управления системой защиты информации через пункт управления отдела мониторинга и безопасности;

${}^{3}D_2$ – моделирование процесса о ранжируемых данных для обнаружения и идентификации инцидентов об объектах воздействия для передачи в отдел мониторинга и безопасности;

${}^{3}D_3$ – моделирование процесса передачи данных об объектах, назначенных для осуществления управления средствами защиты информации, из пункта управления отдела мониторинга и безопасности на пункт управления сервера;

${}^{2}D_4$ – моделирование процесса приема данных об объектах, имеющихся в организации и назначенных для осуществления обнаружения и идентификации инцидентов, из пункта управления отдела мониторинга и безопасности на пункт управления сервера;

${}^{2}D_5$ – моделирование процесса проанализированных данных для регистрации и анализа событий безопасности между имеющимися в организации группами программных средств, объектах воздействия и условиях обстановки на полноту;

${}^{2}D_6$ – моделирование процесса распределения объектов воздействия для управления изменениями базовой конфигурации путем осуществления доопределения данных между пунктом управления сервера и пунктом управления АРМ, имеющимися в организации;

$^{2}D_{7}$ – моделирование процесса распределения каждого объекта воздействия для управления изменениями базовой конфигурации системы путем доопределения данных об объектах, имеющихся в организации, на два сервера, на одном из которых будет осуществляться непосредственное измерение состояния системы на пункт управления АРМ, а на другом – удаленное измерение состояния системы на пункт управления АРМ;

$^{2}D_{8}$ – моделирование процесса определения состояния системы для регистрации и анализа событий безопасности на пункт управления сервера;

$^{2}D_{9}$ – моделирование процесса измерения состояния системы для обнаружения и идентификации инцидентов на пункт управления сервера;

$^{2}D_{10}$ – моделирование процесса передачи значений состояния системы, предназначенных для одного или нескольких других серверов для управления изменениями базовой конфигурации системы одной группы программных средств, имеющихся в организации, в качестве удаленно измеренных;

$^{2}D_{11}$ – моделирование процесса приема удаленно измеренных значений состояния системы для обнаружения и идентификации инцидентов объектов воздействия, на другом пункте управления сервера, имеющемся в организации;

$^{2}D_{12}$ – моделирование процесса вычисления запущенных характеристик для контроля за событиями безопасности и действиями на пункт управления сервером;

$^{2}D_{13}$ – моделирование процесса выбора объектов по характеристикам для управления средствами защиты информации на пункт управления сервера;

$^{2}D_{14}$ – моделирование процесса доопределения данных о выделенной части объектов воздействия на пункт управления сервера. Одновременно с первым процессом происходит моделирование процесса формирования команды на доопределение данных о программных средствах, объектах воздействия и условиях обстановки, для управления изменениями базовой конфигурации системы, имеющейся в организации;

$^{2}D_{15}$ – моделирование процесса передачи команды на доопределение данных с пункта управления сервера на пункт управления АРМ, входящих в состав одной группы программных средств организации для управления средствами защиты информации;

$^{1}D_{16}$ – моделирование процесса формирования базы данных программных средств, объектов воздействия и условий обстановки, на пункт управления АРМ для регистрации и анализа событий в системе, имеющейся в организации;

$^{1}D_{17}$ – моделирование процесса определения состояния системы для регистрации и анализа событий на пункте управления АРМ;

$^{1}D_{18}$ – моделирование процесса измерения состояния системы для обнаружения и идентификации инцидентов на пункт управления АРМ;

$^{1}D_{19}$ – моделирование процесса передачи значений состояния системы, предназначенного для одного или нескольких других пунктов управления АРМ одной группы в качестве удаленно измеренных систем, на эти пункты управления АРМ для управления средствами защиты информации;

$^{1}D_{20}$ – моделирование процесса приема удаленно измеренных на другом пункте управления АРМ значений состояния системы объектов воздействия, для управления изменениями базовой конфигурации системы, имеющейся в организации;

$^{1}D_{21}$ – моделирование процесса вычисления запущенных процессов на пункте управления АРМ для контроля за событиями безопасности, имеющимися в организации;

$^{1}D_{22}$ – моделирование процесса выбора объектов по характеристикам на пункте управления АРМ для управления изменениями базовой конфигурации системы;

$^{1}D_{23}$ – моделирование процесса передачи данных на пункт управления сервера о программных средствах, объектах воздействия и условиях обстановки, для управления средствами защиты информации, имеющихся в организации;

$^{2}D_{24}$ – моделирование процесса сбора доопределенных данных на пункт управления сервера о состоянии программных средств группы, объектах воздействия и условиях обстановки, для регистрации и анализа событий системы, имеющейся в организации;

$^{2}D_{25}$ – моделирование процесса идентификации объектов воздействия на пункт управления сервера для обнаружения и идентификации системы;

$^{2}D_{26}$ – моделирование процесса классификации объектов воздействия на пункт управления сервера для контроля за событиями безопасности;

$^{2}D_{27}$ – моделирование процесса формирования списка объектов воздействия в соответствии с полученными значениями их приоритетов для управления изменениями базовой конфигурации системы;

$^{2}D_{28}$ – моделирование процесса оценки эффективности осуществления воздействия на внесенные в список приоритетных объектов воздействия штатными программными средствами, для контроля за событиями безопасности;

$^{2}D_{29}$ – моделирование процесса формирования списка программных средств, значения эффективности которых оказались достаточными для осуществления воздействия на объекты из сформированного списка для управления изменениями базовой конфигурации системы;

$^{2}D_{30}$ – моделирование процесса формирования команд управления в виде управляющих сигналов для управления изменениями базовой конфигурации;

$^{2}D_{31}$ – моделирование процесса передачи по каналам связи для обнаружения и идентификации инцидентов.

Система управления решает задачи управления, поступающие от вышестоящего пункта управления с интервалом 10 мин. Каждая задача управления характеризуется количеством объектов воздействия, по каждому из которых принято решение на осуществление воздействия, произведено распределение этих объектов между подчиненными элементами, сформирована команда на осуществление воздействия и доведена до подчиненных. Система позволяет создавать цепь процессов, соединенных между собой. Процессы в свою очередь задают последовательность операций, через которые проходят заявки.

Необходимо учесть, что единых подходов оценки эффективности [2, 3] нет – не только к обеспечению защиты информации, но и к построению самих систем и их компонентов. Поэтому необходимо разработать инструменты для определения подходов к построению систем защиты [5], так и для определения показателей ее эффективности.

При выборе показателя эффективности защиты информации нужно исходить из того, что эффективность управления защитой информации [4] оценивается с помощью показателя эффективности управления. Исходя из основного целевого назначения системы управления – своевременной выработки и реализации правильного управляющего воздействия на управляемый объект, показателем эффективности управления защитой информации Wэ целесообразно выбрать вероятность своевременного принятия и реализации правильного решения, обеспечивающего оптимальное использование возможностей подчиненных технических средств.

Трехуровневая модель обеспечивает полноту и логичность системы защиты информации в ГИС и визуализирует качество функционирования системы во времени, что позволяет обеспечить эффективность процесса обеспечения управления безопасностью.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Селифанов В. В., Звягинцева П. А., Юракова Я. Ю. Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных системах с применением банка данных угроз ФСТЭК России // Вестник СГУГиТ. – 2017. – Т. 22, № 4. – С. 202–209.

2. Селифанов В. В. Оценка эффективности системы защиты информации государственных информационных систем от несанкционированного доступа // Интеграция науки, общества, производства и промышленности: сборник статей Международной научно-практической конференции, 2016. – С. 109-113.

3. Селифанов В.В., Звягинцева П.А., Голдобина А.С., Исаева Ю.А. Оценка эффективности системы защиты информации ИСПДН с учетом профиля защиты // Вестник СГУГиТ. – 2017. Т. 22, № 4. – С. 220–225.

4. Селифанов В.В., Ремизова В.А. Проведение аттестационных испытаний средств антивирусной защиты // Информационные системы и процессы, сборник научных трудов, Новосибирский государственный университет экономики и управления «НИНХ» (Новосибирск), 2015. – С. 208–213.

5. Селифанов В.В., Курносов К.В. Требования к системе защиты информации для виртуальной инфраструктуры // Информационное противодействие угрозам терроризма. 2014. № 23. С. 188.