УДК 004.054.53

А.С. Голдобина, Ю.А. Исаева, В.В. Селифанов, А.М. Климова, П.С. Зенкин

Построение адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры

Рассматривается трехуровневая модель процессов управления системой защиты информации на примере объектов критической информационной инфраструктуры. Критические информационные инфраструктуры Российской Федерации во избежание реализации различных инцидентов безопасности нуждаются в постоянном анализе и обновлении правил работы. Авторами был предложен алгоритм, позволяющий делать своевременную выработку решений путём имитации процессов работы систем. Моделирование системы позволяет провести оценку эффективности системы и сделать необходимые предложения по повышению уровня защищенности.

Ключевые слова: трёхуровневая модель, система управления, оценка эффективности, система защиты информации.

doi: 10.21293/1818-0442-2018-21-4-51-58

В связи с появлением новых требований к обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации необходимо обновление правил работы и реагирования систем защиты информации на различные инциденты. Так как объекты критической информационной инфраструктуры представляют собой сложные информационные системы, то эффективность работы системы защиты информации зависит от качества процессов ее управления.

Основное назначение процессов управления – это своевременная выработка и реализация управляющего воздействия на управляемый объект (средства защиты информации, персонал, операционные системы, программное обеспечение и др.). Показателем эффективности является вероятность своевременного принятия и реализации правильного решения.

Одним из наиболее эффективных инструментов, дающих возможность оценки работы системы защиты информации объектов критической информационной инфраструктуры и процессов их управления до принятия решения о реализации конечного варианта технического проекта, является моделирование.

Оно позволяет получить достаточно полное представление о реакции системы защиты на различные ситуации и наглядно демонстрирует ее работу. В процессе моделирования можно увидеть работу каждого объекта в определенный момент времени [17]. Это позволит заранее увидеть и предотвратить нежелательные действия или последствия работы системы с неверными входными данными и позволит избежать значимых экономических потерь [11].

Для оценки работы систем защиты информации объектов критической информационной инфраструктуры Российской Федерации была разработана адаптивная трехуровневая имитационная модель, представляет собой однофазную систему массового обслуживания разомкнутого типа с неограниченной

входной емкостью, т.е. без отказов в обслуживании, с ограничением по времени пребывания заявок в системе, определяемым критическим временем длительности цикла управления и абсолютной надежностью.

Рассматриваемая модель имитирует процессы работы систем на предприятии. Модель состоит из потоков данных, поступающих в обработку системы. Такая детализация является важным аспектом разработки характеристик будущих систем или модернизации уже существующих систем защиты информации [21]. Так как работа критической информационной инфраструктуры должна быть постоянной и непрерывной, имитационное моделирование процессов управления позволит построить систему, способную к максимальным нагрузкам, из расчета всех параметров, которые будут указаны в модели.

В процессе работы имитационная модель способна показать, какие места системы не смогут выдержать предполагаемой нагрузки или какие места используются не в полную силу [22]. Данные функции позволяют не только изменять параметры разрабатываемой системы, но и понять, как лучше организовать архитектуру системы.

Анализ нормативной базы в области безопасности критической информационной инфраструктуры, а именно Федерального закона № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» и приказов ФСТЭК России № 21, 17 и 239, показал, что большинство объектов защиты имеют трехуровневую структуру, где каждый уровень представлен совокупностью объектов управления.

Исходя из анализа примерной структуры объекта исследования и учитывая необходимость минимизации времени реакции системы управления, на изменение принятия решения, целесообразно использовать трехуровневую структуру для построения адаптивной имитационной модели, не исключая нижний уровень ввода (вывода) данных, что с точки зрения управления процессами безопасности увели-

чит эффективность работы модели и физической системы управления [19].

Сама трехуровневая модель представляет собой следующую архитектуру:

- уровень операторского управления или пункты управляющего воздействия (третий уровень);
- уровень автоматического ввода (вывода) данных или автоматизированные пункты управления (второй уровень);
- уровень ввода (вывода) данных исполнительных устройств или пункты приема исходных данных (первый уровень).

Принцип работы трехуровневой архитектуры представлен на рис. 1.

Рис. 1. Принцип работы трехуровневой архитектуры

Трёхуровневая архитектура модели и будущей системы позволит не только наблюдать подробные изменения работы моделируемой системы, но и позволит системе распределять рабочие нагрузки, что приведет к повышению работоспособности системы защиты информации [9].

Исходя из свойств атрибутов безопасности критической информационной инфраструктуры, имитационная модель должна иметь адаптивные свойства, которые обеспечат приспособление моделируемой

системы к новым, измененным свойствам и параметрам. Это позволит изменять характеристики данных, поступающих на вход модели, и регулировать работу имитируемой системы [10].

Алгоритм, вложенный в основу моделирования, заключается в выполнении на пункте управления третьего уровня таких функций управления, как сбор, обработка, анализ, адаптивный выбор порядка доопределения данных и оценки эффективности воздействия [20], доопределение данных об объектах воздействия, оценка возможностей своей группы ТС и принятие решения на осуществление воздействия, а на пункте управления второго уровня – функций доопределения данных об объектах воздействия и оценки эффективности воздействия всех своих ТС на все объекты воздействия [1].

Схема работы трехуровневого алгоритма показана на рис. 2.

Формальная запись действий iD_j алгоритма управления означает i -е действие на j -м уровне управления.

Этот алгоритм позволяет формировать управляющие решения, основываясь на полученных данных, в ходе анализа работы системы защиты информации. Данные, полученные с первого уровня адаптивной двухуровневой имитационной модели, передаются на второй уровень модели, который формирует управляющие воздействия и является пунктом управления.

3D_1 – моделирование (имитация) формирования на пункте управления операторского уровня команд на сбор данных о подчиненных средствах, средствах защиты и сложившейся обстановке;

3D_2 – имитация передачи команд на сбор данных по линиям связи на пункты управления второго уровня автоматического ввода данных;

2D_3 – имитация формирования на ПУ второго уровня автоматического ввода данных базы данных технических средств (ТС) своей группы, средств защиты и сложившейся обстановки;

2D_4 – имитация передачи на ПУ третьего уровня ввода данных исполнительных устройств, данных о ТС своей группы, средствах защиты и сложившейся обстановке;

3D_5 – имитация сбора на ПУ третьего уровня ввода данных исполнительных устройств, данных о состоянии своих групп ТС, средствах защиты и сложившейся обстановке;

3D_6 – имитация формирования базы данных своих групп ТС, средствах защиты и сложившейся обстановке;

3D_7 – имитация анализа данных о своих группах ТС, средствах защиты и сложившейся обстановке на полноту;

3D_8 – имитация ранжирования средств защиты;

3D_9 – имитация оценки возможностей своих групп ТС по осуществлению воздействия на объекты;

${}^3D_{10}$ – имитация распределения проранжированных объектов воздействия между группами ТС в соответствии с их возможностями по осуществлению воздействия;

Рис. 2. Схема работы трёхуровневого алгоритма

$^3D_{11}$ – имитация формирования задания группам ТС для осуществления воздействия на выбранные объекты;

$^3D_{12}$ – имитация передачи на пункты управления второго уровня данных об объектах, назначенных для осуществления воздействия;

$^2D_{13}$ – имитация приема на пунктах управления второго уровня данных об объектах, назначенных для осуществления воздействия;

$^2D_{14}$ – имитация анализа данных о ТС своей группы, объектах воздействия и условиях обстановки на полноту;

$^2D_{15}$ – имитация при необходимости доопределения данных об объектах воздействия, включающего следующие действия:

$^2D_{16}$ – имитация распределения объектов воздействия для осуществления доопределения данных между пунктом управления второго уровня и пунктами управления первого уровня, входящими в состав одной группы;

$^2D_{17}$ – при этом проводят имитацию распределения каждого объекта воздействия для доопределения данных о нем на два пункта управления, на одном из которых будет осуществляться непосредственное измерение первичных характеристик, а на другом – удаленное измерение первичных характеристик;

$^2D_{18}$ – имитация доопределения на пункте управления второго уровня данных о выделенной части объектов воздействия, которое включает следующие действия:

$^2D_{19}$ – имитация определения первичных характеристик;

$^2D_{20}$ – имитация измерения первичных характеристик;

$^2D_{21}$ – имитация передачи значений первичных характеристик, предназначенных для одного или нескольких других пунктов управления одной группы в качестве удаленно измеренных, на эти пункты управления;

$^2D_{22}$ – имитация приема удаленно измеренных на другом пункте управления значений первичных характеристик своих объектов воздействия;

$^2D_{23}$ – имитация вычисления вторичных характеристик;

$^2D_{24}$ – имитация селекции объектов по характеристикам;

$^2D_{25}$ – одновременно с имитациями доопределения на пунктах управления второго уровня данных о выделенной части объектов воздействия – имитация формирования команды на доопределение данных о своих ТС, средствах защиты и сложившейся обстановке;

$^2D_{26}$ – имитация передачи команды на доопределение данных по линиям связи на пункты управления первого уровня, входящие в состав одной группы;

$^1D_{27}$ – имитация формирования на пунктах управления первого уровня базы данных своего ТС, средствах защиты и сложившейся обстановке;

$^1D_{28}$ – имитация доопределения данных об объектах воздействия, которое включает следующие действия:

$^1D_{29}$ – имитация определения первичных данных;

$^1D_{30}$ – имитация измерения первичных данных;

¹D₃₁ – имитация передачи значений первичных характеристик, предназначенных для одного или нескольких других пунктов управления одной группы в качестве удаленно измеренных, на эти пункты управления;

¹D₃₂ – имитация приема удаленно измеренных на другом пункте управления значений первичных характеристик своих объектов воздействия;

¹D₃₃ – имитация вычисления вторичных данных;

¹D₃₄ – имитация селекции объектов по полученным данным;

¹D₃₅ – имитация передачи на ПУ второго уровня данных о своем ТС, средствах защиты и сложившейся обстановке;

²D₃₆ – имитация сбора на ПУ второго уровня доопределенных данных о состоянии ТС своей группы, средствах защиты и сложившейся обстановке;

²D₃₇ – имитация уточнения базы данных ТС своей группы, средствах защиты и сложившейся обстановке.

²D₃₈ – имитация идентификации средств защиты;

²D₃₉ – имитация классификации средств защиты;

²D₄₀ – имитация определения приоритетов объектов воздействия;

²D₄₁ – имитация формирования списка объектов воздействия в соответствии с полученными значениями их приоритетов;

²D₄₂ – имитация оценки эффективности осуществления воздействия на внесенные в список приоритетных объектов воздействия штатными ТС;

²D₄₃ – имитация формирования случайным образом списка ТС, значения эффективности которых оказались достаточными для осуществления воздействия на объекты из сформированного списка;

²D₄₄ – имитация распределения объектов для осуществления воздействия между ТС путем последовательного попарного соотнесения объектов воздействия и ТС из соответствующих сформированных списков;

²D₄₅ – имитация формирования целеуказания штатным ТС для осуществления воздействия на выбранные объекты;

²D₄₆ – имитация формирования команд управления в виде управляющих сигналов;

²D₄₇ – имитация передачи команд управления техническим средствам;

²D₄₈ – имитация канала связи.

Результаты экспериментов

Построение и эксплуатация систем защиты информации новых объектов защиты нуждается в исследовании для определения эффективных подходов на всех стадиях жизненного цикла [16]. Одним из важнейших направлений здесь является оценка эффективности управления защитой информации [15]. При этом основной целью управления будет являться своевременная выработка и реализация управляющего воздействия на управляемый объект. При решении поставленной задачи необходимо учесть, что подобные системы только начинают создавать-

ся, единых подходов нет – не только к обеспечению защиты информации, но и к построению самих систем и их компонентов [12]. Поэтому необходимо разработать инструменты для определения подходов к построению систем защиты, так и для определения показателей её эффективности [18].

При выборе показателя эффективности защиты информации будем исходить из того, что эффективность управления защитой информации оценивается с помощью показателя эффективности управления [13]. Показатель эффективности характеризует степень соответствия рассматриваемой системы своему назначению [14]. Исходя из основного целевого назначения системы управления – своевременной выработки и реализации правильного управляющего воздействия на управляемый объект, показателем эффективности управления защитой информации W_3 целесообразно выбрать вероятность своевременного принятия и реализации правильного решения, обеспечивающего оптимальное использование возможностей подчиненных технических средств.

Её можно представить в следующей форме:

$$W_3 = p[(I_{Pk} \geq I_P), (I_{Mk} \geq I_M), (\tau \leq \tau_{кр})], \quad (1)$$

где p – вероятность того, что вся необходимая для принятия решения информация будет собрана и правильное решение будет своевременно принято и реализовано; I_{Pk} – фактически собираемое и обрабатываемое количество информации об объектах воздействия; I_P – количество требуемой информации об объектах воздействия; I_{Mk} – фактически собираемое и обрабатываемое количество информации о компонентах системы защиты, привлекаемых для выполнения задач; I_M – количество требуемой информации о компонентах системы защиты, привлекаемых для выполнения задач; τ – время цикла управления; $\tau_{кр}$ – критическое (требуемое) время цикла управления.

Приведенное соотношение (1) количественно характеризует противоположные факторы, отражающие, с одной стороны, необходимость сбора и обработки больших объемов информации, а с другой – отводимое на это ограниченное время.

При решении задачи определения показателя эффективности управления защитой информации (далее – ЗИ) целевой составляющей будет являться количество информации об объектах воздействия I_{Pk} , которая фактически собирается и обрабатывается в процессе управления для решения стоящей задачи, и его соотношение с количеством требуемой информации об объектах воздействия I_P , а на время цикла управления τ накладывается ограничение. Значение ограничения выбирается близким к $\tau_{кр}$, исходя из опыта построения подобных систем управления, а также на основе анализа эффективности применения рассматриваемых средств.

Считается, что информация о компонентах системы защиты информации I_M , а также о критическом времени цикла управления $\tau_{кр}$ при выполнении стоящей задачи всегда известна в системе управления из результатов анализа конкретной задачи. По-

этому для оценки параметров процессов управления компонентами системы защиты информации необходимо определять количество требуемой для управления информации об объектах воздействия I_p .

Значение количества информации об объектах воздействия I_{pk} и информации о компонентах системы защиты, привлекаемых для выполнения задач I_{Mk} , привлекаемых для выполнения задачи, которая фактически собирается и обрабатывается в процессе управления для решения задач, а также реальное время цикла управления τ и соотношение этих величин с требуемыми значениями рассчитать аналитическим методом крайне затруднительно ввиду большой сложности исследуемых процессов управления (многомерность, большое количество параметров, стохастичность, параллельность протекания процессов), поэтому они определяются с помощью имитационного моделирования процессов управления. При этом в имитационной модели для оценивания показателя эффективности управления защитой информации будем использовать следующую мультипликативную форму:

$$W_{\Sigma} = P_{\text{св.сб}} \times P_{\text{пр}} \times P_{\text{св.пр}} \times P_p, \quad (2)$$

где $P_{\text{св.сб}}$ – вероятность своевременного сбора всей необходимой для принятия решений информации; $P_{\text{пр}}$ – вероятность правильного принятия решений; $P_{\text{св.пр}}$ – вероятность своевременного и правильного принятия решений; $P_{\text{св.р}}$ – вероятность своевременной реализации принятых решений. Под своевременной реализацией принятых решений понимается своевременное доведение соответствующих команд до компонентов системы защиты информации.

Порядок оценки показателя эффективности при этом может быть следующим:

- вводятся исходные данные;
- вычисляется сумма величин весовых коэффициентов важности K_i базового аргумента, вычисляется весовой коэффициент K ;
- анализируется соответствие вариантов решений и ситуаций;
- учитывается коэффициент важности первого аргумента;
- вычисляется число совпадений вариантов решений и ситуаций;
- анализируются результаты оценки числа совпадений вариантов решений и ситуаций и по наибольшему числу совпадений выбирается лучшее решение;
- оценивается время, затраченное на принятие решения i -м лицом, принимающим решения (далее – ЛПР) в j -й ситуации;
- одновременно с оценкой времени, затраченного на принятие решения i -м ЛПР в j -й ситуации, оценивается время реализации решений t_{ij} ;
- одновременно с оценкой времени, затраченного на принятие решения i -м ЛПР в j -й ситуации, оценивается время t_{ij} , затраченное на сбор всей необходимой для принятия решения информации в j -й ситуации;
- определяется количество своевременно принятых для j -й ситуации решений R_j , одновременно

определяется количество своевременно реализованных решений;

– с определением количества своевременно принятых для j -й ситуации решений R_j одновременно определяется количество своевременно реализованных решений C_j ;

– одновременно с определением количества своевременно принятых для j -й ситуации решений R_j определяется количество ситуаций $M_{\text{св.инф.}j}$, для принятия решения в которых вся необходимая информация была собрана своевременно;

– определяются правильно принятые решения для j -й ситуации;

– определяется количество правильно принятых решений для j -й ситуации S_j ;

– определяется общее количество правильно принятых решений;

– определяется общее относительное количество правильно принятых решений;

– определяется относительное количество своевременно и правильно принятых решений;

– определяется общее относительное количество своевременно и правильно принятых решений;

– одновременно с определением общего относительного количества своевременно и правильно принятых решений определяется общее относительное количество своевременно реализованных решений;

– определяется вероятность правильного принятия решений $P_{\text{пр}}$:

$$P_{\text{пр}} = \frac{1}{M} \sum_{j=1}^M \frac{S_{\text{пр.}j}}{L}, \quad (3)$$

где M – число рассматриваемых ситуаций; L – количество ЛПР, участвующих в работе для j -й ситуации; $S_{\text{пр.}j}$ – число правильно принятых решений для j -й ситуации;

– одновременно с определением вероятности правильного принятия решений определяется вероятность своевременного сбора всей необходимой для принятия решений информации $P_{\text{св.сб}}$;

– определяется вероятность своевременного и правильного принятия решений $P_{\text{св.пр}}$:

$$P_{\text{св.пр}} = \frac{1}{M} \sum_{j=1}^M \frac{R_j}{S_{\text{пр.}j}}, \quad (4)$$

где R_j – число своевременно и правильно принятых для j -й ситуации решений;

$$R_j = \sum_{i=1}^L R_{ij}, \quad (5)$$

где

$$\begin{cases} R_{ij} = 1, & \text{если } t_{ij} \leq t_{\text{доп}}, \\ R_{ij} = 0, & \text{если } t_{ij} > t_{\text{доп}}, \end{cases} \quad (6)$$

где t_{ij} – текущее значение времени, затраченного на принятие решения i -м ЛПР в j -й ситуации; $t_{\text{доп}}$ – допустимое время на принятие решения; – одновременно с определением вероятности правильного принятия решений и вероятности своевременного и правильного принятия решений определяется вероятность своевременной реализации принятых решений $P_{\text{св.р}}$:

$$P_{с.вр} = \frac{1}{Q \times M} \sum_{j=1}^M \frac{C_j}{R_j}, \quad (7)$$

где C_j – число своевременно реализованных правильно и своевременно принятых для j -й ситуации решений;

$$C_j = \sum_{q=1}^Q C_{qj}, q = \overline{1, Q}, \quad (8)$$

где Q – число направлений связи, соответствующее числу исполнителей;

$$\begin{cases} C_{qj} = 1, & \text{если } t_{qj} \leq t_{\text{доп.р}}, \\ C_{qj} = 0, & \text{если } t_{qj} > t_{\text{доп.р}}, \end{cases} \quad (9)$$

где t_{qj} – текущее значение времени, затраченное на реализацию правильно и своевременно принятых решений в j -й ситуации; $t_{\text{доп.р}}$ – допустимое время на реализацию принятого решения;

– определяется значение показателя эффективности управления защитой информации W_z .

В результате работы появляется возможность определить показатель эффективности управления защитой информации, получить следующие результаты:

– статистические характеристики оцениваемых показателей (текущее, минимальное, максимальное, среднее значение);

– графики текущих и средних значений оцениваемых показателей;

– гистограммы и статистические функции распределения значений оцениваемых показателей, которые позволяют проводить оценку эффективности управления системой защиты информации таких компонентов, как:

– контроль и оперативное реагирование за событиями безопасности и действиями персонала;

– анализ и оценка функционирования системы защиты информации, включая выявление, анализ и устранение недостатков в ее функционировании;

– оперативное принятие мер по устранению инцидентов.

Результаты экспериментов

Предложенная модель и способ оценки эффективности позволят оценить предлагаемые технические решения по проектированию систем защиты информации объектов критической информационной инфраструктуры и выбрать оптимальные. В дальнейших исследованиях авторами предлагается апробировать предложенные алгоритмы на конкретных объектах.

Литература

1. Пат. 2326442 РФ, МПК: G 07 C 3 00, G 06 F 17 00. Способ оценки эффективности управления и устройство для его осуществления / В.А. Селифанов (РФ), В.В. Селифанов (РФ). – № 2007102742/09; заявл. 24.01.2007; опубл. 10.06.2008. – Бюл. № 16. – 19 с.
2. Пат. 2517409 РФ, МПК: G 07 C 3 00, G 06 F 17 00. Способ оценки эффективности управления и устройство для его осуществления / Г.Н. Акиншина (РФ), Ю.Н. Богданов (РФ), А.М. Леонтьев (РФ), Е.А. Решетняк (РФ), В.А. Селифанов (РФ). – № 2011106224/08; заявл. 17.02.2011; опубл. 27.05.2014. – Бюл. № 15. – 25 с.

3. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]. – Режим доступа: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702>, свободный (дата обращения: 15.05.2018).

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691>, свободный (дата обращения: 15.05.2018).

5. Приказ ФСТЭК России от 14 марта 2014 г. № 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]. – Режим доступа: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot>, свободный (дата обращения: 15.05.2018).

6. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования» [Электронный ресурс]. – Режим доступа: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossii-ot-21-dekabrja-2017-g-n-236>, свободный (дата обращения: 15.05.2018).

7. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: <https://minjust.consultant.ru/documents/38914>, свободный (дата обращения: 15.05.2018).

8. Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: <http://www.kremlin.ru/acts/bank/42128>, свободный (дата обращения: 15.05.2018).

9. Пат. 2451965 РФ, МПК: G 07 C 3 00, G 06 F 17 00. Способ трёхуровневого управления техническими средствами и система для его осуществления / В.А. Селифанов (РФ). – № 2011114534/08; заявл. 13.04.2011; опубл. 27.05.2012. Бюл. № 15. – 29 с.

10. Пат. 2451966 РФ, МПК: G 07 C 3 00, G 06 F 17 00. Способ адаптивного управления и система адаптивного управления для его осуществления / В.А. Селифанов (РФ). – № 2011118677/08; заявл. 10.05.2011; опубл. 27.05.2012. Бюл. № 15. – 31 с.

11. Голдобина А.С. Выбор имитационной модели процессов управления защитой информации для оценки эффективности государственных и муниципальных систем / А.С. Голдобина, Ю.А. Исаева // Инновационное развитие науки и образования: сб. статей междунар. науч.-практ. конф. (Пенза). – 2018. – Т. 2, № 2. – 86 с.

12. Селифанов В.В. Оценка эффективности системы защиты информации государственных информационных систем от несанкционированного доступа // Интеграция науки, общества, производства и промышленности: сб. ст. междунар. науч.-практ. конф. (Новосибирск). – 2016. – 109 с.

13. Надежность и эффективность в технике: справочник: в 10 т. – Т. 1: Методология. Организация, терминология / В.С. Авдусевский, И.В. Аполонов, Е.Ю. Барзелович и др. – М.: Машиностроение, 1986. – 223 с.

14. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения [Электронный ресурс]. – Режим доступа: <http://docs.cntd.ru/document/1200058320>, свободный (дата обращения: 15.05.2018).

15. Старикова А.А. Оценка эффективности управления системой защиты информации в государственных информационных системах / А.А. Старикова, Д.Г. Макарова // Интерэкспо Гео-Сибирь. – 2017. – Т. 8. – 188 с.

16. Исаев И.И. Анализ методов эффективности защиты информации // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сб. матер. Всерос. науч.-практ. конф. – 2017. – Воронеж: Воронеж. ин-т МВД России. – 235 с.

17. Даурцев А.В. Разработка математических моделей оценки показателей эффективности программных систем защиты информации в автоматизированных системах электронного документооборота // Вестник Воронеж. гос. техн. ун-та. – 2011. – Т. 7, № 2. – С. 27–31.

18. Меньших В.В. Получение оценок эффективности системы защиты информации с использованием автоматной модели имитации функционирования защищенной информационной системы / В.В. Меньших, Е.В. Петрова // Информация и безопасность. – 2011. – Т. 14, № 1. – 125 с.

19. Анисимов В.Г. Методика оценки эффективности защиты информации в системе межведомственного информационного взаимодействия при управлении обороной государства / В.Г. Анисимов, А.А. Селиванов, Е.Г. Анисимов // Информация и космос. – 2016. – № 4. – С. 76–80.

20. Звягинцева П.А. Оценка эффективности средств защиты информации / П.А. Звягинцева, О.А. Крыжановская // Интерэкспо Гео-Сибирь. – 2017. – Т. 8. – С. 199.

21. Беляева О.В. Имитационное моделирование систем защиты / О.В. Беляева, В.А. Грицык // Междунар. журнал экспериментального образования. – 2010. – Вып. 5. – С. 67.

22. Цветкова О.Л. Имитационное моделирование зависимости информационной безопасности организации от области деятельности / О.Л. Цветкова, С.А. Заслонов // Вестник Донского гос. техн. ун-та. – 2017. – Т. 18, № 4 (91). – 116 с.

Голдобина Анастасия Сергеевна

Магистрант Сибирского гос. ун-та геосистем и технологий, инженер-аналитик
ООО «Акстел-безопасность»
Колхидская ул., д. 9, г. Новосибирск, Россия, 630096
Тел.: +7-923-220-80-89
Эл. почта: nastya-gold09@mail.ru

Исаева Юлия Алексеевна

Магистрант Сибирского гос. ун-та геосистем и технологий, специалист по информационной безопасности,
ООО «Первый строительный фонд»
Гоголя ул., д. 188, г. Новосибирск, Россия, 630112
Тел.: +7-913-980-23-09
Эл. почта: isaeva.ja@hotmail.com

Селифанов Валентин Валерьевич

Доцент каф. информационной безопасности
Сибирского гос. ун-та геосистем и технологий
Ельцовская ул., д. 2/3, г. Новосибирск, Россия, 630001
Тел.: +7-913-905-64-02
Эл. почта: sf01@mail.ru

Климова Александра Михайловна

Магистрант Новосибирского гос. технического ун-та,
Немировича-Данченко ул., д. 136, г. Новосибирск,
Россия, 630073
Тел.: +7-999-466-39-66
Эл. почта: aleksandra.kl.15.6@gmail.ru

Зенкин Павел Сергеевич

Аспирант Томского гос. ун-та систем управления и радиоэлектроники (ТУСУР)
Ленина пр., д. 40, г. Томск, Россия, 634050
Тел.: +7-906-995-61-15
Эл. почта: zenkin.pavel.88@mail.ru

Goldobina A.S., Isaeva Yu.A., Selifanov V.V.,
Klimova A.M., Zenkin P.S.

Building an adaptive three-tier model of management processes for the information security system of critical information infrastructure objects

The article discusses a three-tier model of information security management processes based on the example of objects of critical information infrastructure. Critical information infrastructures of the Russian Federation, in order to avoid the implementation of various security incidents, require constant analysis and updating of work rules. The authors proposed an algorithm that allows making timely development of solutions by simulating the processes of the systems. System modeling allows to assess the effectiveness of the system and make the necessary proposals to improve the level of security.

Keywords: three-level model, control system, performance evaluation, information protection system.

doi: 10.21293/1818-0442-2018-21-4-51-58

References

1. Pat. 2326442 RF, IPC: G 07 C 3 00, G 06 F 17 00. *A method for evaluating the effectiveness of control and a device for its implementation* / V.A. Selifanov (RF), V.V. Selifanov (RF). – No. 2007102742/09; declare 01/24/2007; publ. 10.06.2008, Bull. № 16, 19 p. (in Russ.).
2. Pat. 2517409 RF, IPC: G 07 C 3 00, G 06 F 17 00. *A method for evaluating the effectiveness of control and a device for its implementation* / G.N. Akinshina (RF), Yu.N. God Dan (RF), A.M. Leontyev (RF), E.A. Reshetnyak (RF), V.A. Selifanov (RF). – No. 2011106224/08; declare February 17, 2011; publ. 05/27/2014, Bull. № 15, 25 p. (in Russ.).
3. Order of the FSTEC of Russia of February 11, 2013 No. 17 «On approval of requirements for the protection of information that is not a state secret contained in state information systems». – Access mode: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702>, free (accessed: May 15, 2018) (in Russ.).
4. Order of the FSTEC of Russia dated February 18, 2013 No. 21 «On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data when Processing the Information Systems of Personal Data». – Access mode: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691>, free (accessed: May 15, 2018) (in Russ.).
5. Order of the FSTEC of Russia dated March 14, 2014 No. 31 «On approval of Requirements for ensuring the protection of information in automated systems for managing production and technological processes at critical facilities, potentially dangerous objects, as well as facilities that pose an increased risk to life and health of people and for the environment». – Access mode: <https://fstec.ru/normotvor>

cheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot, free (accessed: May 15, 2018) (in Russ.).

6. Order of the FSTEC of Russia of December 21, 2017 No. 235 «On approval of Requirements for the creation of security systems for significant facilities of the Russian Federal Institute of Exercises and ensuring their functioning». – Access mode: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-236>, free (accessed: May 15, 2018) (in Russ.).

7. Order of the FSTEC of Russia of December 25, 2017 No. 239 “On Approval of Requirements for Ensuring the Security of Important Objects of Critical Information Infrastructure of the Russian Federation”. – Access mode: <https://minjust.consultant.ru/documents/38914>, free (accessed: May 15, 2018) (in Russ.).

8. Federal Law of 26.07.2017 No. 187 «On the Security of the Critical Information Infrastructure of the Russian Federation». – Access mode: <http://www.kremlin.ru/acts/bank/42128>, free (accessed: May 15, 2018) (in Russ.).

9. Pat. 2451965 RF, IPC: G 07 C 3 00, G 06 F 17 00. A method of three-level control of technical equipment and a system for its implementation, V.A. Selifanov (RF). No. 2011114534/08; declare 04/13/2011; publ. 27.05.2012, Bull. № 15, 29 p. (in Russ.).

10. Pat. 2451966 RF, IPC: G 07 C 3 00, G 06 F 17 00. Adaptive control method and adaptive control system for its implementation / V.A. Selifanov (RF). No. 2011118677/08; declare 05/10/2011; publ. 27.05.2012, Bull. № 15, 31 p. (in Russ.).

11. Goldobina A.S., Isaeva Yu.A. Choosing a simulation model of information security management processes for assessing the effectiveness of state and municipal systems. *Innovative development of science and education. Collection of articles of the International Scientific and Practical Conference (Penza)*, 2018, vol. 2, no. 2, 86 p. (in Russ.).

12. Selifanov V.V. Assessment of the effectiveness of the information security system of state information systems from unauthorized access. *Integration of science, society, industry and industry. Collection of articles of the International Scientific and Practical Conference (Novosibirsk)*, 2016, 109 p. (in Russ.).

13. Reliability and efficiency in technology: Reference book in 10 tons. No. 1. Methodology. The organization of terminology and logic. Moscow: Mashinostroy-Publishing House, 1986, 26 p. (in Russ.).

14. GOST R 50922-2006. Protection of information. Basic terms and definitions. Access mode: <http://docs.cntd.ru/document/1200058320>, free (accessed: May 15, 2018) (in Russ.).

15. Starikova A.A., Makarova D.G. Evaluation of the effectiveness of managing the information security system in state information systems. *Interexpo Geo-Siberia*, 2017, vol. 8, 188 p. (in Russ.).

16. Isaev I.I. Analysis of methods for the effectiveness of information protection. *Actual issues of operating security systems and protected telecommunication systems: Coll. materials of the All-Russian scientific-practical conference*, 2017, Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia, 235 p. (in Russ.).

17. Daurtsev A.V. Development of mathematical models for assessing the performance of software information protection systems in automated electronic document

management systems. *Bulletin of the Voronezh State Technical University*, 2011, vol. 7, no. 2, p. 27–31 (in Russ.).

18. Smaller V.V., Lesser V.V., Petrova E.V. Obtaining estimates of the effectiveness of the information security system using an automaton model for simulating the functioning of a protected information system. *Information and security*, 2011, vol. 14, no. 1, 125 p. (in Russ.).

19. Anisimov V.G., Selivanov A.A., Anisimov E.G. Methods of assessing the effectiveness of information protection in the system of interdepartmental information interaction in the management of state defense. *Information and space*, 2016, № 4, 76 p. (in Russ.).

20. Zvyagintseva P.A., Kryzhanovskaya O.A. Evaluation of the effectiveness of information security. *Interexpo Geo-Siberia*, 2017, vol. 8, 199 p. (in Russ.).

21. Belyaeva O.V., Grytsyk V.A. Simulation modeling of protection systems. *International Journal of Experimental Education*, 2010, vol. 5, 67 p. (in Russ.).

22. Tsvetkova O.L., Barriers S.A. Simulation modeling of the information security of an organization as a function of its field of activity. *Bulletin of the Don State Technical University*, 2017, vol. 18, no. 4 (91), 116 p. (in Russ.).

Anastasiya S. Goldobina

Master Student, Siberian state University of Geosystems and Technologies, Analyst Engineer LLC «Axxtel-security» 9, Kolkhidskaya st., Novosibirsk, Russian Federation, 630096
Phone: +7-923-220-80-89
Email: nastya-gold09@mail.ru

Julia A. Isaeva

Master Student, Siberian state University of Geosystems and Technologies, LLC «The First Building Fund» 188, Gogoly st., Novosibirsk, Russian Federation, 630112
Phone: +7-913-980-23-09
Email: isaeva.ja@hotmail.com

Valentin V. Selifanov

Federal Service for Technical and Export Control, 2/3, El'tsovskaya st., Novosibirsk, Russian Federation, 630001
Phone: +7-913-905-64-02
Email: sfo1@mail.ru

Aleksandra M. Klimova

Master Student, Department of Computer Science, Novosibirsk State Technical University 136, Nemirovicha-Danchenko st., Novosibirsk, Russian Federation, 630073
Phone: +7-999-466-39-66
Email: aleksandra.kl.15.6@gmail.ru

Pavel S. Zenkin

Postgraduate Student of Tomsk State University of Control Systems and Radioelectronics, 40, Lenin av., Tomsk, Russian Federation, 634050
Phone: +7-906-995-61-15
Email: zenkin.pavel.88@mail.ru