Методы Оценки Защищенности Компьютерных Систем Информационной Поддержки Цифровой Экономики

А. А. Грушо, Н. А. Грушо, М. И. Забежайло, Е. Е. Тимонина

***Аннотация* — В работе разработаны методы оценки защищенности распределенных информационно-вычислительных систем в условиях предположений безопасности с использованием языка диаграмм информационной безопасности. В основе любой оценки защищенности лежит принцип предотвращения ущерба, который может быть нанесен распределенной информационно-вычислительной системе при реализации различных угроз. Предотвращение реализации угроз основано на анализе уязвимостей и учете возможности использования этих уязвимостей.**

В основе диаграммы безопасности всей распределенной информационно-вычислительной системы лежат элементарные диаграммы информационной безопасности. Показано, каким образом можно оценить по построенным элементарным диаграммам информационной безопасности информационную безопасностью всей системы, описываемой глобальной диаграммой информационной безопасности. Множество предположений безопасности строится на основе достижимости уязвимостей распределенных информационно-вычислительных систем. Таким образом, в условиях предположений безопасности обосновывается защищенность всей распределенной информационно-вычислительной системы.

В данной работе рассматривается компромисс между ценностью информации и предположениями о возможностях противника. Ценность информации определяется с помощью метода классификации и величины ущерба в случае утечки или нарушения целостности информации.

При таком подходе существенную роль начинает играть экономический фактор обеспечения информационной безопасности. А именно, целесообразно создавать наименее дорогие системы защиты информации, которые гарантируют защищенность в условиях заданного набора предположений. Рассматриваемый в работе подход определяется требованием массовой цифровизации, которая потребуется для развития малого и среднего бизнеса в условиях цифровой экономики.

***Ключевые слова*— Безопасная архитектура, диаграмма информационной безопасности, информационная безопасность в цифровой экономике, предположения безопасности.**

Статья получена 21 марта 2019.

Работа поддержана РФФИ (проект № 18-29-03081-мк).

А. А. Грушо, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: grusho@yandex.ru).

Н. А. Грушо, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: info@itake.ru).

М. И. Забежайло, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: m.zabezhailo@yandex.ru).

Е. Е. Тимонина, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: eltimon@yandex.ru).

I. Введение

Оценка защищенности распределенных компьютерных систем (РИВС) – часто обсуждаемая проблема [1]–[3]. Существует несколько базовых концепций, в которые укладываются исследования в данной области.

В основе любой оценки защищенности лежит принцип предотвращения ущерба, который может быть нанесен РИВС при реализации различных угроз. Предотвращение реализации угроз основано на анализе уязвимостей и учете возможности использования этих уязвимостей. Основным недостатком этого подхода является необходимость модернизации системы защиты при выявлении новых уязвимостей.

Альтернативой этому подходу является концепция обеспечения защищенности на основе дата-центричности [4].

Глубокий анализ обоих концепций позволяет сделать вывод о том, что в основе этих концепций лежит система предположений относительно возможностей нарушителя безопасности (противника). Понятие «предположение безопасности» включено в стандарт МЭК ИСО 15408 [5]–[7]. В частности, ограниченность возможностей (финансовых и др.) нарушителя безопасности позволяет сделать вывод о том, что определенные уязвимости для него недостижимы. Например, взлом даже простого шифра требует больших вычислительных возможностей и глубоких знаний криптографии. Ясно, что обычному хакеру эти возможности недоступны. Поэтому если сеть в РИВС защищена хорошими криптографическими средствами и протоколами, то можно доказать, что, не имея требуемых возможностей, противник не может вскрыть информацию, передаваемую по сети.

Концепция дата-центрической защиты собственно информации также основана на предположениях. Например, предположения о недоступности резервной копии ценной информации достаточно, чтобы доказать невозможность утечки информации с помощью доступа к ней в резервных копиях.

В данной работе рассматривается компромисс между ценностью информации и предположениями о возможностях противника. Ценность информации определяется с помощью метода классификации и

величины ущерба в случае утечки или нарушения целостности информации.

При таком подходе существенную роль начинает играть экономический фактор обеспечения информационной безопасности. А именно, целесообразно создавать наименее дорогие системы защиты информации, которые гарантируют защищенность в условиях заданного набора предположений. Такой подход определяется требованием массовой цифровизации, которая потребуется для развития малого и среднего бизнеса в условиях цифровой экономики.

II. Общая Схема Системы Защиты

В данной работе используется ранее разработанный авторами язык диаграмм информационной безопасности (ДИБ) [8]. Общая схема системы защиты информации описывается глобальной ДИБ [9] (см. Рис. 1).

Включение механизмов безопасности определяется механизмом управления, которое в свою очередь возникает исходя из опасности ущерба и требований политики безопасности. Опасность оценивается по данным мониторинга системой анализа процессов в РИВС. Глобальная ДИБ распадается на множество локальных ДИБ, описывающих защиту информации в отдельных подсистемах и при воздействии отдельных классов угроз [9] (Рис. 1).

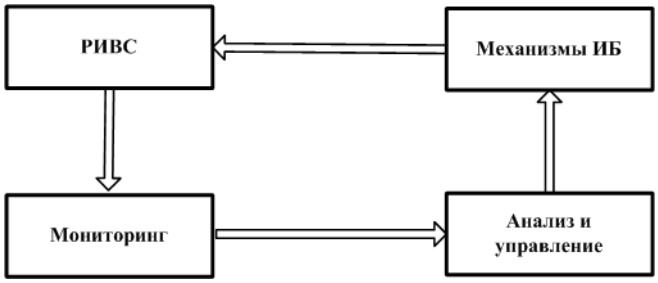

Рис. 1. Глобальная диаграмма подсистемы информационной безопасности

Во введении была отмечена роль понятия предположения безопасности. Предположения безопасности позволяют строить защиту информации, предполагая только угрозы вне предположений. Соответственно глобальная ДИБ учитывает только противодействие угрозам, исключенным предположениями безопасности. Аналогичный подход называется «принятие рисков».

Как правило, предположения безопасности значительно упрощают систему защиты информации. Поэтому защищенность РИВС рассматривается в двух аспектах:

- формирование и обоснование предположений безопасности;
- построение системы информационной безопасности на основе исключения угроз, которые считаются невозможными по предположениям безопасности. предположений безопасности.

Такое деление связано с тем, что оценки достижимости уязвимостей во многих случаях являются очень сложными. Поэтому часто приходится ограничиваться организационными методами защиты или обрабатывать информацию, ценность которой не предполагает наличие возможностей у противника решать задачи высокой сложности. Именно эти уязвимости предполагаются недостижимыми для противника, что и отражается в предположениях безопасности.

Элементарная ДИБ описывает защищенность простейшего действия. Например, рассмотрим элементарное действие, связанное с доступом на чтение субъекта *S* к объекту *O*. Узел мониторинга дает информацию для анализа о запросе субъекта *S* на чтение объекта *O*. Узел анализа рассматривает возможность разрешения этого действия с помощью Access Control List [10] и определяет:

- допустимость запрашиваемого доступа;
- опасность того, что за именем субъекта *S* реально действует другой субъект.

Тогда узел управления *U* сначала запускает ДИБ, описывающую систему аутентификации субъекта *S*. В этой ДИБ мониторинг соответствует получению аутентификационной информации, узел анализа позволяет подтвердить или опровергнуть эту информацию, а узел управления позволяет передать информацию о подтверждении имени субъекта *S* в исходную систему управления действием. Тогда узел управления ДИБ исходного действия через механизм безопасности разрешает доступ на чтение субъекта *S* к объекту *O*.

Ясно, что для всех действий невозможно обеспечить защиту по своим диаграммам информационной безопасности. Поэтому часть действий предполагаются безопасными по предположениям безопасности. Это другие предположения безопасности, и они отличаются от исходных. Однако они играют ту же самую роль, т.е. все действия, которые покрываются этими предположениями, считаются безопасными.

В результате получается глобальный перечень предположений безопасности для РИВС. Корректное описание того перечня нигде не приводится из-за его огромного объема.

Однако существуют методы, агрегирующие предположения безопасности. Как правило, эти методы связаны с изоляцией процессов и подсистем РИВС. Одним из способов изоляции процессов и подсистем РИВС является комплексная виртуализация [11]-[13].

Очевидно, что в РИВС возможна только частичная изоляция. РИВС как система едина и, следовательно, она является связной. Связность обеспечивается через сетевые взаимодействия. Поэтому удобно выделять сеть (сети) как самостоятельную изолированную подсистему.

Изолированными могут быть виртуальные или физические компьютерные системы или их компоненты. Изоляция обеспечивается системой интерфейсов, которые можно считать самостоятельной подсистемой РИВС. Каждый компонент РИВС соединяется с одним или несколькими каналами связи. Однако говорить о том, что интерфейс касается только компонента РИВС и канала связи нельзя, т.к. безопасный интерфейс [14] связан как с отправителем, так и с получателем

информации через сеть связи. Безопасные интерфейсы определяются защищенными протоколами.

Таким образом, оценка защищенности каждой элементарной ДИБ строится на основе четырех параметров:

- возможность увидеть аномалию действий средствами мониторинга, связанными с этой ДИБ;
- возможность системы анализа, связанной с ДИБ, распознать опасность по данным мониторинга;
- возможность системы управления механизмами безопасности, связанной с этой ДИБ, выбрать оптимальный набор действий для предотвращения ущерба;
- возможность механизмов безопасности предотвратить ущерб в тех случаях, которые не попали в предположения безопасности.

Рассмотрим вопрос агрегации элементарных ДИБ в глобальную ДИБ. Эту агрегацию можно реализовать с помощью логических операций. Для каждой элементарной ДИБ, связанной с *i*-ым компонентом РИВС, определим переменную x_i, принимающую значение 1, если реализация ДИБ удовлетворяет требованиям политики безопасности, и обоснована защита информации от угроз, касающихся данной ДИБ. В противном случае переменная $x_i = 0$.

Для каждой пары (*i, j*) компонентов РИВС определена переменная x_{ij}, которая принимает значение 1, если в сети обоснован безопасный интерфейс взаимодействия *i*-го и *j*-го компонентов. Отметим, что сама сеть – это компонент РИВС и также имеет свою переменную.

Все компоненты РИВС, которые считаются безопасными по предположениям, не имеют ДИБ и не имеют соответствующих переменных. Тогда безопасность *y* системы, описываемой глобальной ДИБ, выражается следующей формулой

$$y = \left(\bigwedge_i x_i \right) \wedge \left(\bigwedge_{ij} x_{ij} \right).$$

III. Примеры

A. Figures and Tables

Рассмотрим компьютерную систему, одним из компонентов которой является персональный компьютер, подключенный к интернету. Персональный компьютер через интернет подключается к ряду сервисных систем. Например, это дистанционное банковское обслуживание, взаимодействие с системой коммунального обслуживания и, возможно, др. В системе, состоящей из персональных компьютеров и компьютерной системы, предоставляющей сервисы, обрабатывается ценная информация (уровень High) и открытая информация (уровень Low). Кроме того, из любого персонального компьютера возможен доступ к любым ресурсам интернета.

Если интерфейс персонального компьютера и сервисной компьютерной системы безопасен, то персональный компьютер представляет собой изолированную систему. Рассмотрим возможности сделать эту изолированную систему безопасной в условиях ряда предположений безопасности.

Допустим следующие предположения безопасности.

1) Безопасность аппаратной платформы и контроллеров внешних устройств считаем предположением безопасности. В самом деле, платформа может быть небезопасной только, если там находится вредоносный код, заложенный производителем, или через BackDoor. В силу того, что сумма платежей за обслуживание (банковское, ЖКХ и др.) является небольшой, а участвующие в этих транзакциях электронные документы дублируются различными подсистемами, то данные уязвимости можно считать недоступными для противника (на уровне хакера). Эти аргументы обосновывают данное предположение безопасности.
2) Будем считать, что действия с информацией уровней High и Low пользователь осуществляет на гостевых виртуальных машинах. Для проникновения противника на уровень гипервизора или управляющей операционной системы необходим его высокий уровень квалификации, что является недоступным для противника средней квалификации. Отсюда можно сделать предположение безопасности о том, что гостевые виртуальные машины не могут нелегально взаимодействовать между собой, а также с управляющей ОС и гипервизором.

Для безопасного использования информации уровня High в рассматриваемом примере определим следующую архитектуру (см. Рис. 2).

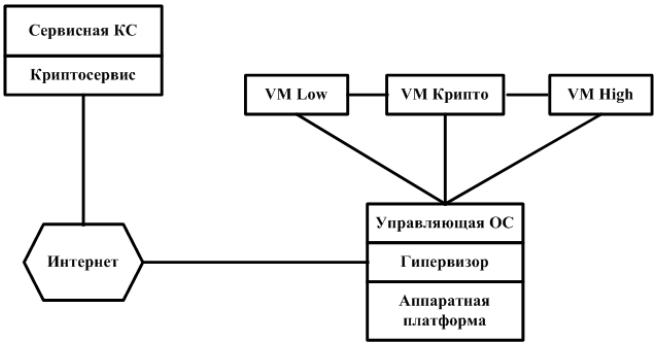

Рис. 2. Архитектура безопасного персонального компьютера Примера 1.

Информация уровня High обрабатывается на гостевой виртуальной машине (далее VM High), связанной с защищенным (с помощью криптографии) разделом памяти персонального компьютера. Для взаимодействия с сервисами используется отдельная гостевая виртуальная машина (далее VM Крипто), на которую при каждом запуске загружается значительно ограниченный образ операционной системы, но достаточный для проведения операций зашифрования и расшифрования и, возможно, с электронной подписью владельца персонального компьютера.

Управление этими функциями осуществляется из гостевой виртуальной машины уровня High.

Третья гостевая виртуальная машина (далее VM Low)

имеет выход в интернет и обрабатывает информацию уровня Low.

Между виртуальной машиной VM Low и виртуальной машиной VM Крипто организован безопасный интерфейс. Этот интерфейс просто реализуется для получаемой из виртуальной машины VM Low информации с помощью проверки правильности расшифрования.

Информация из виртуальной машины VM Крипто поступает в виртуальную машину VM Low в шифрованном виде и преобразуется в сообщение для взаимодействия с сервисной компьютерной системой.

Безопасный интерфейс взаимодействия виртуальной машины уровня High и Сервисной компьютерной системы, обрабатывающей информацию уровня High достигается с помощью криптографической защиты информации, при которой ключ шифрования персонального компьютера также находится в Сервисной компьютерной системе.

В условиях сделанных предположений нелегальный доступ в гостевую виртуальную машину VM High и виртуальную машину VM Крипто из виртуальной машины VM Low невозможен.

Таким образом, рассматривая каждый изолированный компонент построенной архитектуры компьютерной системы, в условиях предположений безопасности обосновывается защищенность всей компьютерной системы.

B. Пример 2

Рассмотрим задачу примера 1 в тех же основных предположениях безопасности 1) и 2) для персонального компьютера. В указанных выше практических задачах для дистанционного банковского обслуживания и обслуживания ЖКХ основная проблема информационной безопасности – сохранение целостности сообщений.

Вместе с тем, криптография служит, в основном, для защиты конфиденциальности и не удобна тем, что в компьютерной системе сервисных услуг необходимо хранить ключи каждого персонального компьютера. Поэтому целесообразно немного изменить политику безопасности и избавиться от шифрования. В этом случае архитектуру изолированной системы можно немного упростить.

По-прежнему будем считать, что имеются три виртуальные машины VM High, VM Крипто и VM Low, однако функционал виртуальной машины VM High и виртуальной машины VM Крипто немного изменим. Электронную подпись перенесем в виртуальную машину VM High. Отметим, что общение с системой дистанционного банковского обслуживания и системой обслуживания ЖКХ осуществляется на языках шаблонов. Такие языки являются «бедными» и в них легко проверяется отсутствие вредоносных вставок и вредоносных воздействий [14]. Поэтому в функционале третьей гостевой виртуальной машины криптография замещается программой проверки принадлежности получаемых данных к указанным «бедным» языкам.

Итак, информация, исходящая из виртуальной машины VM High, должна подписываться электронной подписью, а входящая в нее информация должна быть проверена на предмет отсутствия вредоносных вставок. Отметим, что в стандартном Web-интерфейсе данные защищаются с помощью протоколов SSL и TLS. Таким образом, обеспечивается безопасный интерфейс с сервисной компьютерной системой.

3) Отсюда следует, что в сделанных предположениях безопасности обеспечивается защищенность изолированного персонального компьютера в соответствии с требованиями политики безопасности.

IV. Заключение

В работе разработаны методы оценки защищенности в условиях предположений безопасности с использованием языка диаграмм информационной безопасности. Показано, каким образом можно легко связать обеспечение информационной безопасности в элементарных ДИБ с информационной безопасностью всей системы глобальной ДИБ в условиях предположений безопасности.

Множество предположений безопасности строится на основе оценки достижимости уязвимостей и не входит в задачи данной работы. Для оценок достижимости уязвимостей обычно используются специальные базы данных, например, CERT и др. Однако даже с использованием этой информации оценка достижимости найденных уязвимостей является сложной самостоятельной задачей.

Библиография

[1] А. А. Грушо, М. И. Забежайло, А. А. Зацаринный, “Контроль и управление информационными потоками в облачной среде,” *Информатика и ее применения*, Т. 9, № 4, С. 91–97, 2015.

[2] A. A. Grusho, E. E. Timonina, S. Y. Shorgin, “Modelling for ensuring information security of the distributed information systems,” in *Proc. of 31th European Conference on Modelling and Simulation*,” 2017, pp. 656–660.

[3] А. А. Грушо, Н. А. Грушо, Е. Е. Тимонина, “Оценка защищенности в безопасных архитектурах распределенных информационных систем,” *Системы и средства информатики*, Т. 26, № 4, С. 31–37, 2016.

[4] A. Woody, *Enterprise Security: A Data-Centric Approach to Securing the Enterprise*. Birmingham, UK: Packt Publishing, 2013.

[5] ISO/IEC 15408-1:2009. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, 2009. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[6] ISO/IEC 15408-2:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components, 2008. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[7] ISO/IEC 15408-3:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components, 2008. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[8] А. А. Грушо, Н. А. Грушо, Е. Е. Тимонина, “Синтез архитектуры информационной безопасности в распределенных информационно-вычислительных системах,” *Проблемы информационной безопасности. Компьютерные системы*, № 2, С. 23–30, 2017.

[9] A. Grusho, N. Grusho, M. Levykin, E. Timonina, “Analysis of information security of distributed information systems,” in *Proc. of 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops* (ICUMT 2017), 2017, pp. 96–100.

[10] А. А. Грушо, Э. А. Применко, Е. Е. Тимонина, *Теоретические основы компьютерной безопасности*. Москва: Академия, 2009.

[11] А. А. Грушо, Н. А. Грушо, Е. Е. Тимонина, С. Я. Шоргин, “Возможности построения безопасной архитектуры для

динамически меняющейся информационной системы," *Системы и средства информатики*, Т. 25, № 3, С. 79–93, 2015.

[12] А. А. Грушо, Н. А. Грушо, М. В. Левыкин, Е. Е. Тимонина, "Безопасные архитектуры распределенных информационно-вычислительных систем на основе комплексной виртуализации," *Проблемы информационной безопасности. Компьютерные системы*, № 4, С. 32–35, 2016.

[13] Н. А. Грушо, В. В. Сенчило, "Моделирование безопасных архитектур распределенных информационно-вычислительных систем на основе комплексной виртуализации," *Системы и средства информатики*, Т. 28, № 1, С. 110–122, 2018.

[14] А. А. Грушо, Д. В. Смирнов, "Защита бизнес-логики от атак нулевого дня," *Системы и средства информатики*, Т. 26, № 3, С. 61–73, 2016.

Methods of Estimation of Security of Computer Systems of Information Support of Digital Economy

A. A. Grusho, N. A. Grusho, M. I. Zabezhailo, E. E. Timonina

***Abstract* — In the paper the methods of estimation of security of the distributed information systems in the conditions of assumptions of security with usage of language of diagrams of information security are developed. The principle of prevention of damage which can be caused to the distributed information system at realization of various threats is the cornerstone of any assessment of security. Prevention of realization of threats is based on the analysis of vulnerabilities and accounting of a possibility of usage of these vulnerabilities.**

Diagram of information security of the whole distributed information system is based on elementary diagrams of information security. It is shown how it is possible to estimate an information security of the whole system described by the global diagram of information security on the basis of elementary diagrams of information security. The set of security assumptions is constructed on the basis of ways to vulnerabilities of the distributed information systems. Thus, in the conditions of security assumptions the security of all distributed information system is proved.

In this paper the compromise between the value of information and the assumptions of malicious opportunities is considered. The value of information is estimated on the basis of classification and size of damage in case of leak or violation of integrity of information.

At such approach the economic factor of ensuring information security begins to play an essential role. Namely, it is expedient to create the least expensive systems of information security which guarantee security in the conditions of the set of security assumptions. The approach considered in the paper is defined by the requirement of mass digitalization which will be required for development of small and medium business in the conditions of digital economy.

***Keywords* — Secure architecture, diagram of information security, information security in digital economy, security assumptions.**

REFERENCES

[1] A. A. Grusho, M. I. Zabezhailo, A. A. Zatsarinny, “Information flow monitoring and control in cloud computing environment,” *Informatics and Applications*, vol. 9, no. 4, pp. 91–97, 2015.

[2] A. A. Grusho, E. E. Timonina, S. Y. Shorgin, “Modelling for ensuring information security of the distributed information systems,” in *Proc. of 31th European Conference on Modelling and Simulation*,” 2017, pp. 656–660.

[3] A. A. Grusho, N. A. Grusho, E. E. Timonina, “Security evaluation in secure architecture of distributed information systems,” *Systems and means of informatics*, vol. 26, no. 4, pp. 31–37, 2016.

[4] A. Woody, *Enterprise Security: A Data-Centric Approach to Securing the Enterprise*. Birmingham, UK: Packt Publishing, 2013.

[5] ISO/IEC 15408-1:2009. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, 2009. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[6] ISO/IEC 15408-2:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components, 2008. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[7] ISO/IEC 15408-3:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components, 2008. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[8] A. A. Grusho, N. A. Grusho, E. E. Timonina, “Information Security Architecture Synthesis in Distributed Information Computation Systems,” *Automatic Control and Computer Sciences*, vol. 51, no. 8, pp. 799–804, 2017.

[9] A. Grusho, N. Grusho, M. Levykin, E. Timonina, “Analysis of information security of distributed information systems,” in *Proc. of 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops* (ICUMT 2017), 2017, pp. 96–100.

[10] A. A. Grusho, Ed. A. Primenko, E. E. Timonina, *Theoretical bases of computer security*. Moscow: Publishing Center "Academy", 2009.

[11] A. Grusho, N. Grusho, S. Shorgin and E. Timonina, “Possibilities of Secure Architecture Creation for Dynamically Changing Information Systems,” *Systems and means of informatics*, vol. 25, no. 3, pp. 78–93, 2015.

[12] A. A. Grusho, N. A. Grusho, M. V. Levykin, E. E. Timonina, “ Secure architecture of distributed information systems on the basis of integrated virtualization,” *Problems of information security. Computer systems*, № 4, С. 32–35, 2016.

[13] N. A. Grusho, V. V. Senchilo, “Modeling of secure architecture of distributed information systems on the basis of integrated virtualization,” *Systems and means of informatics*, vol. 28, no. 1, pp. 110–122, 2018.

[14] A. A. Grusho, D. V. Smirnov, “Protection of business logic against zero day attacks,” *Systems and means of informatics*, vol. 26, no. 3, pp. 61–73, 2016.

Alexander A. Grusho, Professor (1993), Doctor of Science in physics and mathematics (1990). He is principal scientist at Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences and Professor of Moscow State University.

Research interests: probability theory and mathematical statistics, information security, discrete mathematics, computer sciences.

Nick A. Grusho has graduated from the Moscow Technical University. He is Candidate of Science (PhD) in physics and mathematics. At present he works as senior scientist at Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences.

Research interests: probability theory and mathematical statistics, information security, simulation theory and practice, computer sciences.

Michael I. Zabezhailo has graduated from the Institute of Physics and Technology and gained the Candidate degree (PhD) in theoretical computer science (1983). He is Doctor of Science in physics and mathematics (2016). Now he works as Head of laboratory in Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences.

Research interests: mathematical foundations of artificial intelligence, reasoning modeling, information security, theoretical computer sciences.

Elena E. Timonina has graduated from the Moscow Institute of Electronics and Mathematics and obtained the Candidate degree (PhD) in physics and mathematics (1985). She is Doctor in Technical Science (2005), Professor (2007). Now she works as leading scientist in Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences.

Research interests: probability theory and mathematical statistics, information security, cryptography, computer sciences.