УДК 681.3.067

И.А. Носаль

МЕТОД ОБОСНОВАНИЯ МЕРОПРИЯТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНО-ВАЖНЫХ ОБЪЕКТОВ

Носаль И.А. **Метод обоснования мероприятий информационной безопасности социально-важных объектов.**

Аннотация. Рассматривается задача обоснования целесообразных мероприятий информационной безопасности социально важных объектов. Для ее решения предлагается усовершенствованный метод, ориентированный на более гибкий учет особенностей текущих ситуаций. Предложен ряд новых марковских моделей защищаемых процессов и возможных угроз применительно к структурам Пенсионного фонда. Приведены результаты моделирования.

Ключевые слова: метод, модели, информационная безопасность, обоснование мероприятий.

Nosal I.A. **Method of Information Security Measures Substantiation for Socially Important Objects.**

Abstract. The justification of appropriate information security measures of socially important objects is considered. To solve it an improved method that focuses on a more flexible accounting features of the current situation is provided. The set of new Markov models protected processes and possible threats in relation to the structures of the Pension Fund is offered. The simulation results are given.

Keywords: method, models, information security, substantiation and feasibility of measures.

1. Введение. Под социально-важным объектом (СВО) в данной работе подразумевается социально-ответственный институт, не являющийся при этом органом государственной власти. Основной целью СВО является предоставление государственных услуг населению (обеспечение прав граждан), нарушение или прерывание работы которого может привести к нарушению нормальной жизнедеятельности населения.

Примеры таких организаций – Фонд социального страхования, Фонд обязательного медицинского страхования, Пенсионный фонд Российской Федерации. Все эти организации по форме образования и расходования денежных средств являются внебюджетными государственными фондами, имеют схожие цели, задачи, принципы работы, административно-управленческую структуру и являются крупнейшими операторами персональных данных.

Информационная безопасность для социально-важных объектов – это одно из главнейших условий надлежащего предоставления ими качественных государственных услуг населению.

Она является частью системы национальной безопасности и внутренней политики, а также влияет на безопасность личности, общества и государства [1]. Для государства обеспечение информационной безопасности СВО гарантия надлежащего исполнения своих функций (обязательств перед населением).

Для обеспечения информационной безопасности (ИБ) СВО предоставляется не много инструментов и ресурсов, однако предъявляется достаточно требований, как со стороны государства, так и со стороны населения. И, поскольку, каждый субъект этой системы имеет свой круг интересов и задач, которые он решает с помощью СВО, а значит разнятся наборы требований, которые предъявляются к ИБ СВО. Поэтому система информационной безопасности СВО остро нуждается в удобном, эффективном и надежном методе поиска и обоснования мероприятий ИБ. Необходимо также разработать систему моделей угроз информационной безопасности актуальных для деловых процессов СВО, учитывая широкий круг условий, отражающих объективные закономерности.

Известны многочисленные экономические и математические методы решения этой задачи [2–8]. В большинстве случаев применяются методы, базирующиеся на статистических данных и экспертных оценках с применением различного математического аппарата [9–11]. Но даже методы, использующие хорошо адаптированные для этих целей математические инструменты оценки, такие как нечеткие множества, нечеткая логика и искусственные нейронные сети [12–15], в конечном счете, опираются на опыт и субъективные мнения экспертов. Это влечет за собой все недостатки и проблемы использования экспертных методов оценивания [16–18].

Следует также упомянуть о требованиях государственных регуляторов в области ИБ [19–23], отраслевых и международных стандартах ИБ [24–27]. Все они в той или иной мере раскрывают подходы, которыми должна руководствоваться организация при выборе мероприятий ИБ. Чаще предлагают, основываясь на предложенной методике, выбрать из ограниченного списка соответствующие контрмеры, а иные и вовсе тоталитарно требуют выполнения конкретных мер. В итоге, при отсутствии высококвалифицированных специалистов, которые смогут эффективно и с пониманием внедрить требования стандарта в существующую систему, обоснование мероприятий ИБ сводится к тому, что их выполнение обязательно, со всеми вытекающими последствиями. К эти последствиям относятся: нарушения или затруднения деятельности СВО, увеличение нагрузки на персонал, усложнение документооборота, дублирование документации, мер и методов защиты. Как показали результаты расчетов, опубликованные в работе [28], даже «подогнанный» ISO/IEC 27001 – 2006 (универсальный стандарт по ИБ для организаций любых типов, размеров, отраслей) не отражает всей картины, не охватывает

уникальные для конкретной организации детали и не гарантирует адекватность и обоснованность выстроенной системы защиты.

Главный недостаток всех перечисленных методов в том, что область их использования ограничена и распространяется либо на противодействие именно техническим и сетевым атакам, либо основывается исключительно на оценке экономической эффективности мероприятий. В первом случае объектом защиты является информационная система. Не рассматривается безопасность всего объекта информатизации, непрерывность деловых процессов, не учитываются интересы владельцев бизнеса и информации. Во втором случае не учитывается широкий ряд других важных параметров: удобство для пользователей, интегрируемость в текущую инфраструктуру, контролируемость и т.п. Выстраиваемая таким образом система обеспечения ИБ не в полной мере обладает требуемыми свойствами: системностью, интегрируемостью, комплексностью, прозрачностью, адекватностью, оптимальностью и подконтрольностью.

Поэтому необходимо совершенствование соответствующего научно-методического аппарата. Требуется разработка более точного метода обоснования целесообразности принятия решений и мероприятий ИБ, учитывающего особенности объекта защиты, его деловых процессов, внешней и внутренней среды функционирования, позволяющего повысить уровень информационной безопасности СВО в целом.

Необходимо решить научно-техническую задачу по разработке новых моделей и методов обоснования мероприятий информационной безопасности СВО, повышающих эффективность функционирования этих объектов.

2. Метод гибкого обоснования мероприятий ИБ. Учитывая ранее полученные результаты [29, 30] в интересах решения сформулированной задачи предлагается уточненный метод гибкого обоснования мероприятий ИБ СВО.

В обобщенном виде этот метод можно представить в виде следующей последовательности шагов:

Ш1. Анализ защищаемого процесса, выделение ключевых его особенностей.

Ш2. Анализ текущего состояния ИБ на защищаемых участках, уточнение или пересмотр целей защиты информации, условий их достижения.

Ш3. Разработка нескольких альтернативных моделей защищаемого процесса с учетом того или иного набора мероприятий

ИБ. В частности, опираясь на предельную теорему теории вероятностей для потоков событий, защищаемый процесс можно рассматривать как марковский. В этом случае такие модели могут быть представлены в виде соответствующих процессу графов состояний.

Ш4. Формулировка условий оценивания эффективности мероприятий ИБ (требований к итоговой безопасности процесса, входным и выходным экономическим показателям, ограничений по времени выполнения мероприятия или времени простоя и т.п.) на качественном уровне.

Ш5. Разработка адекватной оптимизационной модели ИБ.

Ш6. Определение текущих параметров переходов моделируемого процесса из одних состояний в другие.

Ш7. Задание начальных и интересующих состояний процесса.

Ш8. Расчет вероятностей нахождения процесса в интересующих состояниях для каждого из альтернативных наборов мероприятий и определение значений других показателей эффективности, входящих в выбранную оптимизационную модель. В качестве таких показателей могут выступать временные и материальные затраты, интегральные потери ценности защищаемой информации на заданном интервале времени, математическое ожидание удовлетворенных заявок и другие.

Ш9. Проверка выполнимости условий, связанных с этими показателями.

Ш10. Поиск экстремума основного показателя эффективности (целевой функции) на заданном наборе альтернативных мероприятий, удовлетворяющих условиям задачи.

Ш11. Принятие в качестве целесообразного того мероприятия, при котором достигнут экстремум целевой функции.

При разработке марковской модели защищаемого процесса с учетом мероприятий ИБ в виде графа состояний следует исходить из целесообразного уровня формализации этого процесса. Излишняя детализация влечет за собой повышение затрат на разработку модели процесса и определение ее параметров. Грубая формализация позволяет оперативно получать интересующие оценки, однако не обеспечивает необходимой точности результатов. Для определения целесообразного уровня формализации анализируемых процессов применим метод экспертных оценок.

Для построения такого графа, в соответствии с предлагаемым подходом, следует, прежде всего, определиться с уровнем масштабирования модели, интересующими результатами и изучить объект моделирования – защищаемый деловой процесс, затем

выделить:

– основные этапы его выполнения;

– задействованные ресурсы;

– определить есть ли в процессе стандартные ответвления, связанные с принятием решений;

– какие могут быть ошибки, сбои в выполнении процесса;

– какие атаки на процесс актуальны и к каким последствиям (нарушениям) на каких этапах могут привести;

– какие из нарушений связаны с защищаемыми ресурсами, какие с нарушениями требований, какие с человеческими ошибками.

На основании указанных выше данных могут быть выделены последовательности состояний, в которых может находиться процесс, и возможные переходы между ними. Следует уделить построению модели процесса в виде графа состояний наибольшее внимание, поскольку именно этим выбором будет определяться область получаемых результатов и характер возможных выходных данных.

Следующим важным моментом является задание исходных данных, условий поиска. Одновременно в качестве них могут выступать следующие параметры:

– наличие тех или иных связей и переходов из состояния в состояние;

– интенсивности переходов из состояния в состояние;

– вероятности нахождения в рассматриваемых состояниях на момент $t = 0$;

– затраты на реализацию защиты;

– ущерб от реализации угрозы и другие.

В качестве входных данных интенсивности переходов из состояния в состояние и ограничения по времени могут задаваться, основываясь на регламенте моделируемого делового процесса, статистических оценках и требуемых значениях показателей.

Некоторые из интенсивностей переходов зависят от особенностей мероприятий ИБ (к примеру, от частоты проведения проверок). Эта неопределенность может быть исключена в ходе разработки оптимизационных моделей ИБ, поскольку эти интенсивности становятся искомыми параметрами. В другом случае, они могут быть определены путем сбора и обработки статистических данных. В ряде случаев, когда известны начальные и конечные состояния процесса на некотором интервале времени определение исходных интенсивностей осуществимо также путем подбора параметров с использованием метода наименьших квадратов.

Важным моментом моделирования является распознавание

состояний, в которых система может находиться в исходный момент времени.

Для расчета вероятностей нахождения процесса в интересующих состояниях в соответствии с построенным графом составляется система дифференциальных уравнений. Затем она разрешается относительно заданных начальных и интересующих состояний.

В соответствии с этим методом выбор конкретной оптимизационной модели должен осуществляться, исходя из наибольшего соответствия ее реальной ситуации с учетом преследуемых целей, текущих условий и неопределенностей.

Новизна этого метода обоснования мероприятий ИБ СВО состоит в особенностях его отдельных этапов, в возможностях гибкого реагирования на возникающие ситуаций. При обосновании мероприятий ИБ СВО предлагается учитывать более широкий круг возможных условий - ограничений, свойственных не только ИБ СВО, но и самому процессу обоснования. При практическом использовании этого метода возможно накопление множества готовых для использования моделей целесообразных мероприятий ИБ, ориентированных на типовые ситуации.

3. Модели защищаемых процессов социально-важных объектов. Для реализации рассмотренного метода предлагается использовать следующие типовые модели защищаемых процессов, характерных для СВО, применительно к структурам Пенсионного фонда (рисунок 1). На рисунке 1*a* приняты обозначения: 1 – начальное состояние (поступление заявления); 2 – прием и проверка правильности оформления представленных документов; 3 – возврат заявления без регистрации и разъяснение причины отказа; 4 – регистрация заявления; 5 – заявление ошибочно зарегистрировано. Согласно рисунку 1*b* выделены: 1 – начальное состояние (направление запроса в другие органы (истребование документов); 2 – поступление необходимых документов; 3 – принято корректное решение об удовлетворении заявления/отказе в приеме заявления; 4 – документы не получены/получены поддельные документы, 5 - решение принято не верно). Графу на рисунке 1c свойственны состояния: 1 – принято решение об удовлетворении заявления; 2 – произведен расчет сумм, полагающихся к выплате в соответствии с последним принятым решением; 3 – выплатные документы сформированы; 4 – выплатные документы приняты на выплату; 5 – в выплатные документы внесены несанкционированные изменения, 6 – на выплату приняты выплатные документы с несанкционированными изменениями. На рисунке 1*d*

приняты обозначения: 1 – выплатные документы приняты на выплату; 2 – произведена проверка принятых на выплату документов; 3 – выплата произведена в соответствии с законодательством; 4 – выплата произведена некорректно (поддельные списки направлены в банк, платежные документы с не корректными суммами направлены в Казначейство).

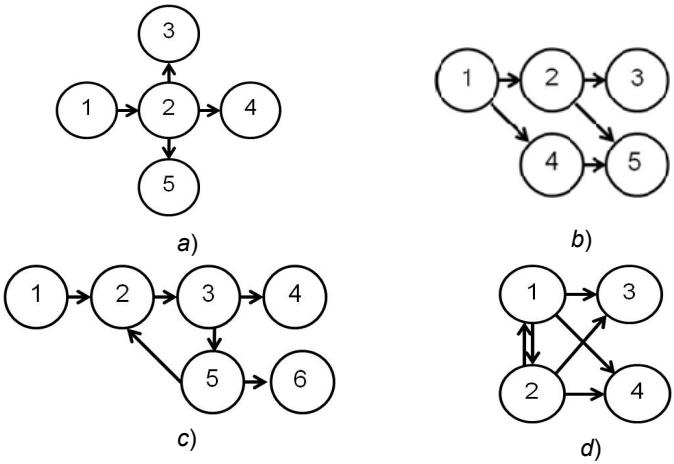


Рис. 1. Типовые модели защищаемых процессов в структурах Пенсионного фонда: *a* - модель приема документов; *b* - модель принятия решений по назначению пенсий; *c* - модель перерасчета выплат; *d* - модель осуществления выплат

Модели на рисунке 1 представлены в виде графов состояний. Дугам этих графов могут быть поставлены в соответствие интенсивности переходов из состояния в состояние. Они в свою очередь могут задаваться, исходя из регламента моделируемого делового процесса. Для каждой из этих моделей свойственна соответствующая система дифференциальных уравнений.

Поясним модели на рисунке 1. Согласно модели на рисунке 1*c*, чем меньше процесс находится в состоянии 6, тем выше уровень ИБ. Также уровень ИБ зависит от изменения параметров переходов из состояния 3 в состояния 4 и 5, и из состояния 5 в состояния 2 и 6. Увеличение времени перехода из состояния 5 в состояние 6 связано с улучшением эффективности защитных мер. Заметим, что в случае предоставления пользователям неоптимального набора прав доступа, граф состояний может обладать еще одним ребром перехода из состояния 2 в состояние 5, поскольку несанкционированные

изменения могут оказаться не исправленными.

Точно такая же ситуация с моделью на рисунке 1*c*. Актуальной угрозой для этого процесса является возможность некорректной проверки направленных на выплату документов и отправки документов с поддельными данными. Вероятность этой угрозы можно снизить только контролем выдачи ролей и прав доступа на ввод и проверку данных. В случае, когда процесс организован по всем требованиям безопасности, то отсутствуют какие-либо искаженные данные. Переход из состояния 2 в состояние 4 исключен и наоборот. При этом, уровень ИБ зависит от изменения параметров переходов в состояния 3 и 4.

Новизна этих моделей состоит в структурах предложенных графов состояний, отражающих объективные закономерности формализуемых процессов, применительно к Пенсионному фонду.

Представленные на рисунке 1 модели могут быть использованы в качестве типовых при обосновании целесообразных мероприятий ИБ на СВО. Однако кроме них необходимо иметь также модели процессов нарушения ИБ СВО.

4. Модели процессов нарушения ИБ СВО. В качестве таких типовых моделей могут выступать графы состояний, показанные на рисунке 2.

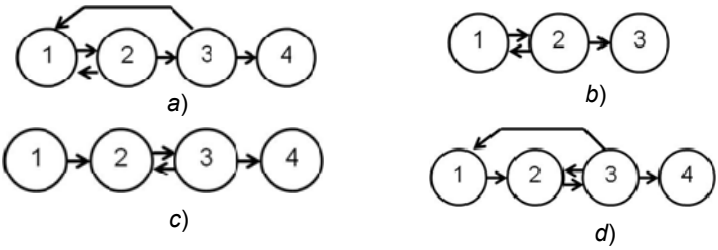


Рис. 2. Типовые модели нарушения информационной безопасности, применительно к структурам Пенсионного фонда: *a* - модель подмены источника (поставщика) данных, атака «masquerading»; *b* - модель перехвата передаваемых данных, атака «man in the middle» (компрометация канала связи); *c* – модель нарушения целостности данных; *d* - модель подачи поддельных данных на входе

В качестве вершин графа на рисунке 2*a* выделены: 1 – злоумышленник отследил обращения СВО к внешнему источнику (поставщику) данных; 2 – запрос СВО к внешнему источнику данных перехвачен; 3 – злоумышленник замаскировался и направил ответ от имени источника; 4 – некорректные данные

приняты (нарушение аутентичности и целостности данных). На рисунке 2*b*: 1 – злоумышленник отследил обращения СВО к внешнему источнику (поставщику) данных; 2 – злоумышленник перехватил/вычислил/подобрал ключевую/парольную информацию; 3 – НСД к защищаемым информационным ресурсам получен. Согласно рисунку 2*c*: 1 – злоумышленник получил доступ к данным; 2 – злоумышленник внес изменения в данные; 3 – данные проверены на подлинность; 4 – некорректные данные приняты. Для модели на рисунке 2*d* характерны следующие состояния процесса: 1 – злоумышленником сформированы поддельные документы; 2 – поддельные документы поданы в СВО; 3 –поддельные документы приняты СВО; 4 – деловой процесс нарушен.

Согласно рисунку 2 применительно к структурам Пенсионного фонда, как СВО, неправомерное начисление пенсии из-за нарушений ИБ может произойти:

- на уровне персонифицированного учета за счет подачи в СВО поддельных документов, на протяжении всей жизни;
- путем подделки дополнительных документов, влияющих на социальные надбавки независимые от пенсионного капитала;
- внесением изменений непосредственно в суммы выплаты пенсии и другими способами.

Возможны четыре типа атак на процесс назначения и выплаты пенсий (НВП). Первая – подделка документов еще до момента их подачи в СВО, таким образом, чтобы создать эффект «мертвых душ». Тогда ни на одном из этапов невозможно будет обнаружить, что такого человека фактически не существует. Данную угрозу реализует внешний нарушитель. Здесь идет нарушение аутентичности информации (подмена персональных данных – одного человека выдают за другого);

Вторая – подделка документов на этапе проверки правильности заявления и сопутствующих документов, когда оператор принимает к регистрации оформленные с нарушениями документы. Это может быть как заявитель, так и ошибка или содействие оператора, принимающего документы.

Третья – подделка документов на этапе ответа на запрос, когда в СВО приходят искаженные данные о лице, подавшем заявление, что провоцирует неверное определение прав на предоставление госуслуги и неправомерное принятие решения об удовлетворении или отказе в услуге. Эта угроза может осуществляться как внутренними нарушителями (с которыми реализуется взаимодействие в рамках оказания услуги, инсайдеров в СВО), так внешним

злоумышленниками с помощью технического перехвата данных – атака “man in the middle”.

Четвертая – это неправомерная корректировка сумм выплат перед направлением списков в банки. Последняя в этом списке, но первая по количеству инцидентов атака, реализуется внутренним нарушителем. К данной категории нарушений следует отнести также подделку данных (не только сумм выплат, а любых данных) уже непосредственно при передаче в банки и расчетный центр с использованием атаки "man in the middle”.

Общими, для процессов обеспечения ИБ являются противоречия между: уровнем защищенности и доступности информационных ресурсов; уровнем защищенности и затратами на обеспечение ИБ; затратами на обеспечение ИБ и возможным информационным ущербом со стороны несанкционированных пользователей и другие.

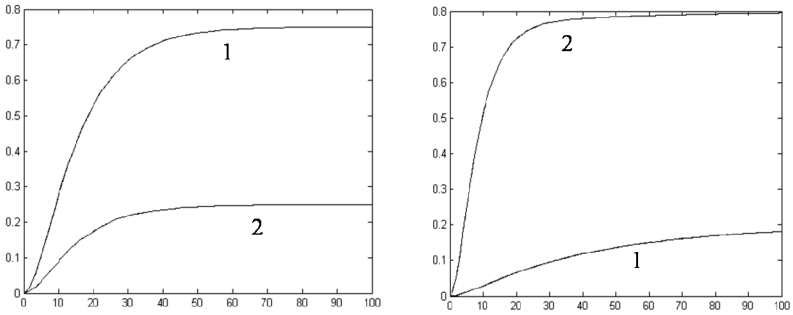
Предложенные модели нарушения ИБ СВО расширяют взгляды на возможные угрозы процессам, свойственным структурам Пенсионного фонда.

5. Результаты моделирования. В интересах подтверждения справедливости предложенных теоретических положений по обоснованию ИБ на СВО проводилось математическое моделирование. Исходные данные по параметрам моделей, отраженных на рисунках 1, 2, формировались автором с учетом ранее накопленного опыта практической деятельности в сфере ИБ на СВО.

В результате такого моделирования с применением пакета прикладных программ MatLab применительно к графам на рисунках 1*b* и 1*c* , были получены зависимости, приведенные на рисунках 3*a*, *b* и 4*a*, *b*, соответственно.

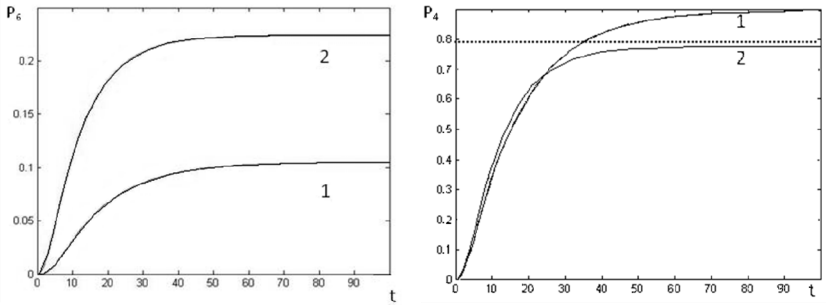
Для анализа был выбран конечный промежуток времени от нуля до 100 минут, поскольку в дальнейшем функции не меняли своего поведения. Все рассчеты были произведены при начальных состояниях [1,0,0,0,0].

Сравнивая рисунки 3*a* *и* 3*b*, наблюдаем прямо пропорциональную картину изменения вероятностей принятия правильного и не правильного решений в зависимости от наличия и отсутствия защищаемых информационных ресурсов (ЗИР). Эти графики наглядно показывают насколько важна роль ЗИР, достоверных входных данных, документов, необходимых для процесса назначения и расчета пенсии.



a) *b*)

Рис. 3. Зависимость вероятности корректного (кривая 1) и некорректного (кривая 2) принятия решений от времени при наличии (*a*) и отсутствии защищаемых информационных ресурсов (*b*)



a) *b*)

Рис. 4. Зависимости вероятности некорректной (a) и корректной (b) выплаты пенсии от времени для наборов мероприятий защиты с разделением прав (кривая 1) доступа и без их разделения (кривая 2)

Согласно рисункам 3 а,б на момент времени, равный 20-ти минутам, вероятность принятия верного решения равна 0,5282 и 0,06561, соответственно. Таким образом, можно говорить о том, что правильно полученные документы, которые находятся в ведомстве других организаций, имеют вклад, оказываемый на правильность принятого решения, равный 46%. Интересно также наблюдать характер роста вероятности принятия правильного решения в обоих вариантах. В первом случае первые 30 минут наблюдается экспоненциальный рост. Последующие 0,5 часа рост продолжается, но значительно медленнее, и практически прекращается на 60-той минуте. В итоге достигается значение вероятности, равное 0,8. Во втором случае вероятность принятия верного решения возрастает

постоянно с практически неизменной скоростью и на наблюдаемом промежутке не превышает 0,2.

Для примера обоснования мероприятий ИБ применительно к процессам Пенсионного фонда в соответствии с моделью в виде графа состояний на рисунке 1*с* характерны несколько другие зависимости от времени вероятностей нахождения его в состояниях P_6 и P_4.

Из анализа рисунка 4 видно, что мероприятия защиты с разделением прав доступа являются более эффективными, чем со смешением этих прав.

Оптимизацию мероприятий ИБ, в частном случае, можно осуществлять, исходя из минимизации вероятности некорректной выплаты пенсий при различных дополнительных условиях – ограничениях.

Для расчета ценности защищаемых информационных ресурсов в рамках предлагаемого метода можно использовать известную модель [30].

Таким образом, результаты моделирования показывают, что предлагаемые решения позволяют успешно обосновывать мероприятия ИБ.

7. Заключение. Для обоснования мероприятий ИБ СВО предлагается более полно учитывать особенности текущих ситуаций. В соответствии с этими ситуациями рекомендуется гибко разрабатывать модели целесообразных мероприятий ИБ. Отличительной особенностью предлагаемого метода выступает ориентированность его на использование для формализации ИБ СВО математического аппарата марковских процессов. Учитывая, что на все случаи невозможно заранее разработать целесообразные модели мероприятий ИБ СВО, следует опираться на комплексы типовых моделей, которые при необходимости можно легко корректировать. При разработке марковских моделей исследуемых процессов следует исходить из целесообразного уровня их формализации. Излишняя детализация влечет за собой повышение затрат на разработку модели и определение ее параметров. Грубая формализация позволяет оперативно получать интересующие оценки, однако не обеспечивает необходимой точности результатов.

Предложенные в статье новые типовые марковские модели защищаемых процессов и возможных угроз могут быть успешно применимы в практической деятельности специалистов по защите информации при обосновании целесообразных мероприятий ИБ СВО.

Литература

1. *Юсупов Р.М.* Наука и национальная безопасность. 2-е издание, переработанное и

дополненное // СПб.: Наука. 2011. 369 с.
2. *Петренко С.А., Попов Ю.И.* Оценка затрат на информационную безопасность // Конфидент. 2003. №1(49). С. 68–73.
3. *Обухов А.А.* Диагностика необходимости инвестирования в безопасность в современном предпринимательстве и формирование на ее основе рекомендаций // Вестник Омского университета. Серия «Экономика». 2013. №3. С. 78–84.
4. *Рытов М.Ю., Рудановский М.В.* Управление безопасностью информационных технологий на основе методов когнитивного моделирования // Информационная безопасность. 2010. №4. С. 579–582.
5. *Ажмухамедов И.М., Ханжина Т.Б.* Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник АГТУ. 2011. № 1 С. 185–190.
6. *Бирюков Д.Н., Ломако А.Г.* Подход к построению системы предотвращения киберугроз // Проблемы информационной безопасности. Компьютерные системы. 2013. №2. С. 13–19.
7. *Крамаров Л.С., Бабенко Л.К.* Обнаружение сетевых атак и выбор контрмер в облачных системах // Известия ЮФУ. Технические науки. 2013. №12(149). С. 94–101.
8. *Абрамов Е.С., Кобилев М.А., Крамаров Л.С., Мордвин Д.В.* Использование графа атак для автоматизированного расчета мер противодействия угрозам информационной безопасности сети // Известия ЮФУ. Технические науки. 2014. №2(151). С. 92–100.
9. *Трофимов И.Б.* Методы оценки информационной безопасности предприятия на основе процессного подхода:дис. канд. техн. наук // Санкт-Петербург. 2010. 134 с.
10. *Ажмухамедов И.М., Ханжина Т.Б.* Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник АГТУ. 2011. №1. С. 185–190.
11. *Миронов В. В., Носаль И.А.* Моделирование и оценка системы обеспечения информационной безопасности на примере ГОУ ВПО «СыктГУ» // Информация и безопасность. 2011. № 2. С. 209–211.
12. *Васильев В.И., Савина И.А., Шарипова И.И.* Построение нечетких когнитивных карт для анализа и управления информационными рисками вуза // Вестник УГАТУ. 2008. №2. Т. 10. С. 199–209.
13. *Schneier B.* Attack Trees // Dr. Dobb's Journal. 1999. vol. 24. no. 12. pp. 21–29.
14. *Sodiya A. S., Onashoga S. A., Oladunjoye B. A.* Threat Modeling Using Fuzzy Logic Paradigm // Issues in Informing Science and Information Technology. 2007. vol. 4. pp. 53–61.
15. *Чечулин А.А.* Методика оперативного построения, модификации и анализа деревьев атак // Труды СПИИРАН. СПб: Наука. 2013. №3 (26). С.40–55.
16. *Карпеев Д.О.* Исследование и развитие методического обеспечения оценки и управления рисками информационных систем на основе интересо-ориентированного подхода: дис. канд. техн. наук // Воронеж. 2009. 171 с.
17. *Корнилова А.Ю,. Палей Т.Ф.* Проблемы применения методов экспертных оценок в процессе экономического прогнозирования развития предприятия // Проблемы современной экономики. 2010. № 3 (35). С.124–128.
18. *Ефимов Е.И.* Возможность применения существующих средств анализа рисков в системах принятия решений с привлечением экспертов // Омский научный вестник. 2011. № 3-103. С.281–284.
19. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. 2008. № 149/54-144.
20. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их

обработке в информационных системах персональных данных». 2013. № 21.
21. Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». 2013. № 7.
22. Положение Центрального Банка Российской Федерации «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». 2012. № 382-П.
23. Постановление Правительства Российской Федерации «Об утверждении Положения о защите информации в платежной системе». 2012. № 584.
24. Payment Card Industry Data Security Standard (PCI DSS) // PCI Security Standards Council LLC. Version 2.0. 2010. 75 p. URL: https://www.pcisecuritystandards.org/documents.
25. Стандарт Банка России СТО БР ИББС-1.0-2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения // М.:Вестник Банка России. 2014. № 48–49. 37 с.
26. ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования // М.: Стандартинформ. 2008. 26 с.
27. ГОСТ Р ИСО/МЭК 13335-1 – 2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий // М.: Стандартинформ. 2006. 23 с.
28. *Осипов В. Ю., Носаль И. А.* Обоснование периода пересмотра мероприятий по защите информации // Информационно-управляющие системы. 2014. № 1. С. 63–69.
29. *Осипов В.Ю., Носаль И.А.* Обоснование мероприятий информационной безопасности // Информационно-управляющие системы. 2013. № 2(63). С. 48–53.
30. *Носаль И.А.* Обоснование оптимального набора прав доступа // Комплексная защита объектов информатизации и измерительные технологии. Сб. научн. тр. Всероссийской научно-практической конф. с междунар. участ. Санкт-Петербург:Издательство Политехнического университета. 2014. С. 41–45.

References

1. Jusupov R.M. *Nauka i nacional'naja bezopasnost'. 2-e izdanie, pererabotannoe i dopolnennoe.* [Science and national security. 2nd edition, revised and enlarged]. Spb.: Nauka. 2011. 369 p. (In Russ.).
2. Petrenko S.A., Popov Ju.I. [Assessment of the cost of information security]. *Konfident – Confident.* 2003. no.1(49). pp. 68–73. (In Russ.).
3. Obuhov A.A. [Diagnosis of the need to invest in security in today's business and formation on its basis recommendations]. *Vestnik Omskogo universiteta. Serija «Jekonomika» - Bulletin of Omsk University. Series "Economy".* 2013. no. 3. pp. 78–84. (In Russ.).
4. Rytov M.Ju., Rudanovskij M.V. [Security management of information technologies based on cognitive modeling methods]. *Informacionnaja bezopasnost' – Information Security*. 2010. no. 4. pp. 579–582. (In Russ.).
5. Azhmuhamedov I.M., Hanzhina T.B. [Evaluation of cost-effectiveness of information security]. *Vestnik AGTU – Bulletin AGTU.* 2011. no. 1. pp. 185–190. (In Russ.).
6. Birjukov D.N., Lomako A.G. [Approach to building systems to prevent cyber threats]. *Problemy informacionnoj bezopasnosti. Komp'juternye sistemy – Problems of information security. Computer systems.* 2013. no. 2. pp. 13–19. (In Russ.).
7. Kramarov L.S., Babenko L.K. [Detection of network attacks and countermeasures in the range of cloud systems]. *Izvestija JuFU. Tehnicheskie nauki – Proceedings of the JuFU. Technical sciences.* 2013. no. 12(149). pp. 94–101. (In Russ.).

8. Abramov E.S., Kobilev M.A., Kramarov L.S., Mordvin D.V. [Using the attack graph for automated calculation of countermeasures network information security threats]. *Izvestija JuFU. Tehnicheskie nauki – Proceedings of the JuFU. Technical sciences.* 2014. no. 2(151). pp. 92–100. (In Russ.).
9. Tronikov I.B. *Metody ocenki informacionnoj bezopasnosti predprijatija na osnove processnogo podhoda:dis. kand. tehn. nauk.* [Methods for assessing information security based on the process approach: Thesis. cand. tehn. Sciences]. Spb. 2010. 134 p. (In Russ.).
10. Azhmuhamedov I.M., Hanzhina T.B. [Evaluation of cost-effectiveness of information security]. *Vestnik AGTU – Bulletin AGTU.* 2011. no. 1. pp. 185–190. (In Russ.).
11. Mironov V.V., Nosal' I.A. [Modeling and assessing information security system on the example of GOU VPO "SyktGU"]. *Informacija i bezopasnost' – Information and Security.* 2011. no. 2. pp. 209–211. (In Russ.).
12. Vasil'ev V.I., Savina I.A., Sharipova I.I. [Construction of fuzzy cognitive maps for analysis and information risk management university]. *Vestnik UGTU – Bulletin UGTU.* 2008. vol. 2. Issue 10. pp. 199–209. (In Russ.).
13. Schneier B. Attack Trees. *Dr. Dobb's Journal*. 1999. vol. 24. no. 12. pp. 21–29.
14. Sodiya A. S., Onashoga S. A., Oladunjoye B. A. Threat Modeling Using Fuzzy Logic Paradigm. Issues in Informing Science and Information Technology. 2007. vol. 4. pp. 53–61.
15. Chechulin A.A. [Methodology operational formation, modification and analysis of attack trees]. *Trudy SPIIRAN – SPIIRAS Proceedings. Spb.: Nauka*. 2013. no. 3(26). pp. 40–53. (In Russ.).
16. Karpeev D.O. *Issledovanie i razvitie metodicheskogo obespechenija ocenki i upravlenija riskami informacionnyh sistem na osnove intereso-orientirovannogo podhoda: dis. kand. tehn. nauk.* [Research and development of methodological support risk assessment and management of information systems based on interests-oriented approach: Thesis. cand. tehn. Sciences.]. Voronezh. 2009. 171 p. (In Russ.).
17. Kornilova A.Ju,. Palej T.F. [Problems of application of expert assessments in the process of economic forecasting enterprise development]. *Problemy sovremennoj jekonomiki – Problems of the modern economy.* 2010. no. 3 (35). pp.124–128. (In Russ.).
18. Efimov E.I. [The possibility of using existing tools of risk analysis in decision-making systems with experts]. *Omskij nauchnyj vestnik – Omsk Scientific Bulletin.* 2011. no. 3. pp. 281–284. (In Russ.).
19. *Metodicheskie rekomendacii po obespecheniju s pomoshh'ju kriptosredstv bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh s ispol'zovaniem sredstv avtomatizacii* [Methodical recommendations for using kriptosredstv personal data security at their processing within the information systems of personal data with the use of automation]. 2008. No 149/54-144. (In Russ.).
20. *Prikaz Federal'noj sluzhby po tehnicheskomu i jeksportnomu kontrolju (FSTJeK Rossii) «Ob utverzhdenii Sostava i soderzhanija organizacionnyh i tehnicheskih mer po obespecheniju bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh»* [Order of the Federal Service for Technical and Export Control (FSTEC Russia) "On approval of the composition and content of organizational and technical measures to ensure the security of personal data at their processing in information systems of personal data"]. 2013. no 21. (In Russ.).
21. *Prikaz FSTJeK Rossii «Ob utverzhdenii sostava i soderzhanija organizacionnyh i tehnicheskih mer po obespecheniju bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh».* [Order FSTEC Russia "On approval of the composition and content of organizational and technical measures to ensure the security of personal data at their processing in information systems of personal data"]. 11.02.2013. no 17. (In Russ.).
22. *Polozhenie Central'nogo Banka Rossijskoj Federacii «O trebovanijah k obespecheniju zashhity informacii pri osushhestvlenii perevodov denezhnyh sredstv i o porjadke osushhestvlenija Bankom Rossii kontrolja za sobljudeniem trebovanij k obespecheniju*

zashhity informacii pri osushhestvlenii perevodov denezhnyh sredstv». [The position of the Central Bank of the Russian Federation "On requirements to ensure the protection of sensitive information in the transfer of funds and the exercise of the Bank of Russia control over compliance with requirements to ensure the protection of sensitive information in the transfer of funds"]. 2012. no 382-P. (In Russ.).
23. *Postanovlenie Pravitel'stva Rossijskoj Federacii «Ob utverzhdenii Polozhenija o zashhite informacii v platezhnoj sisteme»* [Resolution of the Government of the Russian Federation "On Approval of the Regulations on the Protection of the information in the payment system"]. 2012. no. 584. (In Russ.).
24. Payment Card Industry Data Security Standard (PCI DSS). PCI Security Standards Council LLC. Version 2.0. 2010. 75 p. URL: https://www.pcisecuritystandards.org/documents.
25. *Standart Banka Rossii STO BR IBBS-1.0-2014 Obespechenie informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii. Obshhie polozhenija.* [The Standard Bank of Russia STO BR IBBS-1.0-2014 Information security organizations of the banking system of the Russian Federation. General provisions. - Instead of STO BR IBBSS-1.0-2010; Introduced 06/01/2014]. M.: Vestnik Banka Rossii. 2014. no. 48–49. 37 p. (In Russ.).
26. GOST R ISO/MJeK 27001—2006. [Information technology. Methods and means of ensuring safety. Information security management systems. Requirements.]. M.: Standartinform. 2008. 26 p. (In Russ.).
27. GOST R ISO/MJeK 13335-1- 2006. [Information technology. Methods and means of ensuring safety. Part 1: Concepts and models for the management of security of information and telecommunication technologies.]. M.: Standartinform. 2006. 23 p. (In Russ.).
28. Osipov V. Ju., Nosal' I. A. [Substantiation of the period of revision of information security measures]. *Informacionno–upravljajushhie sistemy - Information and Control Systems.* 2014. no. 1. pp. 63–69. (In Russ.).
29. Osipov V. Ju., Nosal' I. A. [Substantiation of information security measures]. *Informacionno–upravljajushhie sistemy – Information and Control Systems.* 2013. no. 2. pp. 48–53. (In Russ.).
30. Nosal' I. A. [Justification of the optimal set of permissions]. *Kompleksnaja zashhita ob"ektov informatizacii i izmeritel'nye tehnologii: Sb. nauchn. tr. Vserossijskoj nauchno-prakticheskoj konf. s mezhdunar. uchast.* [Comprehensive protection of information objects and measurement technology: Sat. Scien. tr. All-Russian Scientific-Practical Conference. with int. participation]. Sankt-Peterburg:Izdatel'stvo Politehnicheskogo universiteta. 2014. pp. 41–45.

Носаль Ирина Алексеевна — аспирант лаборатории прикладной информатики и проблем информатизации общества, Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: защита информации, информационная безопасность. Число научных публикаций — 6. ironia.i@gmail.com; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7(812)3281113, Факс: +7 (812)3284450.

Nosal Irina Alexeevna — Ph.D. student of laboratory of Applied Informatics and Problems of Society Informatization, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: information security. The number of publications — 6. ironia.i@gmail.com; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7 (812)328-1113, Fax: +7 (812)3284450.

РЕФЕРАТ

Носаль И.А. **Метод обоснования мероприятий информационной безопасности социально-важных объектов.**

Исследуется процесс обеспечения информационной безопасности в структурах Пенсионного фонда Российской Федерации, как социально-важных объектов. Отмечается, что существующее научно-методическое обеспечение такой безопасности не совершенно. Для повышения информационной безопасности в структурах Пенсионного фонда Российской Федерации предлагается усовершенствованный метод поиска целесообразных мероприятий защиты от возможных угроз. Разработана совокупность типовых моделей для оценки информационной безопасности этих объектов, применимых в рамках предложенного метода. Разработанные метод и модели ориентированы на обоснование мероприятий информационной безопасности в изменяющихся внутренних и внешних условиях. Приведены результаты моделирования, подтверждающие справедливость предложенного метода и входящих в него моделей.

SUMMARY

Nosal I.A. **Method of Information Security Measures Substantiation for Socially Important Objects.**

The process of information security in the structures of the Pension Fund of the Russian Federation, as a socially important objects, is studied. It is noted that the existing scientific and methodological support of such security is not perfect. To improve information security in the structures of the Pension Fund of the Russian Federation an improved method of searching for appropriate measures to protect against potential threats is proposed. The set of standard models for the evaluation of information security of these objects that are applicable within the proposed method are developed. The methods and models are focused on study of information security measures in the changing internal and external conditions. The simulation results confirm the validity of the proposed method and its constituent models.