РАЗРАБОТКА ИССЛЕДОВАТЕЛЬСКОГО АППАРАТА ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕР ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Кондаков С.Е.[1], Чудин К.С.[2]

Цель статьи: *исследовать предпосылки для разработки методического аппарата для обеспечения защиты персональных данных в деятельности кадрового органа службы защиты государственной тайны.*

Метод исследования*. Системный анализ, синергетика.*

Полученный результат*. Сформулирован порядок формирования соответствующей исследовательской среды, приводятся этапы формирования концепции построения исследовательского аппарата для оценки эффективности мер обеспечения защиты персональных данных в деятельности кадрового органа службы защиты государственной тайны. Предложена концепция построения исследовательского аппарата для оценки характеристик мер обеспечения защиты персональных данных в деятельности кадрового органа службы защиты государственной тайны, позволяющая сформировать среду для адекватной оценки эффективности таких мер, а также определения набора гипотез и аналогий, необходимых для постановки и решения задачи повышения адекватности оценки эффективности мер обеспечения защиты персональных данных в деятельности кадрового органа службы защиты государственной тайны как задачи разработки математических моделей характеристик угроз безопасности персональных данных и процессов их защиты.*

Ключевые слова: *кадровые органы, методология, метрика оценки, концепция мер обеспечения защиты, математическая модель.*

DOI:10.21681/2311-3456-2021-5-45-51

Введение

Исходя из общеметодологической (философской) трактовки категории «эффективность» (*лат. efficientia*), как «способности производить определённый эффект», эффективность мер обеспечения защиты персональных данных (ПДн) в деятельности кадрового органа службы защиты государственной тайны (СЗГТ) следует рассматривать как способность к предотвращению нарушения, в процессе такого рода деятельности, основных состояний защищенности информации – ее конфиденциальности, целостности и доступности.

Для процесса обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, как объекта исследования характерна необходимость анализа двух взаимосвязанных явлений – действий нарушителя по реализации угроз безопасности ПДн и действий должностных лиц органа СЗГТ по обеспечению безопасности ПДн [1, 2].

Подобная специфичность трансформируется и на исследовательский аппарат, применяемый для оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ.

С учетом этого сформулируем концепцию построения данного исследовательского аппарата.

В основе концепции лежит положение о системном характере показателя эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, что является следствием системной природы такого рода мер [3-5].

Это приводит к необходимости интегрированного отражения в данном показателе двух взаимосвязанных множеств характеристик – характеристик угроз безопасности ПДн и характеристик механизмов обеспечения безопасности ПДн [6-8]. В свою очередь в соответствии с [9] интегральный характер показателя эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ требует однотипную метрику оценки этих характеристик.

Важнейшей особенностью концепции построения исследовательского аппарата для оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ является то, что при проведении исследований в данной сфере деятельности, как, впрочем, и в деятельности по обеспечению безопасности информации в целом, натурные эксперименты применяются в самом минимальном объеме. Это обстоятельство обусловлено существенным ущербом деятельности кадрового органа СЗГТ, связанного с рисками нарушения безопасности ПДн при проведении таких экспериментов [10]. Следствием этого является построение исследовательского аппарата для оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ на основе методологии математического моделирования.

Это влечет за собой необходимость адаптации данной методологии к рассматриваемой области исследо-

1 Кондаков Сергей Евгеньевич, кандидат технических наук, сотрудник Восьмого управления ГШ ВС РФ, г. Москва, Россия. E-mail: sergeikondakov@list.ru

2 Чудин Кирилл Сергеевич, сотрудник Восьмого управления ГШ ВС РФ, г. Москва, Россия. E-mail: 4ydo-kirill@rambler.ru

ваний как в теоретическом, так и в практическом плане. Направлением совершенствования теории моделирования должна стать разработка методологических основ систематизации математических моделей для оценки возможностей нарушителя по реализации угроз безопасности ПДн и возможностей по обеспечению деятельности кадрового органа СЗГТ в условиях подобного рода угроз. Направлениями совершенствования практики моделирования в данной области должно стать научное обоснование требований к совершенствованию мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ на основе вычислительных экспериментов с разработанными моделями.

Как любая концепция, концепция построения исследовательского аппарата для оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ реализует два базовых принципа – принцип дифференциации исследуемых явлений и принцип их интегративности. Дифференциация исследуемых явлений предполагает их системный анализ. С этой целью производится декомпозиция соответствующих целевых функций – целевой функции действий нарушителя по реализации угроз безопасности ПДн и целевой функции действий должностных лиц органа СЗГТ по обеспечению безопасности ПДн. В соответствии с принципом интегративности исследуемых явлений предполагается, что показатель эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ формируется в результате синтеза характеристик угроз безопасности ПДн и характеристик механизмов обеспечения безопасности ПДн.

Методологическим базисом концепции построения исследовательского аппарата для оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ являются основы информационной безопасности.

Исходя из вышеизложенного, это предполагает:

1. Формулировку цели оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, задач, решаемых для достижения этой цели и определение методов построения соответствующей исследовательской среды для их решения.

2. Разработку методик, позволяющих характеризовать возможности нарушителя по реализации угроз безопасности ПДн и возможности по обеспечению деятельности кадрового органа СЗГТ в условиях подобного рода угроз как факторы, определяющие эффективность мер обеспечения защиты ПДн.

3. Разработку структурного представления процессов обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, как следствия угроз безопасности ПДн.

4. Обоснование системной классификации характеристик мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ на основе анализа различных вариантов угроз безопасности ПДн и процессов реагирования на них механизмами защиты.

5. Разработка математических моделей для исследования угроз безопасности ПДн и процессов реагирования на них механизмами защиты.

6. Формирование исследовательской среды для проведения вычислительных экспериментов по оценке эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ.

7. Определение критериев, обеспечивающих возможность формального обоснования требований к направлениям совершенствования мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ.

На рис. 1 приводятся предпосылки для разработки методического аппарата для исследования эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, а в табл.1 – порядок формирования соответствующей исследовательской среды.

Исходя из общеметодологических положений системного анализа методические основы построения исследовательской среды для оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ следует рассматривать как систему взглядов относительно возможностей исследования угроз безопасности ПДн и процессов реагирования на них. Присущая такой системе целостность представления о путях решения исследуемой проблемы достигается за счет систематизации опыта оценки возможностей механизмов защиты ПДн и адекватного отображение структуры и содержания взаимосвязей с другими проблемами в сфере обеспечения безопасности информации. Выбор направлений эффективного решения задач моделирования таких механизмов и предоставление для этого соответствующих методических средств достигается за счет реализации в данной предметной области общеметодологических принципов системного анализа, теории моделирования систем и практики проведения вычислительных экспериментов с математическими моделями.

Основными этапами формирования концепции построения исследовательского аппарата для оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ являются:

1) сбор и систематизация сведений о необходимости создания соответствующей исследовательской среды, адекватно учитывающих потребности этих данного органа в обеспечении информационной безопасности и объективные предпосылки обеспечения защиты ПДн;

2) анализ существующего опыта разработки теоретических основ решения подобных задач;

3) формулировка формализованной постановка научно обоснованной задачи создания исследовательской среды для адекватной оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, обоснование порядка решения данной задачи;

4) выработка системных требований к порядку исследования эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, учитывающих условия обеспечения высокой адекватности оценки;

5) разработка макроструктуры содержания конкретных прикладных методов оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ и реализация этих методов.

Остановимся на наиболее важном этапе формирования концепции построения исследовательского аппарата для оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ – этапе

УДК 004.056; 621.3

Рис. 1. Предпосылки для разработки методического аппарата для исследования эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ

Таблица 1

Порядок формирования исследовательской среды для оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ

1. Формулировка цели разработки и исследования моделей оценки эффективности мер обеспечения ПДн в деятельности кадрового органа СЗГТ.
2. Систематизация существующих подходов к оценке эффективности защиты информации от НСД.
3. Анализ особенностей обеспечения безопасности ПДн.
4. Обоснование моделей угроз безопасности ПДн.
5. Формулировка принципов оценки характеристик эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ.
6. Разработка методов исследования характеристик угроз безопасности ПДн и характеристик процессов реагирования на такого рода угрозы.
7. Разработка математических моделей характеристик исследуемых процессов.
8. Постановка вычислительных экспериментов по оценке эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ.

формулировки формализованной постановка научно обоснованной задачи создания исследовательской среды для адекватной оценки эффективности. Корректность сформулированной задачи является основным фактором ее правильного решения.

В содержательном плане задача ставится как задача обоснования методики систематизации функционального и формализованного представления угроз безопасности ПДн и мер обеспечения их защиты позволяющей разработать совокупность формальных оснований для математического моделирования характеристик эффективности таких мер с целью повышения адекватности используемого методического аппарата при заданных ограничениях на формальную интерпретацию модели угрозы, что дает возможность научно обосновать требования к характеристикам механизмов защиты ПДн.

С целью формализованной постановки данной задачи воспользуемся базовыми определениями теории моделирования такими как гипотеза, аналогия, модель и ее адекватность.

Как известно, гипотеза (от греч. hypothesis – основание, основа) представляет собой хорошо продуманное предположение, выраженное в форме научных понятий, которое должно в определенном месте восполнить пробелы эмпирического познания или связать различные эмпирические знания в единое целое либо дать предварительное объяснение факту или группе фактов. Гипотеза является научной лишь в том случае, если она подтверждается фактами. Гипотеза может существовать лишь до тех пор, пока не противоречит достоверным фактам опыта; она верифицируется (проверяется) соответствующими фактами опыта, в особенности экспериментом.

Аналогия (греч. — соответствие, сходство) определятся как сходство предметов (явлений, процессов и т. д.) в каких-либо свойствах. При умозаключении по аналогии знание, полученное из рассмотрения какого-либо объекта («модели»), переносится на другой, менее изученный (менее доступный для исследования, менее наглядный и т. п.) в каком-либо смысле объект. По отношению к конкретным объектам заключения, получаемые по аналогии, носят, как правило, лишь правдоподобный характер; они являются одним из источников научных гипотез и индуктивных рассуждений.

Модель (в науке) — это объект-заместитель объекта-оригинала, инструмент для познания, который исследователь ставит между собой и объектом и с помощью которого изучает некоторые свойства оригинала. В качестве модели выступает другой материальный или мысленно представляемый объект, замещающий в процессе исследования объект-оригинал.

Математическая модель – это эквивалент объекта, отражающий в математической форме важнейшие его свойства — законы, которым он подчиняется, связи, присущие составляющим его частям, и т.д.[3]

Соответствие свойств модели исходному объекту характеризуется адекватностью [11, 12]. Применительно к исследуемой проблеме в качестве гипотезы предположим, что характеристики эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ являются характеристиками функциональными.

Доказательством данной гипотезы служит то обстоятельство, что эффективность мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, как объект исследования, характеризует действия (функции) нарушителя по реализации угроз безопасности ПДн и действия (функции) должностных лиц органа СЗГТ по обеспечению безопасности ПДн.

Аналогией, характеризующей эти действия, является их функциональное представление, например представление в терминах функционального моделирования [13, 14].

При характеристике адекватности аппарата математического моделирования приходится констатировать тот факт, что существующий уровень проработки вопросов использования методов математического моделирования в проблематике защиты информации не позволяет рассматривать применяемый аппарат математического моделирования как адекватный.

Это обусловлено рядом обстоятельств.

Первое обстоятельство связано с применением процедур оценки возможностей нарушителя, основанных на эмпирике. Характерным примером здесь являются методические документы ФСТЭК России (далее — ФСТЭК), регламентирующие порядок оценки актуальных угроз безопасности информации. Как показано в [15] и лингвистический характер оценки субъектно-объектных отношений между угрозами и порождающими их уязвимостями информации, и последующий переход к количественному представлению их вероятностных характеристик, основанные на экспертном подходе, привносят большую долю субъективизма в результаты оценки и, как следствие, являются причиной низкой адекватности используемых процедур оценки.

Второе обстоятельство связано с отсутствием учета динамики случайных состояний угроз безопасности информации. В п. 5 «Определение вероятностей реализации угроз» нормативного методического документа ФСТЭК, регламентирующего порядок оценки актуальных угроз безопасности информации, прямо указывается, что модели для определения вероятности угрозы в динамике ее возникновения и реализации в настоящее время отсутствуют.

Третье обстоятельство связано с ограниченным числом случайных событий, в тех моделях, которые учитывают динамику возникновения и реализации угроз безопасности информации. К таким моделям относятся модели, учитывающие лишь продолжительность угрозы, но не учитывающие случайные состояния, связанные с динамикой их возникновения [16].

Преодоление указанных недостатков в проблематике адекватной оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ возможно лишь в том случае, когда формальное описание угроз безопасности ПДн позволяет математически представить все условия, характерные для их динамики.

3 Самарский А.А., Михайлов А.П. Математическое моделирование. Идеи. Методы. Примеры. — 2-е изд., испр. — М.: Физматлит, 2001.

Указанные обстоятельства позволяют формальную постановку задачи повышения адекватности оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ сформулировать следующим образом [17].

Заданы:

- гипотезы $H_{(ва)}$ и $h_{(ва)}$ относительно проявляемых угрозами безопасности ПДн свойств для характеристики эффективности мер обеспечения защиты ПДн от такого рода угроз для случая, когда имеет место учет динамики обнаружения угрозы и для случая, когда учет динамики обнаружения угрозы отсутствует;
- гипотезы $H_{(ав)}$ и $h_{(ав)}$ относительно проявляемых механизмами защиты ПДн свойств для характеристики эффективности мер защиты для случая, когда имеет место учет динамики обнаружения угроз безопасности ПДн и для случая, когда учет динамики обнаружения такого рода угроз отсутствует;
- аналогия $A_{(ва)}$ относительно гипотезы $H_{(ва)}$;
- аналогия $a_{(ва)}$ относительно гипотезы $h_{(ва)}$;
- аналогия $A_{(ав)}$ относительно гипотезы $H_{(ав)}$;
- аналогия $a_{(ав)}$ относительно гипотезы $h_{(ав)}$;
- ограничения $\{r_i\}$ на интерпретацию модели угрозы безопасности ПДн.

Кроме того, обозначим через $Э = Э(H_{(ва)}, A_{(ва)}, H_{(ав)}, A_{(ав)})$ и $э = э(h_{(ва)}, a_{(ва)}, h_{(ав)}, a_{(ав)})$ функциональное описание связей между гипотезами и их аналогиями для характеристики эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ для случая, когда имеет место учет динамики обнаружения угрозы безопасности ПДн и для случая, когда учет динамики обнаружения угрозы отсутствует.

Определим ошибку $ΔЭ = |Э - э|$ в представлении эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, возникающую вследствие отсутствия учета динамики обнаружения угроз безопасности ПДн.

Требуется разработать математическую модель М(Э) эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, адекватность которой превосходит существующие показатели адекватности оценки такого рода мер:

Сформулированная задача решается следующей последовательностью этапов:

1. Обоснование гипотез относительно свойств исследуемых процессов и имеющихся соотношений между этими свойствами для характеристики эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ.
2. Разработка методических основ формализации случайных событий, характерных для динамики обнаружения угроз безопасности ПДн.
3. Обоснование ограничений на интерпретацию модели угроз безопасности ПДн.
4. Разработка функционального представления угроз безопасности ПДн и процессов защиты ПДн.
5. Обоснование формализованного представления целевых функций исследуемых процессов.
6. Разработка математических моделей характеристик процессов реализации угроз безопасности ПДн в деятельности кадрового органа СЗГТ и процессов защиты ПДн на основе формализованного представления целевых функций этих процессов.
7. Разработка математической модели показателя эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ.на основе формализованного представления случайных событий, характерных для динамики обнаружения угроз безопасности ПДн.
8. Проведение вычислительных экспериментов с математическими моделями для обоснования требований к характеристикам мер защиты ПДн в деятельности кадрового органа СЗГТ.

Вывод

Предложенная концепция построения исследовательского аппарата для оценки характеристик мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ позволяет сформировать исследовательскую среду для адекватной оценки эффективности таких мер.

Кроме того, концепция дает возможность определить набор гипотез и аналогий, необходимый для постановки и решения задачи повышения адекватности оценки эффективности мер обеспечения защиты ПДн в деятельности кадрового органа СЗГТ, как задачи разработки математических моделей характеристик угроз безопасности ПДн и процессов их защиты.

Литература

1. Грибунин В.Г., Гришаненко Р.Л., Лабазников А.П., Тимонов А.А. Безопасность систем машинного обучения. защищаемые активы, уязвимости, модель нарушителя и угроз, таксономия атак // Известия Института инженерной физики. 2021. № 3 (61). С. 65-71.
2. Кондаков С.Е., Мещерякова Т.В., Скрыль С.В., Стадник А.Н., Суворов А.А. Вероятностное представление условий своевременного реагирования на угрозы компьютерных атак // Вопросы кибербезопасности. 2019. № 6 (34). С. 59-68. DOI: 10.21681/2311-3456-2019-6-59-68
3. Покусов В.В. Оценка эффективности системы обеспечения ИБ. Часть 1. Показатели и модели представления // Защита информации. Инсайд. 2019. № 2 (86). С. 54-60.
4. Язов Ю.К., Авсентьев О.С., Рубцова И.О. К вопросу об оценке эффективности защиты информации в системах электронного документооборота // Вопросы кибербезопасности. 2019. № 1 (29). С. 25-34. DOI: 10.21681/2311-3456-2019-1-25-34
5. Функционал качества для выбора варианта АПК АИС с показателями различной природы, размерности и вектора полезности. / С.Е. Кондаков, Г.Н. Рассохин // Научно-технический сборник № 3, Юбилейный: 4 ЦНИИ МО РФ, 2014. С. 6-11.
6. Лившиц И.И. Оценка степени влияния General Data Protection Regulation на безопасность предприятий в Российской Федерации // Вопросы кибербезопасности. 2020. № 4 (38). С. 66-75. DOI: 10.21681/2311-3456-2020-4-66-75

7. Максимова Е.А., Кузнецова М.А., Топилин Я.Н., Федонюк Н.И., Петрищева Т.С. Внутренний контроль соответствия обработки ПДн требованиям к их защите // Защита информации. Инсайд. 2019. № 6 (90). С. 5-9.
8. Терентьева Л.В. Критерий «направленной деятельности» применительно к отношениям, связанным с защитой персональных данных // Правовая информатика. 2021. № 1. С. 61-69. DOI: 10.21681/1994-1404-2021-1-61-69
9. Сравнение оценок качества решения по выбору варианта системы защиты комплекса средств автоматизации, полученных при применении энтропийного и полезностного подходов. / С.Е. Кондаков // Безопасные информационные технологии. М.: НТб. НИИ РЛ МГТУ им. Н.Э.Баумана. 2014. С. 8-11.
10. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov — London: IntechOpen, 2018. 278 p. 10.5772/ intechopen.71396. DOI: 10.5772/intechopen.71396
11. Булдакова Т.И., Миков Д.А. Обеспечение согласованности и адекватности оценки факторов риска информационной безопасности // Вопросы кибербезопасности. 2017. № 3 (21). С. 8-15. DOI: 10.21681/2311-3456-2017-3-08-15
12. Марков А.С. Модели оценки и планирования испытаний программных средств по требованиям безопасности информации // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия Приборостроение. 2011. №S1. С. 90-103.
13. Дорофеева Л.И. Моделирование и оптимизация разделительных процессов. / Томск: Изд-во Томского политехнического университета, 2008. 128 с.
14. Функциональное моделирование как методология исследования конфиденциальности информационной деятельности / С.В. Скрыль, А.А. Малышев, С.Н. Волкова А.А. Герасимов // Интеллектуальные системы: Труды Девятого международного симпозиума. М.: РУСАКИ, 2010. С. 590 – 593.
15. Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры. / С.В. Скрыль, В.В. Гайфулин, В.М. Сычев, Ю.В. Грачева [и др.] // Безопасность информационных технологий. М.: МИФИ, 2021. № 1. С. 24 – 33.
16. Обоснование показателя для оценки эффективности мер обеспечения защиты персональных данных в деятельности кадрового органа службы защиты государственной тайны / С.В. Скрыль, С.Е. Кондаков, К.С. Чудин // Информационная безопасность – актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности: материалы XXI Всероссийской межведомственной научно-технической конференции, Том 1. Краснодар, КВВУ, 2020. С. 19 – 24.
17. Постановка задачи обоснования варианта системы защиты информации комплекса средств автоматизации информационно-расчетной системы ракетных войск стратегического назначения. / С.Е. Кондаков, С.В. Скрыль // Научно-технический сборник ОАО «Концерн «Системпром». 2014. № 1(5), С. 17-22.

DEVELOPMENT OF A RESEARCH APPARATUS FOR ASSESSING THE EFFECTIVENESS OF MEASURES TO ENSURE THE PROTECTION OF PERSONAL DATA

Kondakov S.E. [4]***, Chudin K.S.*** [5]

The purpose *of the article: to investigate the prerequisites for the development of a methodological apparatus for ensuring the protection of personal data in the activities of the personnel body of the state secret protection service.*

Research method. *system analysis, synergetics.*

The result: *the procedure for the formation of the appropriate research environment is formulated, the stages of formation of the concept of building a research apparatus for assessing the effectiveness of measures to ensure the protection of personal data in the activities of the personnel body of the state secret protection service are given. The concept of building a research apparatus for assessing the characteristics of measures to ensure the protection of personal data in the activities of the personnel body of the state secret protection service is proposed, which allows forming an environment for an adequate assessment of the effectiveness of such measures, as well as determining a set of hypotheses and analogies necessary for setting and solving the problem of increasing the adequacy of assessing the effectiveness of measures to ensure the protection of personal data in the activities of the personnel body of the state secret protection service as a task of developing mathematical models of the characteristics of threats to the security of personal data and the processes of their protection.*

Keywords: *personnel bodies, methodology, evaluation metric, concept of protection measures, mathematical model.*

4 Sergey Kondakov, Ph.D., Russian Defense Ministry employee, Moscow, Russia. E-mail: sergeikondakov@list.ru

5 Kirill Chudin, Russian Defense Ministry employee, Moscow, Russia. E-mail: 4ydo-kirill@rambler.ru

References

1. Gribunin V.G., Grishanenko R.L., Labaznikov A.P., Timonov A.A. Bezopasnost` sistem mashinnogo obucheniia. zashchishchaemy`e aktivy`, uiazvimosti, model` narushitelia i ugroz, taksonomiia atak // Izvestiia Instituta inzhenernoi` fiziki. 2021. № 3 (61). S. 65-71.
2. Kondakov S.E., Meshcheriakova T.V., Skry`l` S.V., Stadnik A.N., Suvorov A.A. Veroiatnostnoe predstavlenie uslovii` svoevremennogo reagirovaniia na ugrozy` komp`iuterny`kh atak // Voprosy` kiberbezopasnosti. 2019. № 6 (34). S. 59-68. DOI: 10.21681/2311-3456-2019-6-59-68
3. Pokusov V.V. Ocenka e`ffektivnosti sistemy` obespecheniia IB. Chast` 1. Pokazateli i modeli predstavleniia // Zashchita informatcii. Insai`d. 2019. № 2 (86). S. 54-60.
4. Iazov Iu.K., Avsent`ev O.S., Rubtcova I.O. K voprosu ob ocenke e`ffektivnosti zashchity` informatcii v sistemakh e`lektronnogo dokumentooborota // Voprosy` kiberbezopasnosti. 2019. № 1 (29). S. 25-34. DOI: 10.21681/2311-3456-2019-1-25-34
5. Funktcional kachestva dlia vy`bora varianta APK AIS s pokazateliami razlichnoi` prirody`, razmernosti i vektora poleznosti. / S.E. Kondakov, G.N. Rassohin // Nauchno-tekhnicheskii` sbornik № 3, Iubilei`ny`i`: 4 TCNII MO RF, 2014. S. 6-11.
6. Leevshitc I.I. Ocenka stepeni vliianiia General Data Protection Regulation na bezopasnost` predpriiatii` v Rossii`skoi` Federatcii // Voprosy` kiberbezopasnosti. 2020. № 4 (38). S. 66-75. DOI: 10.21681/2311-3456-2020-4-66-75
7. Maksimova E.A., Kuznetcova M.A., Topilin Ia.N., Fedoniuk N.I., Petrishcheva T.S. Vnutrennii` kontrol` sootvetstviia obrabotki PDn trebovaniiam k ikh zashchite // Zashchita informatcii. Insai`d. 2019. № 6 (90). S. 5-9.
8. Terent`eva L.V. Kriterii` “napravlennoi` deiatel`nosti” primenitel`no k otnosheniiam, sviazanny`m s zashchitoi` personal`ny`kh danny`kh // Pravovaia informatika. 2021. № 1. S. 61-69. DOI: 10.21681/1994-1404-2021-1-61-69
9. Sravnenie ocenok kachestva resheniia po vy`boru varianta sistemy` zashchity` kompleksa sredstv avtomatizatcii, poluchenny`kh pri primenenii e`ntropii`nogo i poleznostnogo podhodov. / S.E. Kondakov // Bezopasny`e informatcionny`e tekhnologii. M.: NTb. NII RL MGTU im. N.E`.Baumana. 2014. S. 8-11.
10. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov — London: IntechOpen, 2018. 278 p. 10.5772/ intechopen.71396. DOI: 10.5772/intechopen.71396
11. Buldakova T.I., Mikov D.A. Obespechenie soglasovannosti i adekvatnosti ocenki faktorov riska informatcionnoi` bezopasnosti // Voprosy` kiberbezopasnosti. 2017. № 3 (21). S. 8-15. DOI: 10.21681/2311-3456-2017-3-08-15
12. Markov A.S. Modeli ocenki i planirovaniia ispy`tanii` programmny`kh sredstv po trebovaniiam bezopasnosti informatcii // Vestneyk Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E`. Baumana. Seriia Priborostroenie. 2011. №S1. S. 90 103.
13. Dorofeeva L.I. Modelirovanie i optimizatciia razdelitel`ny`kh protcessov. / Tomsk: Izd-vo Tomskogo politekhnicheskogo universiteta, 2008. 128 s.
14. Funktcional`noe modelirovanie kak metodologiia issledovaniia konfidentcial`nosti informatcionnoi` deiatel`nosti / S.V. Skry`l`, A.A. Maly`shev, S.N. Volkova A.A. Gerasimov // Intellektual`ny`e sistemy`: Trudy` Deviatogo mezhdunarodnogo simpoziuma. M.: RUSAKI, 2010. S. 590 – 593.
15. Aktual`ny`e voprosy` problematiki ocenki ugroz komp`iuterny`kh atak na informatcionny`e resursy` znachimy`kh ob``ektov kriticheskoi` informatcionnoi` infrastruktury`. / S.V. Skry`l`, V.V. Guyfulin, V.M. Sy`chev, Iu.V. Gracheva [i dr.] // Bezopasnost` informatcionny`kh tekhnologii`. M.: MIFI, 2021. № 1. S. 24 – 33.
16. Obosnovanie pokazatelia dlia ocenki e`ffektivnosti mer obespecheniia zashchity` personal`ny`kh danny`kh v deiatel`nosti kadrovogo organa sluzhby` zashchity` gosudarstvennoi` tai`ny` / S.V. Skry`l`, S.E. Kondakov, K.S. Chudin // Informatcionnaia bezopasnost` – aktual`naia problema sovremennosti. Sovershenstvovanie obrazovatel`ny`kh tekhnologii` podgotovki spetcialistov v oblasti informatcionnoi` bezopasnosti: materialy` XXI Vserossii`skoi` mezhvedomstvennoi` nauchno-tekhnicheskoi` konferentcii, Tom 1. Krasnodar, KVVU, 2020. S. 19 – 24.
17. Postanovka zadachi obosnovaniia varianta sistemy` zashchity` informatcii kompleksa sredstv avtomatizatcii informatcionno-raschetnoi` sistemy` raketny`kh voi`sk strategicheskogo naznacheniia. / S.E. Kondakov, S.V. Skry`l` // Nauchno-tekhnicheskii` sbornik OAO «Kontcern «Sistemprom». 2014. № 1(5), S. 17-22.