УДК 004.89 DOI 10.18522/2311-3103-2023-2-67-80

С.Е. Кондаков, К.С. Чудин, М.В. Болычев

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ КАДРОВОГО ОРГАНА ПРЕДПРИЯТИЯ ОПК

Целью данной статьи является обоснование показателя для оценки эффективности мер обеспечения безопасности персональных данных кадрового органа предприятия промышленного комплекса (далее – ОПК). Для построения математической модели вероятности возникновения угрозы используется методический аппарат оценки актуальных угроз безопасности информации, сформированных на основе нормативно-методических документов ФСТЭК России. В статье приводится авторская интерпретация основных методических положений, представленных в рассматриваемых документах, применительно к оценке угроз безопасности персональных данных (далее - ПДн) кадрового органа предприятия ОПК. Особенностью выявления уязвимостей информационных ресурсов кадрового органа предприятия ОПК, через которые возможна реализация угроз безопасности ПДн, является использование расчетных методик, позволяющих установить факт потенциальной возможности угрозы. Для определения уязвимостей информационных ресурсов кадрового органа предприятия ОПК к реализации угроз безопасности ПДн проводится экспертный анализ информационной среды ИС. В результате формируется множество, элементы которого и определяют уязвимости. Таким образом, следует рассматривать математическую модель вероятностной характеристики возникновения угрозы безопасности ПДн кадрового органа предприятия ОПК как произведение вероятностей предотвращения несанкционированного копирования, несанкционированной модификация и блокирование доступа к информационным ресурсам ИС кадрового органа предприятия ОПК.

Персональные данные; угрозы безопасности; экспертный анализ.

S.E. Kondakov, C.S. Chudin, M.V. Bolichev

MATHEMATICAL MODEL OF EMERGENCY SAFETY OPK

The purpose of this article is to substantiate the indicator for evaluating the effectiveness of measures to ensure the security of personal data of the personnel body of an industrial complex enterprise (hereinafter - the defense industry). To build a mathematical model of the probability of a threat, the methodological apparatus for assessing current threats to information security, formed on the basis of regulatory and methodological documents of the FSTEC of Russia, is used. The article presents the author's interpretation of the main methodological provisions presented in the documents under consideration in relation to the assessment of threats to the security of personal data (hereinafter - PD) of the personnel body of the defense industry enterprise. The peculiarity of identifying vulnerabilities of information resources of the personnel body of the defense industry enterprise, through which it is possible to implement threats to the security of PD, is the use of calculation methods that allow to establish the fact of the potential possibility of a threat. o determine the vulnerabilities of the information resources of the personnel body of the defense industry enterprise to the implementation of threats to the security of PD, an expert analysis of the information environment of the IP is carried out. As a result, a set is formed, the elements of which determine vulnerabilities. Thus, it is necessary to consider a mathematical model of the probabilistic characteristics of the occurrence of a threat to the security of the PD of the personnel body of the defense industry enterprise as a product of the probabilities of preventing unauthorized copying, unauthorized modification and blocking access to the information resources of the IS of the personnel body of the defense industry enterprise.

Personal data; security threats; expert analysis.

Введение. Современная философия относит понятие «эффективность» (*лат. efficientia*) к общеметодологическим категориям и трактует ее, как «способность производить определённый эффект» [1]. Естественно полагать, что в основе любого частного определения данного понятия будет лежать субъективное понимание эф-

фекта. Анализ исследуемой предметной области дает основание предложить следующий вариант определения понятия «эффективность мер обеспечения безопасности ПДн кадрового органа предприятия ОПК». Исходя из целей обеспечения безопасности ПДн под эффективностью соответствующих мер следует понимать их способность обеспечить заданный уровень качества деятельности кадрового органа предприятия ОПК в условиях угроз нарушения состояний защищенности ПДн.

Из данного определения очевидно, что для процесса обеспечения безопасности ПДн кадрового органа предприятия ОПК, как объекта исследования, характерна необходимость анализа трех взаимосвязанных явлений – угроз безопасности ПДн, обеспечение безопасности ПДн, а так же обработка ПДн в условиях угроз безопасности ПДн и реализации мер по обеспечению безопасности ПДн.

Подобная специфичность трансформируется и на исследовательский аппарат, применяемый для оценки эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК.

Постановка задачи исследования. С учетом этого сформулируем задачу построения математической модели угрозы безопасности персональных данных кадрового органа предприятия ОПК.

Для этого необходимо сформулировать концепцию построения исследовательского аппарата. В основе концепции лежит положение о системном характере показателя эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК, что является следствием системной природы такого рода мер.

Это приводит к необходимости интегрированного отражения в данном показателе трех взаимосвязанных множеств характеристик, отражающих возможности по реализации угроз безопасности ПДн, возможности по реализации мер обеспечения безопасности ПДн, а так же возможности кадрового органа предприятия ОПК, как оператора ПДн [2], по их обработке в условиях угроз безопасности и реализации мер обеспечения безопасности ПДн. В свою очередь интегральный характер показателя эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК требует однотипной метрики оценки этих характеристик.

Важнейшей особенностью концепции построения исследовательского аппарата для оценки эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК 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 предприятия ОПК, связанного с рисками нарушения безопасности ПДн при проведении таких экспериментов. Следствием этого является построение исследовательского аппарата для оценки эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК на основе методологии математического моделирования.

Это влечет за собой необходимость адаптации данной методологии к рассматриваемой области исследований как в теоретическом, так и в практическом плане. Направлением совершенствования теории моделирования должна стать разработка методического аппарата систематизации математических моделей для оценки возможностей нарушителя по реализации угроз безопасности ПДн и возможностей по обеспечению заданного уровня качества деятельности кадрового органа предприятия ОПК в условиях подобного рода угроз. Направлениями совершенствования практики моделирования в данной области должно стать научное обоснование требований к совершенствованию мер обеспечения безопасности ПДн кадрового органа предприятия ОПК на основе вычислительных экспериментов с разработанными моделями [3, 4].

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

Таким образом, задача построения математической модели вероятности возникновения угрозы сводиться к построению методического аппарат оценки актуальных угроз безопасности информации, сформированных на основе нормативно-методических документов.

Описание алгоритма исследования. Методологическим базисом концепции построения исследовательского аппарата для оценки эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК являются основы информационной безопасности, что предполагает [5, 6]:

1. Формулировку цели оценки эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК, 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 заданного уровня качества деятельности кадрового органа предприятия ОПК в условиях подобного рода угроз как факторы, определяющие эффективность мер обеспечения безопасности ПДн.

3. Разработку структурного представления процессов обеспечения безопасности ПДн кадрового органа предприятия ОПК, как следствия угроз безопасности ПДн.

4. Обоснование системной классификации характеристик мер обеспечения безопасности ПДн кадрового органа предприятия ОПК на основе анализа различных вариантов угроз безопасности ПДн и процессов обеспечения заданного уровня качества деятельности кадрового органа предприятия ОПК в условиях подобного рода угроз.

5. Разработка математических моделей для исследования угроз безопасности ПДн и процессов обеспечения заданного уровня качества деятельности кадрового органа предприятия ОПК в условиях подобного рода угроз.

6. Формирование исследовательской среды для проведения вычислительных экспериментов по оценке эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК.

7. Определение критериев, обеспечивающих возможность формального обоснования требований к характеристикам средств, используемых в процессе реализации мер обеспечения безопасности ПДн кадрового органа предприятия ОПК.

На рис. 1 приводится порядок формирования соответствующей исследовательской среды.

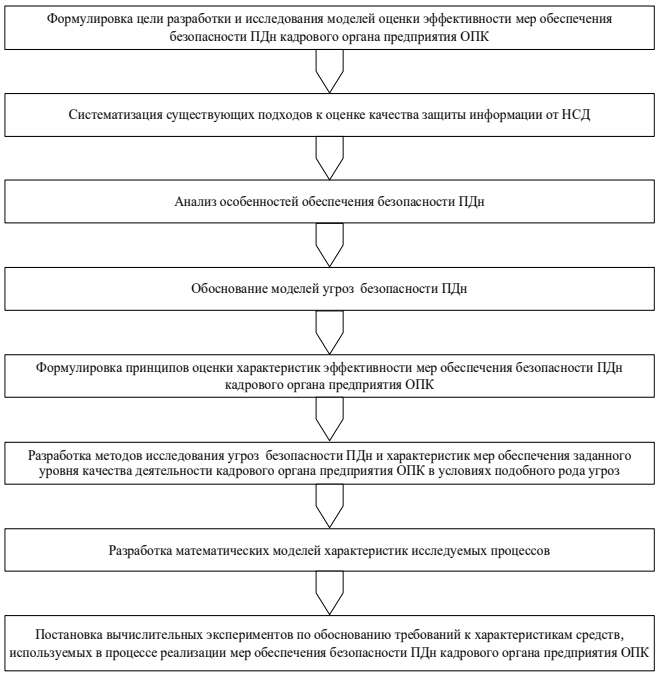

Рис. 1. Порядок формирования исследовательской среды для оценки эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК

Исходя из общеметодологических положений системного анализа методические основы построения исследовательской среды для оценки эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК следует рассматривать как систему взглядов относительно возможностей исследования угроз безопасности ПДн и процессов обеспечения заданного уровня качества деятельности кадрового органа предприятия ОПК в условиях подобного рода угроз. Присущая такой системе целостность представления о путях решения исследуемой проблемы достигается за счет систематизации опыта оценки возможностей механизмов защиты ПДн и адекватного отображения 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 [7–9].

Основными этапами формирования концепции построения исследовательского аппарата для оценки эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК 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 безопасности 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 безопасности ПДн кадрового органа предприятия ОПК, обоснование порядка решения данной задачи;

4) выработка системных требований к порядку исследования эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК, учитывающих условия обеспечения высокой адекватности оценки;

5) разработка макроструктуры содержания конкретных прикладных методов оценки эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК и реализация этих методов.

Предложенная концепция построения исследовательского аппарата для оценки характеристик мер обеспечения безопасности ПДн кадрового органа предприятия ОПК позволяет сформировать исследовательскую среду для адекватной оценки эффективности таких мер.

Исходя из обоснованного выше определения понятия «эффективность мер обеспечения безопасности ПДн кадрового органа предприятия ОПК» очевидно, что соответствующий показатель должен отражать следующие возможности:

- ♦ возможности нарушителя по реализации угроз безопасности ПДн;
- ♦ возможности по предотвращению нарушения состояний защищенности информации в работе кадрового органа предприятия ОПК;
- ♦ возможности кадрового органа предприятия ОПК, как оператора ПДн, по их обработке в условиях угроз безопасности ПДн и реализации процессов защиты информации.

Существующий методический аппарат позволяет оценить возможности нарушителя по реализации угроз безопасности информации двумя типами характеристик.

Первый тип характеристик отражает экспертную оценку причинно-следственных отношений между источниками угроз безопасности информации, ее уязвимостями к такого рода угрозам и возможностями реализации данными угрозами деструктивного воздействия на информационные ресурсы или процессы. Естественно, что эмпирический характер экспертизы приводит к вероятностному характеру оценок.

Второй тип характеристик отражает функциональные возможности по реализации нарушителем угроз безопасности информации и представляется временными характеристиками выполняемых им функций.

Решение задачи исследования. Исходя из этого, к показателям, характеризующим возможности нарушителя по реализации угроз безопасности ПДн, следует отнести вероятность $P_{(уб)}$ угрозы безопасности ПДн и время $\tau_{(уб)}$ ее реализации нарушителем.

При характеристике возможностей по предотвращению нарушения состояний защищенности информации в работе кадрового органа предприятия ОПК следует учитывать варианты формализованного представления такого рода возможностей. Наиболее распространенным в методологии информационной безопасности вариантом является вариант их представления в виде показателя своевременности предотвращения нарушения состояний защищенности информации. Соответствующий показатель формально интерпретируется как характеристика времени $\tau_{(п)}$ предотвращения нарушения нормированного продолжительностью $\tau_{(н)}$ действий нарушителя. Данный показатель определяется исходя из условий:

$$C_{(п)} = 1 \text{ при } \tau_{(п)} \leq \tau_{(н)} \quad (1)$$

и

$$C_{(п)} = 0 \text{ при } \tau_{(п)} > \tau_{(н)}. \quad (2)$$

В общем случае обе входящие в неравенства (1) и (2) величины являются случайными, а их выполнение является случайным событием. Вероятность $P(\tau_{(п)} \le \tau_{(н)})$ данного события представляет собой среднее количество ситуаций, при которых в течение продолжительности деструктивного воздействия на информацию удавалось предотвратить нарушения состояний ее защищенности относительно общего числа попыток нарушения на временном сегменте $[t_{(ни)}, t_{(ои)}]$ от момента начала $t_{(ни)}$ до момента окончания $t_{(ои)}$ исследования:

$$P\left(\tau_{(п)} \le \tau_{(н)}\right) = \frac{\sum_{i=1}^{I} \alpha_i}{I}, \tag{3}$$

где

$$\alpha_i = \begin{cases} 1, при\ \tau_{(п)i} \le \tau_{(н)i}, \\ 0, в\ противном\ случае; \end{cases}$$

$\tau_{(п)i}$ и $\tau_{(н)i}$ – время предотвращения и продолжительность действий нарушителя по реализации i-го, $i = 1, 2, \ldots, I$, нарушения состояний защищенности информации, соответственно;

I – общее число попыток нарушения состояний защищенности информации, фиксируемых на временном сегменте $[t_{(ни)}, t_{(ои)}]$.

С учетом изложенного выражение для характеристики своевременности предотвращения нарушения состояний защищенности информации в работе кадрового органа предприятия ОПК может иметь следующий формат:

$$C_{(п)} = P(\tau_{(п)} \le \tau_{(н)}). \tag{4}$$

Возможности по обработке ПДн в условиях угроз их безопасности и реализации мероприятий, направленных на предотвращение нарушения состояний защищенности информации. В соответствии с сформулированным требованием однотипной метрики оценки характеристик эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК показатель возможностей по обработке ПДн в условиях угроз их безопасности и реализации мероприятий, направленных на предотвращение нарушения состояний защищенности информации, представляется как результат нормирования времени обработки ПДн его максимально допустимым значением. Формально это можно представить, как

$$C = 1 \text{ при } \tau_{(ПДн)} \le \tau_{(max)} \tag{5}$$

и

$$C = 0 \text{ при } \tau_{(ПДн)} > \tau_{(max)}, \tag{6}$$

где C – показатель своевременности обработки ПДн; $\tau_{(ПДн)}$ – время реализации процессов обработки ПДн; $\tau_{(\max)}$ – максимально допустимое значение времени $\tau_{(ПДн)}$.

С учетом рассмотренных выше характеристик и показателей возможностей нарушителя по реализации угроз безопасности ПДн и возможностей по предотвращению нарушения состояний защищенности информации в работе кадрового органа предприятия ОПК время $\tau_{(ПДн)}$ реализации процессов обработки ПДн является функцией

$$\tau_{(ПДн)} = \tau_{(ПДн)}[\tau_{(ПДн)}^{(иу)}, \tau_{(в)}, P_{(уб)}, C_{(п)}(\tau_{(п)}, \tau_{(н)}), \tau_{(вк)}] \tag{7}$$

следующих параметров:

$\tau_{(ПДн)}^{(иу)}$ – случайной величины значения времени обработки ПДн в идеальных условиях (в условиях отсутствия угроз безопасности ПДн и механизмов защиты информации от такого рода угроз безопасности информации);

$\tau_{(в)}$ – случайной величины времени, затрачиваемого на выявление признаков деструктивного воздействия на ПДн, проявляющегося при реализации угрозы их безопасности;

$P_{(уб)}$ – вероятности угрозы безопасности ПДн;

$C_{(п)}(\tau_{(п)}, \tau_{(н)})$ – показателя своевременности предотвращения нарушения состояний защищенности информации в работе кадрового органа предприятия ОПК;

$\tau_{(п)}$ – случайной величины времени предотвращения нарушения состояний защищенности информации в работе кадрового органа предприятия ОПК;

$\tau_{(н)}$ – продолжительности действий нарушителя по реализации угроз безопасности ПДн;

$\tau_{(вк)}$ – случайной величины времени, затрачиваемого на восстановление корректности процессов обработки ПДн.

Величина $\tau_{(\max)}$ определяется нормативными требованиями к времени реализации процессов обработки ПДн.

В соответствии с приведенным в статьях [12–14] обоснованием показателей для оценки эффективности мер обеспечения безопасности ПДн кадрового органа предприятия ОПК возможности нарушителя характеризуются и вероятностью возникновения угрозы $P_{(уб)}$.

С целью построения математической модели вероятностной характеристики возникновения угрозы воспользуемся методическим аппаратом оценки актуальных угроз безопасности информации, сформированным на основе соответствующих нормативно-методических документов ФСТЭК России [10, 11].

Ниже приводится авторская интерпретация основных методических положений, представленных в рассматриваемых документах, применительно к оценке угроз безопасности ПДн кадрового органа предприятия ОПК.

Рассматриваемые методики [15, 16] дают возможность отнести факторы, способствующие возникновению угроз безопасности ПДн кадрового органа предприятия ОПК, путем анализа соответствий между источниками угроз и их признаками. При этом в основе анализа лежит эмпирика опыта экспертов. В результате формируется множество $\{a_k\}$, $k = 1, 2, \ldots, |\{a_k\}|$, элементы которого являются признаками источников угроз, а индексы – их номерами.

Источниками угроз безопасности ПДн кадрового органа предприятия ОПК являются:

$k = 1$ – иностранные спецслужбы;

$k = 2$ – пользователи ИС кадрового органа предприятия ОПК;

$k = 3$ – производители оборудования и организации, осуществляющие ремонт и обслуживание СВТ и периферийного оборудования ИС;

a_1 – наличие интереса у иностранных спецслужб к информационным ресурсам кадрового органа предприятия ОПК;

a_2 – самостоятельное проведение должностными лицами кадрового органа предприятия ОПК обслуживания СВТ и периферийного оборудования ИС;

a_3 – использование несертифицированного программного обеспечения (ПО) при техническом обслуживании и ремонтно-восстановительных работах в ИС.

Особенностью выявления уязвимостей информационных ресурсов кадрового органа предприятия ОПК, через которые возможна реализация угроз безопасности ПДн, является использование расчетных методик, позволяющих установить факт потенциальной возможности угрозы [17, 18, 19].

Для определения уязвимостей информационных ресурсов кадрового органа предприятия ОПК к реализации угроз безопасности ПДн проводится экспертный анализ информационной среды ИС. В результате формируется множество $\{b_l\}$, $l = 1, 2, \ldots, L$, элементы которого определяют уязвимости. При этом индексы соответствуют номерам уязвимостей из их перечня.

Для случая оценки возможностей нарушителя по реализации угрозы безопасности ПДн уязвимыми для такого рода угроз являются:

b_1 – драйверы средств ввода информации;

b_2 – драйверы средств отображения информации;

b_3 – драйверы средств обработки информации;

b_4 – драйверы микросхем BIOS;

b_5 – ПО серверов с открытым физическим доступом;

b_6 – ПО коммуникационного оборудования ИС;

b_7 – стек протоколов TCP/IP;

b_8 – протоколы межсетевого взаимодействия прикладного уровня;

b_9 – недокументированные точки межсетевого взаимодействия;

b_{10} – несертифицированные компоненты ПО;

b_{11} – электронная почта;

b_{12} – Web-браузер;

b_{13} – кабели оборудования ИС на участках, где к ним имеется физический доступ.

Результатом экспертизы возможностей по использованию источниками угроз уязвимостей информации служит качественная оценка этих возможностей, представляемая в терминах лингвистической шкалы, где терминами «да» и «нет» характеризуются высший и низший уровень таких возможностей, соответственно, а терминами «вероятно», «возможно» и «маловероятно» – промежуточные уровни. Лингвистическим значениям оценки возможностей использования k-м источником угрозы компьютерной атаки l-ой уязвимости ставятся в соответствие количественные значения вероятности p_{kl} использования. При этом процедура установки соответствий является эмпирической.

На основании данной вероятности определяется вероятность P_l использования l-й уязвимости ($l = 1, 2, \ldots, 13$) возможными тремя источниками угроз:

$$P_l = 1 - (\gamma_{l1} \cdot (1 - p_{l1}) \cdot \gamma_{l2} \cdot (1 - p_{l2}) \cdot \gamma_{l3} \cdot (1 - p_{l3})), \quad (8)$$

где γ_{lk} – коэффициент соответствия, равный 1, если l-я уязвимость соответствует k-му источнику и 0, если не соответствует.

Это позволяет сформировать множество $\{u_m\}$, $m = 1, 2, \ldots, 14$, угроз безопасности ПДн [18]:

u_1 – загрузка вредоносного ПО с функциями альтернативной ОС с расширенными полномочиями;

u_2 – несанкционированное копирование информации;

u_3 – несанкционированная модификация информации;

u_4 – внедрение ложного доверенного объекта;

u_5 – подмена системного ПО;

u_6 – перенаправление сетевого трафика;

u_7 – манипулирование данными в удаленном режиме;

u_8 – вскрытие электронного почтового ящика;

u_9 – блокирование электронного почтового ящика;

u_{10} – подмена Web-браузеров;

u_{11} – использование ошибок в алгоритмах прикладного ПО;

u_{12} – блокирование хоста пользователя;

u_{13} – блокирования маршрутизатора;

u_{14} – обход межсетевого экрана.

Количественной характеристикой уровня m-ой, $m = 1, 2, \ldots, 14$, угрозы безопасности ПДн является вероятность:

$$P_m^{(У)} = 1 - \prod_{l=1}^{15} \left(1 - \alpha_{lm} \cdot P_l\right), \quad (9)$$

где P_l – соответствует выражению (8);

α_{lm} – коэффициент актуальности уязвимостей информации кадрового органа предприятия ОПК для инициализации угроз безопасности ПДн, равный 1, если *l*-я уязвимость актуальна для инициализации *m*-ой угрозы и 0, если не актуальна.

Значения коэффициента актуальности уязвимостей информации кадрового органа предприятия ОПК для инициализации угроз безопасности ПДн приводятся в табл. 1.

Таблица 1

Значения коэффициента актуальности уязвимостей информации для инициализации угроз безопасности ПДн

Угрозы безопасности ПДн	**Уязвимости ИС к реализации угроз безопасности ПДн**												
	b1	*b2*	*b3*	*b4*	*b5*	*b6*	*b7*	*b8*	*b9*	*b10*	*b11*	*b12*	*b13*
u1	1	0	0	0	1	1	0	0	0	1	1	1	1
u2	0	0	0	0	1	0	0	1	1	1	1	1	1
u3	1	1	1	0	1	0	0	1	1	1	1	1	1
u4	1	1	1	0	1	1	1	1	1	1	1	1	1
u5	1	1	1	0	0	0	0	0	0	0	1	1	1
u6	1	1	1	0	1	1	1	1	1	0	1	1	1
u7	1	1	1	0	0	0	1	0	0	0	1	0	0
u8	1	1	1	0	0	1	0	1	0	0	1	1	0
u9	1	1	1	0	0	1	0	1	0	0	1	1	0
u10	1	1	1	0	0	1	0	1	0	0	1	0	1
u11	1	1	0	0	0	0	0	0	0	0	1	0	0
u12	1	0	0	0	0	1	0	0	0	1	0	0	0
u13	1	0	0	0	0	1	0	0	1	1	0	0	0
u14	1	1	1	0	0	0	0	0	0	0	1	0	0

Количественной характеристикой деструктивного воздействия на информацию в результате реализации угроз безопасности ПДн [20, 21] кадрового органа предприятия ОПК является вероятность:

$$P_n^{(Д)} = 1 - \prod_{m=1}^{14} \left(1 - \delta_{mn} \cdot P_m^{(У)}\right), \quad (10)$$

где $P_m^{(У)}$ – соответствует выражению (2/37);

n – номер деструкции (1 – несанкционированное копирование ПДн, 2 – их несанкционированная модификация, 3 – блокирование доступа к информационным ресурсам ИС кадрового органа предприятия ОПК);

δ_{mn} – коэффициент деструкции, равный 1, если *m*-я угроза реализует *n*-ю деструкцию и 0, если не реализует.

Значения коэффициента деструкции угроз безопасности ПДн кадрового органа предприятия ОПК приводятся в табл. 2. В таблице использованы следующие условные обозначения деструкций: *НК* – несанкционированное копирование ПДн, *НМ* – несанкционированная модификация ПДн, *БД* – блокирование доступа к информационным ресурсам ИС кадрового органа предприятия ОПК.

Таблица 2

Значения коэффициента деструкции угроз безопасности ПДн кадрового органа предприятия ОПК

Деструкции	Угрозы безопасности ПДн													
	и1	*и2*	*и3*	*и4*	*и5*	*и6*	*и7*	*и8*	*и9*	*и10*	*и11*	*и12*	*и13*	*и14*
НК	1	1	0	1	0	0	1	1	0	1	1	0	0	1
НМ	1	0	1	1	1	1	1	0	0	1	1	0	0	1
БД	1	0	0	1	0	0	1	0	1	1	1	1	1	1

На основании изложенного вероятность $P_{(уб)}$ угрозы угроз безопасности ПДн кадрового органа предприятия ОПК определяется в соответствии с выражением:

$$P_{(уб)} = 1 - \prod_{n=1}^{3} \left(1 - P_n^{(Д)}\right). \quad (11)$$

Таким образом, с учетом выражений (8)-(10) выражение (11) следует рассматривать как математическую модель вероятностной характеристики возникновения угрозы безопасности ПДн кадрового органа предприятия ОПК.

Заключение. Фундаментальными свойствами, характеризующими возможности по обеспечению защиты ПДн кадрового органа предприятия ОПК является свойство эффективности соответствующих мер. Эффективность мер обеспечения безопасности ПДн кадрового органа предприятия ОПК определяется как их способность обеспечить заданный уровень качества деятельности кадрового органа предприятия ОПК в условиях угроз нарушения состояний защищенности ПДн. Тривиальность идеи экспертной оценки обстоятельств, влияющих на защищенность объектов информатизации, является предпосылкой широкого использования рассмотренного методического аппарата на практике, что является его несомненным достоинством. Что касается недостатков, то к ним следует отнести низкую адекватность формальной модели угроз безопасности ПДн, не учитывающей особенности действий нарушителя и формальной интерпретации динамики НСД к информации кадрового органа предприятия ОПК, не учитывающей случайные состояния процесса его обнаружения.

Задача исследования сводилась к разработке математической модели, характеризующей возможности предотвращения НСД к ПДн кадрового органа предприятия ОПК, как упорядоченного, за счет структурной согласованности с соответствующими функциональными моделями, множества, что позволяет повысить адекватность оценки и обеспечить обоснованность требований к способам и средствам обеспечения защищенности ИСПДн рассматриваемого класса от НСД к информации.

В соответствии с исходными данными при моделировании исследуемых процессов с целью определения показателей, характеризующих возможности предотвращения НСД к ПДн кадрового органа предприятия ОПК, используются значения времени реализации функций выявления признаков соответствующих действий нарушителя. Данная характеристика является измеряемой, ее значения фиксируются

соответствующими компонентами операционной системы и представляются случайными выборками. Вид аналитических моделей временных характеристик угроз НСД к ПДн кадрового органа предприятия ОПК и процессов предотвращения такого рода угроз определяется функциональными моделями этих процессов. Учитывая выше изложенное построенная математическая модель оценки возможностей предотвращения НСД к ПДн кадрового органа предприятия ОПК позволяет количественно оценивать показатель эффективности мер обеспечения безопасности ПДн.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. https://ru.wikipedia.org/wiki/Эффективность_(философия).
2. Закон Российской Федерации «О персональных данных» от 27 июля 2006 г. № 152-ФЗ // Рос. газ. – 29 июля 2006.
3. *Покусов В.В.* Оценка эффективности системы обеспечения ИБ. Ч. 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.
5. *Кондаков С.Е., Чудин К.С.* Разработка исследовательского аппарата оценки эффективности мер обеспечения защиты персональных данных // Вопросы кибербезопасности. – 2021. – № 5 (45). – С. 45-51.
6. *Мирошниченко Е.Л., Пасечник Р.М., Болычев М.В.* Алгоритм построения диаграммы достижимости модели состояния работоспособности информационной системы // Вопросы кибербезопасности. – 2019. – № 6 (34). – С. 79-91.
7. *Щеглов А.Ю., Щеглов К.А.* Математические модели и методы формального проектирования систем защиты информационных систем: учеб. пособие по дисциплине «Безопасность вычислительных систем и сетей». – СПб., 2015.
8. Probabilistic Modeling in System Engineering / by ed. A. Kostogryzov. – London: IntechOpen, 2018. – 278 p. 10.5772/ intechopen.71396. – DOI: 10.5772/intechopen.71396.
9. *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.
10. Методический документ. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. ФСТЭК России 14.02.2008.
11. Методический документ. Методика оценки угроз безопасности информации. Меры защиты информации в государственных информационных системах. Методический документ ФСТЭК России. Утвержден 11 февраля 2014 г. ии, утв. ФСТЭК России 05.02.2021.
12. *Мещерякова Т.В., Скрыль С.В., Фирюлин М.Е.* Математические модели информационных процессов в автоматизированных информационных системах органов внутренних дел в условиях простейшей модели нарушения безопасности информации: монография. – Воронеж: Воронежский институт МВД России, 2017. – 124 с.
13. *Скрыль С.В., Кондаков С.Е., Чудин К.С.* Обоснование показателя для оценки эффективности мер обеспечения защиты персональных данных в деятельности кадрового органа службы защиты государственной тайны // Информационная безопасность – актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности: Матер. XXI Всероссийской межведомственной научно-технической конференции. Т. 1. – Краснодар: КВВУ, 2020. – С. 19-24.
14. *Казарин О.В., Кондаков С.Е., Троицкий И.И.* Подходы к количественной оценке защищенности информационных ресурсов автоматизированных систем // Вопросы кибербезопасности. – 2015. – № 2 (10). – С. 31-35.
15. *Скрыль С.В., Гайфулин В.В., Сычев В.М., Грачева Ю.В. [и др.].* Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры // Безопасность информационных технологий. – 2021. – № 1. – С. 24-33.
16. *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.

17. *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.
18. *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.
19. *Лившиц И.И.* Оценка степени влияния General Data Protection Regulation на безопасность предприятий в Российской Федерации // Вопросы кибербезопасности. – 2020. – № 4 (38). – С. 66-75.
20. *Хасин Е.В., Астрахов А.В., Кондаков С.Е. [и др.].* Безопасность операционных систем: учебное пособие для системы высшего профессионального образования / под ред. С.В. Скрыля. – М.: Издательский центр «Академия», 2021. – 256 с.
21. *Скрыль С.В., Шелупанов А.А.* Основы системного анализа в защите информации: учеб. пособие для студентов высших учебных заведений. – М.: Машиностроение, 2008. – 138 с.

REFERENCES

1. Available at: https://ru.wikipedia.org/wiki/Effektivnost'_(filosofiya).
2. Zakon Rossiyskoy Federatsii «O personal'nykh dannykh» ot 27 iyulya 2006 g. № 152-FZ [The Law of the Russian Federation "On Personal Data" dated July 27, 2006 No. 152-FZ], *Ros. gaz.* [Russian Gas], 29 iyulya 2006.
3. *Pokusov V.V.* Otsenka effektivnosti sistemy obespecheniya IB. Ch. 1. Pokazateli i modeli predstavleniya [Evaluation of the effectiveness of the information security system. Part 1. Indicators and presentation models], *Zashchita informatsii. Insayd* [Information protection. Inside], 2019, No. 2 (86), pp. 54-60.
4. *Yazov Yu.K., Avsent'ev O.S., Rubtsova I.O.* K voprosu ob otsenke effektivnosti zashchity informatsii v sistemakh elektronnogo dokumentooborota [On the issue of evaluating the effectiveness of information protection in electronic document management systems], *Voprosy kiberbezopasnosti* [Cybersecurity issues], 2019, No. 1 (29), pp. 25-34.
5. *Kondakov S.E., Chudin K.S.* Razrabotka issledovatel'skogo apparata otsenki effektivnosti mer obespecheniya zashchity personal'nykh dannykh [Development of a research apparatus for evaluating the effectiveness of measures to ensure the protection of personal data], *Voprosy kiberbezopasnosti* [Issues of cybersecurity], 2021, No. 5 (45), pp. 45-51.
6. *Miroshnichenko E.L., Pasechnik R.M., Bolychev M.V.* Algoritm postroeniya diagrammy dostizhimosti modeli sostoyaniya rabotosposobnosti informatsionnoy sistemy [Algorithm for constructing a diagram of the reachability of an information system health state model], *Voprosy kiberbezopasnosti* [Questions of cybersecurity], 2019, No. 6 (34), pp. 79-91.
7. *Shcheglov A.Yu., Shcheglov K.A.* Matematicheskie modeli i metody formal'nogo proektirovaniya sistem zashchity informatsionnykh sistem: ucheb. posobie po distsipline «Bezopasnost' vychislitel'nykh sistem i setey» [Mathematical models and methods of formal design of information systems protection systems: a textbook on the discipline "Security of computing systems and networks"]. St. Petersburg, 2015.
8. Probabilistic Modeling in System Engineering, by ed. A. Kostogryzov. London: IntechOpen, 2018, 278 p. 10.5772/ intechopen.71396. DOI: 10.5772/intechopen.71396.
9. *Buldakova T.I., Mikov D.A.* Obespechenie soglasovannosti i adekvatnosti otsenki fakto-rov riska informatsionnoy bezopasnosti [Ensuring consistency and adequacy of information security risk factors assessment], *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2017, No. 3 (21), pp. 8-15. DOI: 10.21681/2311-3456-2017-3-08-15.
10. Metodicheskiy dokument. Metodika opredeleniya aktual'nykh ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh, utv. FSTEK Rossii 14.02.2008 [Methodical document. Methodology for determining the actual threats to the security of personal data when they are processed in personal data information systems, approved by the FSTEC of Russia on 02/14/2008].
11. Metodicheskiy dokument. Metodika otsenki ugroz bezopasnosti informatsii. Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh. Metodicheskiy dokument FSTEK Rossii. Utverzhden 11 fevralya 2014 g. ii, utv. FSTEK Rossii 05.02.2021 [Methodical document. Methodology for assessing information security threats. Information protection measures in state information systems. Methodological document of the FSTEC of Russia. Approved on February 11, 2014 by the ai, approved by the FSTEC of Russia 05.02.2021].

12. *Meshcheryakova T.V., Skryl' S.V., Firyulin M.E.* Matematicheskie modeli informatsionnykh protsessov v avtomatizirovannykh informatsionnykh sistemakh organov vnutrennikh del v usloviyakh prosteyshey modeli narusheniya bezopasnosti informatsii: monografiya [Mathematical models of information processes in automated information systems of internal affairs bodies in the conditions of the simplest model of information security violations: monograph]. Voronezh: Voronezhskiy institut MVD Rossii, 2017, 124 p.
13. *Skryl' S.V., Kondakov S.E., Chudin K.S.* Obosnovanie pokazatelya dlya otsenki effektivnosti mer obespecheniya zashchity personal'nykh dannykh v deyatel'nosti kadrovogo organa sluzhby zashchity gosudarstvennoy tayny [Substantiation of the indicator for evaluating the effectiveness of measures to ensure the protection of personal data in the activities of the personnel body of the state secret protection service], *Informatsionnaya bezopasnost' – aktual'naya problema sovremennosti. Sovershenstvovanie obrazovatel'nykh tekhnologiy podgotovki spetsialistov v oblasti informatsionnoy bezopasnosti: Mater. XXI Vserossiyskoy mezhvedomstvennoy nauchno-tekhnicheskoy konferentsii* [Information security is an urgent problem of our time. Improving educational technologies for training specialists in the field of information security: Materials of the XXI All-Russian Interdepartmental Scientific and Technical Conference]. Vol. 1. Krasnodar: KVVU, 2020, pp. 19-24.
14. *Kazarin O.V., Kondakov S.E., Troitskiy I.I.* Podkhody k kolichestvennoy otsenke zashchishchennosti informatsionnykh resursov avtomatizirovannykh sistem [Approaches to quantifying the security of information resources of automated systems], *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2015, No. 2 (10), pp. 31-35.
15. *Skryl' S.V., Gayfulin V.V., Sychev V.M., Gracheva Yu.V. [i dr.].* Aktual'nye voprosy problematiki otsenki ugroz komp'yuternykh atak na informatsionnye resursy znachimykh ob"ektov kriticheskoy informatsionnoy infrastruktury [Topical issues of the problem of assessing threats of computer attacks on information resources of significant objects of critical information infrastructure], *Bezopasnost' informatsionnykh tekhnologiy* [Information technology security], 2021, No. 1, pp. 24-33.
16. *Kondakov S.E., Meshcheryakova T.V., Skryl' S.V., Stadnik A.N., Suvorov A.A.* Veroyatnostnoe predstavlenie usloviy svoevremennogo reagirovaniya na ugrozy komp'yuternykh atak [Probabilistic representation of conditions for timely response to threats of computer attacks], *Voprosy kiberbezopasnosti* [Questions of cybersecurity], 2019, No. 6 (34), pp. 59-68. DOI: 10.21681/2311-3456-2019-6-59-68.
17. *Maksimova E.A., Kuznetsova M.A., Topilin Ya.N., Fedonyuk N.I., Petrishcheva T.S.* Vnutrenniy kontrol' sootvetstviya obrabotki PDn trebovaniyam k ikh zashchite [Internal control of compliance of PD processing with the requirements for their protection], *Zashchita informatsii. Insayd* [Information protection. Inside], 2019, No. 6 (90), pp. 5-9.
18. *Terent'eva L.V.* Kriteriy «napravlennoy deyatel'nosti» primenitel'no k otnosheniyam, svyazannym s zashchitoy personal'nykh dannykh [Criterion of "directed activity" in relation to relations related to the protection of personal data], *Pravovaya informatika* [Legal Informatics], 2021, No. 1, pp. 61-69. DOI: 10.21681/1994-1404-2021-1-61-69.
19. *Livshits I.I.* Otsenka stepeni vliyaniya General Data Protection Regulation na bezopasnost' predpriyatiy v Rossiyskoy Federatsii [Assessment of the impact of General Data Protection Regulation on the security of enterprises in the Russian Federation], *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2020, No. 4 (38), pp. 66-75.
20. *Khasin E.V., Astrakhov A.V., Kondakov S.E. [i dr.].* Bezopasnost' operatsionnykh sistem: ucheb. posobie dlya sistemy vysshego professional'nogo obrazovaniya [Security of operating systems: a textbook for the system of higher professional education], ed. by S.V. Skrylya. Moscow: Izdatel'skiy tsentr «Akademiya», 2021, 256 p.
21. *Skryl' S.V., Shelupanov A.A.* Osnovy sistemnogo analiza v zashchite informatsii: ucheb. posobie dlya studentov vysshikh uchebnykh zavedeniy [Fundamentals of system analysis in the protection of information: a textbook for students of higher educational institutions]. Moscow: Mashinostroenie, 2008, 138 p.

Статью рекомендовал к опубликованию д.т.н., профессор В.В. Курейчик.

Кондаков Сергей Евгеньевич – Московский государственный технический университет им. Н.Э. Баумана; e-mail: sergeikondakov@list.ru; г. Москва, Россия, тел.: +79037947857; кафедра защиты информации; к.т.н.

Чудин Кирилл Сергеевич – e-mail: 4ydo-kirill@rambler.ru; тел.: +79653295515; кафедра защиты информации; ассистент.

Болычев Максим Владимирович – e-mail: Nat15171@yandex.ru; тел.: +79167260955; кафедра защиты информации; соискатель.

Kondakov Sergey Evgenievch – Bauman Moscow State Technical University; e-mail: sergeikondakov@list.ru; Moscow, Russia; phone: +79037947857; the department of information security; can. of eng. sc.

Chudin Kirill Sergeevich – e-mail: 4ydo-kirill@rambler.ru; phone: +79653295515; the department of information security; assistant.

Bolychev Maxim Vladimirovich – e-mail: Nat15171@yandex.ru; phone: +79167260955; the department of information security; applicant.

УДК 004.067 DOI 10.18522/2311-3103-2023-2-80-89

Ю.А. Брюхомицкий

ИММУНОЛОГИЧЕСКАЯ МОДЕЛЬ КЛАВИАТУРНОГО МОНИТОРИНГА ОПЕРАТОРОВ ИНФОРМАЦИОННЫХ СИСТЕМ

Целью работы является разработка модели клавиатурного мониторинга операторов информационных систем, основанной на использовании цепочного метода учета параметров клавиатурного почерка. Указанный метод предусматривает оценку клавиатурного почерка оператора на цепочках символов заданной длины, отражающих лингвистически связанные параметры клавиатурного набора, характерные для данного оператора. Клавиатурный набор таких цепочек оператором с «хорошим» клавиатурным почерком обладает существенно более высокой индивидуальностью, обусловленной корреляционными зависимостями между временными параметрами последовательно идущих символов и пауз. В итоге цепочный метод позволяет обеспечить более высокую точность верификации личности оператора. Клавиатурный мониторинг на основе цепочного метода предлагается реализовать в базисе искусственных иммунных систем с использованием иммунологической модели клональной селекции, в которой детекторы представлены идентификационными параметрами области распределения клавиатурных параметров «своего». В задачах клавиатурного мониторинга область распределения клавиатурных параметров верифицируемого оператора всегда существенно меньше совокупной области распределения клавиатурных параметров других возможных операторов. Выбор указанной модели позволяет существенно снизить необходимый объем популяции детекторов, и как следствие, – существенно сократить время верификации работающего оператора. Принятие решения о подмене «своего» оператора «чужим» предлагается считать обоснованным при превышении частоты срабатывания детекторов установленного порогового значения. Предложенная иммунологическая модель обладает рядом преимуществ. Использование цепочного метода учета клавиатурных параметров позволяет с бóльшей точностью верифицировать оператора, в сравнении с традиционными методами. Используемая модель клональной селекции в сочетании с векторным представлением клавиатурных данных позволяет существенно ускорить процесс обучения и сократить время, необходимое для своевременного принятия решения о присутствии «чужого» оператора. Важным достоинством модели является возможность обучаться исключительно на примерах клавиатурного почерка оперативно доступных «своих» операторов. Использование модели клональной селекции позволяет также существенно снизить необходимый объем популяции детекторов, способных эффективно «покрыть» область распределения клавиатурных параметров «своего» оператора.

Цепочный метод клавиатурного мониторинга операторов информационных систем; иммунологическая модель клональной селекции с положительным отбором; верификация работающего оператора по принципу «свой-чужой».