Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт Космических и Информационных Технологий
Кафедра прикладной математики и компьютерной безопасности

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А. А. Кытманов
подпись
« ____» _____ 2018 г.

БАКАЛАВРСКАЯ РАБОТА

01.03.04 Прикладная математика

Математические модели обеспечения безопасности информационных систем с учетом человеческого фактора

Руководитель _____ доцент. И.З.Краснов
подпись, дата

Выпускник _____ А. А.Истягин
подпись, дата

Красноярск 2018

РЕФЕРАТ

Выпускная квалификационная работа по теме «Математические модели обеспечения безопасности информационных систем с учетом человеческого фактора» содержит 35 страниц текстового документа и 13 источников.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, ДИФФЕРЕНЦИАЛЬНАЯ ПСИХОЛОГИЯ, УРОВЕНЬ КОМПЕТЕНТНОСТИ, ЧЕЛОВЕЧЕСКИЙ ФАКТОР, МОДЕЛЬ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ, РЕГРЕССИОННЫЙ АНАЛИЗ.

Цели работы: 1. Проанализировать существующие модели обеспечивающие безопасность информационной системы.

2. На основе анализа выявить недостатки и с учетом их смоделировать новую математическую модель обеспечивающую безопасность информационной системы с учётом человеческого фактора.

3. Провести регрессионный анализ для моделей и сравнить результаты.

Ожидаемый результат: Показать, что модель, учитывающая человеческий фактор, даёт более точные результаты.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ……5
1 Математическое моделирование и функциональные задачи безопасности информационной системы……..…….…6
1.1 Понятие математической модели…….…...6
1.2 Классификация и свойства мат. моделей……....8
1.3 Основные этапы мат. моделирования…….…...10
1.4 Модель анализа защищенности персонала информационной системы от социоинженерных атак**.**……..……..…11
1.5 Модель стимулирования пользователя центром в информационной системе ……...16
1.6 Анализ моделей……...17
2 Разработка математической модели безопасности информационных систем с учётом человеческого фактора…….19
2.1 Человеческий фактор как основной источник угроз безопасности КИС…….....19
2.2 Основы дифференциальной психологии…….....20
2.3 Типология Юнга…….....21
2.4 Психологические свойства пользователя, компетентность…….....23
2.5 Математическая модель безопасности информационных систем с учётом человеческого фактора……....27
3 Статистический анализ эффективности разработанной модели в сравнении с рассмотренными моделями……29
3.1 Метод исследования……...29
3.2 Анализ разработанной модели безопасности с учётом человеческого фактора……...29
3.3Анализ модели анализа защищенности персонала информационной системы от социоинженерных атак…….……....30

3.4 Сравнение результатов и выводы…….……32
ЗАКЛЮЧЕНИЕ…….....34
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ……..…….…..35

ВВЕДЕНИЕ

Вторая половина XX века связана с появлением и широким распространением новой методологии исследования сложных объектов и систем. В ее основе лежит метод математического моделирования и реализованные на его основе вычислительные эксперименты. Математические модели использовались и раньше, однако считалось, что методы математического моделирования не пригодны для исследования сложных технических, экономических, биологических и социальных систем.

Положение начало меняться во второй половине XX в. при развитии средств вычислительной техники, в частности современных ЭВМ, которое дало в руки исследователей новое эффективное средство моделирования сложных систем. В настоящее время не существует объектов, при изучении которых не применялись бы методы математического моделирования.

Разработаны и активно используются математические модели технических устройств, модели разнообразных технологических процессов, экономические модели предприятий, модели социальных систем, модели обеспечивающие безопасность систем и др.

Актуальность данной работы заключается в том, что современные методы разработки математических моделей безопасности являются недостаточно точными, так как не учитывают человеческий фактор. В данной работе рассмотрены и проанализированы уже существующие модели, вывялены их достоинства недостатки, предложена скорректированная математическая модель обеспечения безопасности информационных систем с учётом человеческого фактора.

Цель работы: Изучить и проанализировать существующие модели защищенности персонала информационной системы от социоинженерных атак. Провести анализ достоинств и недостатков моделей обеспечения безопасности информационных систем; внести дополнительные переменные учитывающие человеческий фактор. На основе изученного разработать модель

безопасности информационной системы.

1 Математическое моделирование и функциональные задачи безопасности информационной системы.

1.1 Понятие математической модели

По Ляпунову, математическое моделирование — это опосредованное практическое или теоретическое исследование объекта, при котором непосредственно изучается не сам интересующий нас объект, а некоторая вспомогательная искусственная или естественная система (модель), находящаяся в некотором объективном соответствии с познаваемым объектом, способная замещать его в определённых отношениях и дающая при её исследовании, в конечном счёте, информацию о самом моделируемом объект.

Математическое моделирование позволяет до создания реальной системы (объекта) или возникновения реальной ситуации рассмотреть возможные режимы работы, выбрать оптимальные управляющие воздействия, составить объективный прогноз будущих состояний системы. Вычислительные эксперименты, проводимые на основе математических моделей, помогают увидеть за частным общее, развить универсальные методы анализа объектов различной физической природы, познать свойства изучаемых процессов и систем. Наконец, математическое моделирование является основой интенсивно разрабатываемых автоматизированных систем проектирования, управления и обработки данных.

Важнейшей характеристикой моделей является их точность, адекватность действительности. При этом важно иметь в виду, что все модели представляют собой приближенное описание реальных объектов (процессов) и поэтому принципиально неточны. Интегральная оценка модели может быть получена путем сравнения результатов моделирования и экспериментальных данных для конкретных объектов в нашем случае дифференциация

пользователей информационной системы по психологически свойствам. Для оценки значимости совпадения или несовпадения модельных и экспериментальных результатов широко используются методы математической статистики. Вместе с тем не следует переоценивать результаты такой проверки. Хорошее совпадение модельных и экспериментальных данных, вообще говоря, не доказывает точности модели, а лишь подтверждают ее функциональную пригодность для моделирования. Всегда может быть предложена модель, обеспечивающая лучшее совпадение с экспериментом, но не лучшее описание моделируемого объекта или процесса. [1]

Схема применения математической модели при решении реальных задач имеет вид, показанный на рис. 1

Рисунок 1 – Схема применения математической модели

1.2 Классификация математических моделей и их свойства

Существует несколько схем классификации математических моделей. Все они достаточно условны. Одна из таких схем приведена на рис. 2

Рисунок 2 – Схема классификации математических моделей

Все математические модели по использованному формальному языку можно разбить на аналитические и имитационные.

Аналитические – модели, в которых используется стандартный математический язык.

Имитационные – модели, в которых использован специальный язык моделирования или универсальный язык программирования.

Аналитические модели могут быть записаны в виде формул или уравнений. Если какой-либо процесс не может быть описан в виде аналитической модели, его описывают с помощью специального алгоритма

или программы. Такая модель является имитационной.

Аналитические модели в свою очередь разбиваются на теоретические и эмпирические модели. Теоретические модели отражают реальные структуры и процессы в исследуемых объектах, то есть, опираются на теорию их работы. Эмпирические модели строятся на основе изучения реакций объекта на изменение условий окружающей среды. При этом теория работы объекта не рассматривается, сам объект представляет собой так называемый «черный ящик», а модель – некоторую интерполяционную зависимость.

Эмпирические модели могут быть построены на основе экспериментальных данных. Эти данные получают непосредственно на исследуемых объектах или с помощью их физических моделей. По форме описания аналитические модели подразделяются на линейные и нелинейные. Если все входящие в модель величины не зависят от времени, то имеем статическую модель объекта или процесса, в противном случае получаем динамическую модель. В детерминированных моделях все взаимосвязи, переменные и константы заданы точно, что приводит к однозначному определению результирующей функции. Если часть или все параметры, входящие в модель по своей природе являются случайными величинами или случайными функциями, то модель относят к классу стохастических моделей. В стохастических моделях задаются законы распределения случайных величин, что приводит к вероятностной оценке результирующей функции. Если аналитическое исследование может быть доведено до конца, модели называются аналитически разрешимыми. В противном случае говорят о численно разрешимых аналитических моделях.

1.3 Основные этапы разработки математической модели

В математическом моделировании можно выделить следующие основные этапы:

1. Первым этапом математического моделирования является постановка задачи, определение объекта и целей исследования, задание критериев (признаков) изучения объектов и управления ими. Неправильная или неполная постановка задачи может свести на нет результаты всех последующих этапов.
2. Вторым этапом моделирования является выбор типа математической модели, что является важнейшим моментом, определяющим направление всего исследования. Обычно последовательно строится несколько моделей. Сравнение результатов их исследования с реальностью позволяет установить наилучшую из них. На этапе выбора типа математической модели при помощи анализа данных поискового эксперимента устанавливаются: линейность или нелинейность, динамичность или статичность, стационарность или нестационарность, а также степень детерминированности исследуемого объекта или процесса.
3. Процесс выбора математической модели объекта заканчивается ее предварительным контролем, который также является первым шагом на пути к исследованию модели. При этом осуществляются следующие виды контроля (проверки): размерностей; порядков; характера зависимостей; экстремальных ситуаций; граничных условий; математической замкнутости; физического смысла; устойчивости модели.

Контроль размерностей сводится к проверке выполнения правила, согласно которому приравниваться и складываться могут только величины одинаковой размерности.

Контроль порядков величин направлен на упрощение модели. При этом определяются порядки складываемых величин и явно малозначительные слагаемые отбрасываются.

Анализ характера зависимостей сводится к проверке направления и скорости изменения одних величин при изменении других. Направления и скорость, вытекающие из ММ, должны соответствовать физическому смыслу задачи.

Анализ экстремальных ситуаций сводится к проверке наглядного смысла решения при приближении параметров модели к нулю или бесконечности.

Контроль граничных условий состоит в том, что проверяется соответствие ММ граничным условиям, вытекающим из смысла задачи. При этом проверяется, действительно ли граничные условия поставлены и учтены при построении искомой функции и что эта функция на самом деле удовлетворяет таким условиям.

Анализ математической замкнутости сводится к проверке того, что ММ дает однозначное решение.

Анализ физического смысла сводится к проверке физического содержания промежуточных соотношений, используемых при построении ММ.

Проверка устойчивости модели состоит в проверке того, что варьирование исходных данных в рамках имеющихся данных о реальном объекте не приведет к существенному изменению решения. [2]

1.4 Модель анализа защищенности персонала информационной системы от социоинженерных атак

Данная модель была разработана М.В. Абрамовым, А.А. Азаровым, Т.В. Тульпевой и А.Л. Тульпьевым. Целью данной модели является оценка защищённости информационной системы от социоинженерных атак, а так же для выявления наиболее уязвимых звеньев системы.

Под социоинженерной атакой подразумевается такое воздействие на пользователя S, которое сподвигнет пользователя совершать действия

выгодные злоумышленнику M и подвергать информационную систему негативным воздействиям. [3]

Имеется корпоративная информационная система (КИС) в которой критические ресурсы подвергаются внешним и внутренним негативным воздействиям (угрозам) которые могут привести к нарушению функционирования и работоспособности информационной системы. В частности рассматривается социоинженерная атака злоумышленника на пользователя.

Под КИС подразумевается масштабируемая информационно – вычислительная система, предназначенная для комплексной автоматизации всех видов хозяйственной деятельности больших и средних предприятий, в том числе корпораций, состоящих из группы компаний, требующих единого управления. Объединяет систему управления персоналом, материальными, финансовыми и другими ресурсами компании, используется для поддержки планирования и управления компанией, для поддержки принятия управленческих решений ее руководителями.

Под негативными воздействиями будем понимать воздействие злоумышленника на субъект (пользователя) S информационной системы, с целью завладеть ресурсами, к которым есть доступ у пользователя. [4]

Модель пользователя:

Пользователь S может быть представлен в виде S= {C, Z, PV, L}, где

C – критические ресурсы, к которым имеется доступ у пользователя;

Z – контролируемые пользователем зоны;

PV – профиль уязвимостей пользователя (ПУП);

L – матрица взаимоотношений пользователей.

Множество параметров C представляет собой l элементов c_i, которые характеризуют уровень доступа к, соответствующему номеру, критическому ресурсу и принимают значения 0,1,2. Где

0 – Пользователь не имеет доступа к критическому ресурсу;

1 – Пользователь имеет только доступ на чтение;

2 – Пользователь имеет доступ к редактированию и удалению.

Множество параметров Z представляет собой m элементов z_i, которые характеризуют наличие доступа у пользователя к, соответствующей номеру, контролируемой зоне и принимают значения 0,1. Где

0 – Пользователь не имеет доступа к контролируемой зоне;

1 – Пользователь имеет доступ к контролируемой зоне.

Модель злоумышленника:

Злоумышленник M может быть представлен в виде $M=\{R, S_0, U_0, P, G\}$, где

R – ресурсы, к которым есть доступ у злоумышленника, а так же его личностные особенности;

S_0 – пользователи S, к которым злоумышленник имеет доступ до момента негативного воздействия (атаки);

U_0 – начальные знания злоумышленника об архитектуре информационной системы;

P – профиль компетенций злоумышленника (КПЗ);

G – цели злоумышленника.

Множество параметров U_0 представляет собой набор S_i, i = 1..n, при этом параметры принимают следующие значения -1,0,1,2. Где

-1 – Злоумышленник не знает, какие именно права доступа у пользователя;
0 – Злоумышленник знает, что пользователь не имеет доступа к ресурсу;
1 – Злоумышленник знает, что пользователь имеет только доступ к чтению;
2 – Злоумышленник знает, что пользователь имеет доступ к редактированию и удалению.

Более подробно рассмотрим параметр P. Данный параметр может быть охарактеризован известными злоумышленнику навыками социоинженерного атакующего воздействия. Опираясь на опыт исследований аппаратных и программно-технических аспектов информационной безопасности и

адаптируя его к области социоинженерных атак, можно ожидать, что для построения и регулярного последующего пополнения списков атакующих воздействий, ресурсов и прочих параметров, входящих в ПКЗ, а также подходов к их оценке потребуется отдельное и непрерывно длящееся междисциплинарное исследование при участии специалистов по психологии, социологии, информатике и математике.

Таким образом, параметр P может быть представлен следующим образом $P = ((K_1,D(K_1)),..,(K_q,D(K_q)))$, где K_i – это атакующее социоинженерное воздействие, а $D(K_i)$ – это уровень владения навыком данного социоинженерного воздействия. Поскольку каждому злоумышленнику сопоставлен свой параметр P, то для каждого j-того злоумышленника будет свой ПКЗ. То есть $P_j = ((K_1,D_j(K_1)),..,(K_q,D_j(K_q)))$. Таки образом, формализовав параметр P, без учёта параметра PV пользователя, можно огрубленным оценкам вероятности успеха социоинженерных атакующих воздействий злоумышленника p_{ij} представленных в виде $p_{ij} = f(D_j(K_i), T_i)$, где T_i – максимально возможная степень владения атакующим воздействием, а p_{ij} – это вероятность успеха i-той атаки, у j-того злоумышленника. И p_{ij} может принимать вид: $p_{ij} = f(D_j(K_i), T_i) = D_j(K_i) / T_i$. Таким образом, мы переходим от степени владения атакующим воздействием, применяемым злоумышленником, к вероятности успеха социоинженерного атакующего воздействия на пользователя, и параметр P приобретает вид: $p_{1j},..,p_{qj}$. [5]

Стоит учитывать, что модели пользователя информационной системы сопоставлен параметр PV, в который входят степени выраженности уязвимостей (степени его подверженности атакующим социоинженерным воздействиям) пользователя, на основании которых оценивается успех атаки злоумышленника. Существует предположение, что рассмотрение ПКЗ позволит произвести более точную оценку защищённости пользователя информационной системы.

Функция расчёта вероятности успеха такого воздействия при заданных PV и P в простейшем варианте может быть представлена в следующем виде: $p^{lq}_{ij} = g(D_j(K_i), T_i, S_q(V_l, K_i), B_i)$. Одним из возможных примеров данной функции может быть : $p^{lq}_{ij} = g(D_j(K_i), T_i, S_q(V_l, K_i), B_i) = D_j(K_i)S_q(V_l, K_i) / T_i B_i$. Где: $S_q(V_l, K_i)$ – выраженность уязвимости V_l; B_l – максимальная выраженность уязвимости V_l, а p^{lq}_{ij} – Это вероятность успеха социоинженерного атакующего воздействия j-го злоумышленника с использованием его i-го ресурса на l-ю уязвимость k-го пользователя.

Введём функцию $\varphi_{il}(K_i, V_l)$, которая будет содержать в себе оценку вероятности успеха атаки при использовании злоумышленником определенного атакующего воздействия на определенную уязвимость пользователя. Где K_i – это типа атакующего воздействия, а V_l – уязвимость, на которую воздействует злоумышленник. Значения данной функции лежат на отрезке [0,1] где 0 – злоумышленник не имеет воздействия на уязвимость пользователя, 1 – злоумышленник добьётся успеха при воздействии на данную уязвимость.

Для примера, атакующем воздействием может быть: предложение зарегистрироваться на каком-то привлекательном сайте, взлом, подкуп и др., касаемо уязвимостей могут быть следующие варианты: техническая халатность, получение собственной выгоды и др. Примеры можно увидеть в таблице 1.

Таблица 1 - Атакующие воздействия злоумышленника и уязвимости пользователей

Уязвимости пользователей	Атакующие действия			
	Взлом	Подкуп	Бесплатная помощь в настройке ПО	Ссылка на подозрительный сайт
Ненадёжный пароль	1	0	0	0
Техническая	0,9	0	1	0,9

халатность				
Получение собственной выгоды	0	1	0,9	0

Таким образом, с учётом вышеописанной функции конечная формула принимает вид $p^{lq}_{ij} = g(D_j(K_i), T_i, S_q(V_l, K_i), B_i)\ \varphi_{il}(K_i, V_l)$.

1.5 Модель стимулирования пользователя в информационной системе

Данная модель была разработана Д.А. Новиковым и С.Н. Петраковым. Целью данной модели является стимулирование пользователя наиболее выгодным для ЛПР образом.

В данной модели лицо, принимающее решения (ЛПР) воздействует на пользователя (субъекта) стимулируя его деятельность так, чтобы пользователь совершал выгодные для ИС действия, тем самым максимизировал доход и минимизировал риски негативных воздействий.

Предполагается, что взаимодействие ЛПР с пользователем подчиняется теории игр. ЛПР выбирает стратегии так, чтобы максимизировать выгоду для предприятия, а пользователь выбирает так, чтобы максимизировать выгоду для себя, чем порой оказывает негативное воздействие на информационную систему. Модель стимулирования строится таким образом, что ЛПР стимулирует пользователя посредством некоторых правил так, чтобы пользователь выбрал выгодную для ЛПР стратегию. [6]

ЛПР обладает правом первого хода, причем его стратегия – функция от стратегии второго игрока – пользователя, то есть в качестве стратегии $\eta \in U$ центр выбирает функцию $\sigma(y) \in M$, где y - стратегия пользователя, M – множество допустимых функций стимулирования.

При рассмотрении задач стимулирования стратегия первого игрока интерпретируется как функция стимулирования, определяющая поощрение или наказание активного элемента в зависимости от выбираемой им стратегии (действия) и входящая аддитивно в функцию полезности пользователя.

Функция полезности пользователя представляется в одном из двух следующих видов:

$$u(x, z, r, \sigma(.)) = \begin{cases} \sigma(x, z) - c(z, r) - \text{"стимулирование минус затраты"} \\ h(z, r) - \chi(x, z) - \text{"доход минус штрафы"} \end{cases}$$

где

$h^{(}z, r)$ - функция дохода пользователя, h: $A_0 \times \Omega \rightarrow A^1$;

c(z, r) - функция дохода пользователя, c: $A_0 \times \Omega \rightarrow A^1$;

$\sigma(x, z) \epsilon M$ - функция стимулирования пользователя центром, σ: $X \times A_0 \rightarrow R^1|M$;

$\chi(x, z)$ - функция штрафов, налагаемых на пользователя центром,

χ: $X \times A_0 \rightarrow R^1|M$.

В данной постановке стимулирование (изменение предпочтений пользователя центром) осуществляется путем поощрения или наказания пользователя за выбор тех или иных действий, то есть путем изменения его функции полезности. Таким образом, стимулирование заключается либо в прибавлении к функции полезности пользователя функции стимулирования, либо в прибавлении к функции полезности пользователя функции стимулирования и одновременном вычитании этой функции из целевой функции центра.

Механизм стимулирования (механизм управления) определяется заданием функции стимулирования $\sigma^{\sim}$: $X \times A_0 \rightarrow R^1|M$, где

X - множество допустимых планов пользователя;

A_0 - множество возможных результатов деятельности;

$R^1|M$ - множество возможных значений функции стимулирования– подмножество R^1, определяемое ограничениями механизма стимулирования M.

1.6 Анализ моделей

Проведём анализ вышеописанных моделей, опишем их сильные и слабые стороны.

Сильные и слабые стороны модели анализа защищенности персонала информационной системы от социоинженерных атак приведены ниже в таблице 2.

Таблица 2 – Сильные и слабые стороны модели анализа защищенности информационной системы

Сильные стороны	Слабые стороны
Позволяет рассчитать вероятность успеха атаки, из знаний о пользователях.	Модель не рассматривает психологические свойства злоумышленника и психологические свойства пользователя, который напрямую воздействует на уязвимости и на успех атаки.
Модель хорошо анализирует и оценивает внешние воздействия на пользователей.	Модель рассматривает воздействие типа: злоумышленник – пользователь – ИС, но не рассматривает ситуацию: пользователь (инсайдер) – ИС.
Подходит для любой информационной системы.	
Модель учитывает разнообразные типы атаки и их успех.	

Сильные и слабые стороны модели стимулирования пользователя центром в информационной системе приведены ниже в таблице 3.

Таблица 3 – Сильные и слабые стороны модели стимулирования

Сильные стороны	Слабые стороны
Модель хорошо работает для случая внутренних воздействий и предотвращает их.	Модель не учитывает случай внешних воздействий на системы и никак не может на них повлиять.
Модель не столько уменьшает вероятность атаки, сколько максимизирует прибыль на выходе, так что даже в случае атаки, конечная прибыль оправдывает это.	Модель не учитывает психологических свойства пользователя, что может повлиять на выбор стратегии, тем самым негативно воздействовать на ИС.
Универсальность модели; подходит для любой другой информационной системы.	

Рассмотрев обе модели, можно сделать выводы, что первая модель больше направлена на внешнюю атаку, а вторая модель - больше на внутреннюю. Обе модели являются универсальными и могут быть использованы в любых информационных системах. При всём при этом у них есть общий существенный недостаток – они не учитывают психологические свойства пользователя, а точнее человеческий фактор, который сильно влияет на результат. В случае с первой моделью учёт человеческого фактора сильно бы повлиял на функцию уязвимостей пользователя, что позволило бы значительно снизить успех атаки, так же как и учёт человеческого фактора, относительно злоумышленника, что так же влияло бы на успех атаки. Касаемо второй же модели, если бы был учёт человеческого фактора, то можно было бы значительно снизить затраты на стимулирование и избежать лишних штрафов, что повлияло бы на конечную прибыль информационной системы.

Оценка такого параметра как человеческий фактор представлена в следующей главе.

2 Разработка математической модели безопасности информационных систем с учётом человеческого фактора

2.1 Человеческий фактор как основной источник угроз безопасности КИС

Интегральная оценка модели системы информационной безопасности может быть получена путем сравнения результатов моделирования и экспериментальных данных для конкретных объектов. Дифференциация пользователей информационной системы по психологически свойствам позволяет, оценив уровень профессионализма, интегрировать пользователя в модель системы информационной безопасности. Для оценки значимости совпадения или несовпадения модельных и экспериментальных результатов широко используются методы математической статистики применяемые в дифференциальной психологии.

2.2 Основы дифференциальной психологии

По работам Бодрова В.А. одним из критериев характеризующих деятельность человека является профпригодность. Однако, свойство человека и порождается этой деятельностью. Именно поэтому изучение профпригодности должно основываться на определении, исследовании тех психологических факторов, которые побуждают и регулируют трудовую активность личности. Психологические особенности профессиональной деятельности обуславливаются совокупностью регулирующих воздействий, а не воздействием отдельных психических функций и качеств. Совокупность регулирующих воздействий определяет характерные черты функциональной взаимосвязи, достижения определенной цели, взаимодействия этих качеств в контексте конкретной деятельности, и что главное, обеспечения уровня профпригодности.

В данной работе рассматривается психологическая система деятельности, которая представляет собой совокупность психических свойств, качеств субъекта в своей целостности, единстве, организованная для выполнения функций конкретной деятельности. Недостаточная сформированность отдельных элементов психологической системы деятельности, их неадекватность особенностям и требованиям конкретной профессиональной деятельности могут явиться причиной нарушений механизмов регуляции деятельности, необходимого уровня реализации способностей и профессионально ориентированных качеств личности, недостаточной устойчивости организма и психики к воздействию факторов деятельности и, в конечном итоге, снижения уровня профессиональной пригодности.

Характер профессиональной деятельности, ее конечные и промежуточные результаты, критерии этих результатов, в оперативном плане влияющие на эффективность и качество конкретной деятельности, а в долговременном, пролонгированном плане – уровень профпригодности

субъекта деятельности, в значительной мере определяются особенностями профессиональных мотивов человека, той побудительной силой, которая направляет его на достижение определенной цели. Интенсивность и направленность побудительных сил, их устойчивость и изменчивость, содержание мотивов отражают индивидуальные и общественные потребности человека, в том числе и в конкретной деятельности. Как правило, регуляция деятельности обуславливается воздействием совокупности мотивов. На каждом этапе профессионализации, в конкретных условиях деятельности доминирует та или иная система мотивов.

Основная функция мотивов – это мобилизация способностей, функциональных возможностей, профессионального опыта человека на достижение поставленных целей, результатов деятельности. Эти функции реализуются в том случае, когда устанавливается прямая, непосредственная или этапная связь желаемых, ожидаемых целей-результатов с функциональными и профессиональными возможностями человека, с необходимыми приемами, способами реализации и развития этих возможностей. [7]

Таким образом, мы получаем, что от мотивов пользователя будет зависеть его профпригодность, а, следовательно, вероятность негативных воздействий на информационную систему. Для определения мотивов следует обратиться к типологии Юнга, в основе которой лежит утверждение к какому психологическому типу относится субъект тем и будет определен уровень его мотивации.

2.3 Типология Юнга

Типология - система анализа личности, разработанная швейцарским психиатром К. Г. Юнгом в его работе «Психологические типы», опубликованной в 1921 году. Система Юнга основана на понятии психологической установки, которая может быть экстравертной либо

интровертной и на преобладании той или иной психической функции, к которым он относил мышление, чувство, ощущение и интуицию. [8]

Психологический тип – это структура, каркас личности. Множество разных людей одного и того же типа, имея большое сходство во внешности, манерах, особенностях речи и поведения, не будут похожи друг на друга абсолютно во всем. Каждый человек имеет свой интеллектуальный и культурный уровень, свои представления о добре и зле, свой жизненный опыт, собственные мысли, чувства, привычки, вкус. Знание своего типа личности при этом помогает людям найти именно свои средства к достижению целей, быть успешными в жизни, выбирая наиболее приемлемые виды деятельности и достигая в них наилучших результатов.

Юнг установил две жизненные установки: экстраверсия и интроверсия.

Экстраверт (E) - подвижен, разговорчив, быстро устанавливает отношения и привязанности, внешние факторы являются для него движущий силой.

Интроверт (I) - погружен во внутренний мир своих мыслей чувств и опыта. Он созерцателен, сдержан, стремится к уединению, склонен удалятся от объектов, его интерес сосредоточен на себе самом.

Вскоре после того, как Юнг сформулировал концепцию экстраверсии и интроверсии, он пришел к выводу, что с помощью этой противоположных ориентаций невозможно достаточно полно объяснить все различия в отношении людей к миру. Поэтому он расширил свою типологию, включив в неё психологические функции. Четыре основные функции, выделенные им, — это мышление, ощущение, чувство и интуиция.

Рациональные функции (J) (мышление и чувство) - они позволяют образовывать суждения о жизненном опыте

Иррациональные функции (P) (ощущения и интуиция) - они просто пассивно “схватывают”, регистрируют события во внешнем или во внутреннем мире, не оценивая их инее объясняя их значение.

Юнг выделяет основные психологические функции: мышление (T), чувство (F), ощущение (S) и интуиция (N). Все 4 присутствуют в каждом человеке, но одна из них является доминирующей.

Мышление (T) - характерно построение рациональных суждений, цель которых - определить, является оцениваемый опыт истинным или ложным.

Чувство (F) - Психологическая функция определяет является ли опыт приятным/неприятным для человека. Такие люди основываются на оценочных суждениях, вместо жестких логических убеждений.

Ощущение (S) - Для человека свойственно непосредственное, безоценочное реалистичное восприятие окружающего мира.

Интуиция (N) – Для человека свойственно сублимированное и неосознанное восприятие текущего опыта. Получается, он руководствуется предчувствиями и догадками.

2.4 Психологические свойства пользователя, компетентность

Психологический тип формирует компетентность человека Km = (S,D), где S = (Q,P), описывает его мотивацию и то, что им движет. От этого параметра зависит его профпригодность и определяется, на сколько данный субъект подходит на назначенную ему должность. Соответственно, чем выше данный показатель, тем больше пользователь подходит на должность по своей психологической предрасположенности P и образовательной характеристики Q. [9]

Применяя знания, полученные из курса акмеологии мы разбиваем всех людей на 4 психологических типа (их психологические предрасположенности): p_1,p_2,p_3,p_4 (Для выявления психологического типа пользователя с целью расчета уровня Km пользуемся программой тестирования. www.akmekras.ru и www.akmetest.ru). Так же как и виды деятельности: d_1,d_2,d_3,d_4. Где: d_1 – коммуникативный вид деятельности; d_2 – командный вид деятельности; d_3 – регламентный вид деятельности; d_4 – творческий вид деятельности, а p_1 – предрасположенность к

коммуникативному виду деятельности; p_2 – предрасположенность к командному виду деятельности; p_3 – предрасположенность к регламентному виду деятельности; p_4 – предрасположенность к творческому виду деятельности. Так же стоит описать образовательную характеристику, она бывает 4х видов: q_1,q_2,q_3,q_4. Где: q1 – Образование и опыт в профессиональном виде деятельности; q2 – Образование в профессиональном виде деятельности; q3 – Опыт в профессиональном виде деятельности; q4 – Отсутствие образования и опыта в профессиональном виде деятельности. [10]

Для расчёта компетентности используется метод с использованием функции полезности, который представляется следующим образом:

Под функцией полезности будем понимать функцию, с помощью которой можно представить предпочтения на некотором множестве альтернатив.

Критериями в расчёте будут выступать уровень образования и опыта (критерий №1), а также предрасположенность к деятельности на основе особенностей психотипа (критерий №2).

Для расчёта будет использоваться линейная функция полезности. Вид функции зависит от того, будет ли критерий подлежать максимизации, или же минимизации.

Вид, для критериев подлежащих максимизации:

$$P_{ij} = \begin{cases} 1, & X_{ij} > X_i^{max} \\ \dfrac{X_{ij} - X_i^{min}}{X_i^{max} - X_i^{min}}, & X_i^{min} \le X_{ij} \le X_i^{max} \\ \dfrac{X_{ij} - X_i^{min}}{X_i^{max} - X_i^{min}} \cdot S, & X_{ij} < X_i^{min} \end{cases}$$

Вид, для критериев подлежащих минимизации:

$$P_{ij} = \begin{cases} 1, & X_{ij} < X_i^{min} \\ 1 - \dfrac{X_{ij} - X_i^{min}}{X_i^{max} - X_i^{min}}, & X_i^{min} \le X_{ij} \le X_i^{max} \\ \left(1 - \dfrac{X_{ij} - X_i^{min}}{X_i^{max} - X_i^{min}}\right) \cdot S, & X_{ij} > X_i^{max} \end{cases}$$

Xij – оценка j-го объекта по i-му критерию; $Ximin$,$Ximax$ наиболее нежелательное и желательное значение -го критерия (эти величины, как правило, указываются экспертом и представляют собой субъективные суждения);

S – штрафной коэффициент, используемый для вычисления мер полезности альтернатив, у которых оценки хуже, чем наименее желательное значение по данному критерию (обычно используются значения S от 5 до 10);

Pij – мера полезности j-й альтернативы по i-му критерию. [11], [12]

$\tilde{W}p$ и $\tilde{W}q$ – веса критериев для {P} и {Q} соответственно, показывающие какое влияние {P} и {Q} вносят в значение компетентности, $\tilde{W}p + \tilde{W}q = 1$. $Xi\ d$ - непосредственная оценка для pi ∈ {P}, i = $\overline{1,4}$ относительно d ∈ {D} $Xmin\ d$ - минимальное значение непосредственной оценки для p ∈ {P} относительно d ∈ {D} $Xmax\ d$ - максимальное значение непосредственной оценки для p ∈ {P} относительно d ∈ {D} $Yj\ d$ - непосредственная оценка для qj ∈ {Q}, j = $\overline{1,4}$ относительно d ∈ {D} $Ymin\ d$ - минимальное значение непосредственной оценки для q ∈ {Q} относительно d ∈ {D} $Ymax\ d$ - максимальное значение непосредственной оценки для q ∈ {Q} относительно d ∈ {D

$$\tilde{W}_q = \frac{1}{2}\left(W_q + \frac{\widetilde{Rnd}_q}{\widetilde{Rnd}_p + \widetilde{Rnd}_q}\right)$$

Где Wp и Wq – экспертные веса критериев для {P} и {Q} соответственно, показывающие какое влияние {P} и {Q} вносят в значение компетентности, $Wp + Wq = 1$. $\widetilde{Rnd}\ p$и $\widetilde{Rnd}\ q$ – средний разброс значений для {P} и {Q} соответственно, показывающих соответствие непосредственных оценок $Xi\ d$ и $Yj\ d$ одному из субъектов s ∈ {S}.

$$\widetilde{Rnd}_p = \frac{\sum_{i=1}^{16} \left| Z_i - \frac{1}{16} \sum_{i=1}^{16} Z_i \right|}{\sum_{i=1}^{16} Z_i}$$

$$\widetilde{Rnd}_q = \frac{\sum_{j=1}^{16} \left| T_j - \frac{1}{16} \sum_{j=1}^{16} T_j \right|}{\sum_{j=1}^{16} T_j}$$

Z - значения для {P}, показывающие соответствие непосредственной оценки $Xi\ d$ одному из субъектов s ∈ {S}. T - значения для {Q}, показывающие соответствие непосредственной оценки $Yj\ d$ одному из субъектов s ∈ {S}.

В соответствии с методом функций полезности компетентность Km[s, d] субъекта s ∈ {S} относительно вида деятельности d ∈ {D} может быть найдена как:

$$Km[s,d] = \widetilde{W}_p \cdot \frac{X_i^d - X_{min}^d}{X_{max}^d - X_{min}^d} + \widetilde{W}_q \cdot \frac{Y_j^d - Y_{min}^d}{Y_{max}^d - Y_{min}^d}$$

2.5 Математическая модель обеспечения безопасности информационных систем с учётом человеческого фактора

Исходя из анализа вышеописанных моделей, а так же ссылаясь на работы [7],[8] и вводя такой параметр как компетенция (для учёта того самого человеческого фактора) можно составить новую математическую модель обеспечения безопасности информационной системы с учетом человеческого фактора. Исходя из анализа моделей, наиболее подходящей моделью является модель предложенная М.В. Абрамовым «Анализ защищенности персонала ИС от социоинженерных атак [3]. Предложенную модель можно улучшить, рассмотрев мотивацию и профпригодность пользователя, а так же мотивацию злоумышленника. Для этого следует учесть компетентность пользователя и злоумышленника и ввести их в модель.

Так как злоумышленник негативно воздействует на ресурсы через пользователя, исходя из уязвимостей пользователя, то шанс на успешную атаку можно уменьшить, если переписать модель с учётом человеческого фактора. Введём вышеописанный параметр – компетентность Km (расчёт которой описан ниже). Логично предположить, что чем компетентнее злоумышленник и чем менее компетентен пользователь, тем выше шанс на успешную атаку. Перепишем модель с учётом компетентностей для злоумышленника и пользователя.

Злоумышленник M может быть представлен в виде $M=\{R, S_0, Km_z\}$, где:

R – ресурсы, к которым есть доступ у злоумышленника, а так же его личностные особенности;

S_0 – пользователи S, к которым злоумышленник имеет доступ до момента негативного воздействия (атаки);

Объединим КПЗ и U_0 злоумышленника в его компетентность Km_z от величины которой зависит успех атаки.

Km_z – компетентность злоумышленника, всегда будем принимать её за единицу.

Пользователь S может быть представлен в виде $S= \{C, Z, Km_p, L\}$, где

C – критические ресурсы, к которым имеется доступ у пользователя;

Z – контролируемые пользователем зоны;

Km_p – компетентность пользователя, влияющая на уязвимости;

L – матрица взаимоотношений пользователей.

Будем рассматривать шансы на успех, исходя из того, кто является более компетентным, злоумышленник или пользователь. Введём функцию уязвимости пользователя $\psi(V_l,Km_p)$. Где: V_l – возможные уязвимости пользователя.

Тогда конечная формула подсчёта успеха атаки будет выглядеть следующим образом: $p^{lq}_{ij} = g(Km_z, \psi(V_l,Km_p), B_i)$

3. Статистический анализ эффективности разработанной модели в сравнении с рассмотренными моделями

3.1 Метод исследования

В данной работе, для анализа эффективности разработанной модели был использован регрессионный анализ, так как нам требуется определить форму зависимости успеха атаки (результативный признак) от изменения компетентности (факторный признак). А так же был проведён сравнительный анализ результатов изначальной модели (без учёта человеческого фактора) и разработанной.

3.2 Анализ разработанной модели безопасности с учётом человеческого фактора

Проведя анализ пользователей с выявлением их психологических особенностей, полученных с помощью тестирующей программы представленной на *www.akmekras.ru и www.akmetest.ru* и, рассчитав их компетентности Km, данные были занесены в таблицу 4 для последующего регрессионного анализа.

Таблица 4 - Исходные данные разработанной модели безопасности

Пользователи	Вероятность успеха атаки, y	Компетентность пользователя, x
S_1	0,6	0,42
S_2	0,74	0,21
S_3	0,28	0,83
S_4	0,05	0,86
S_5	0,69	0,43
S_6	0,83	0,15
S_7	0,47	0,67
S_8	0,58	0,53
S_9	0,11	0,82
S_{10}	0,82	0,17

Регрессионный анализ проводился с использованием следующих формул:

Для расчета параметров a и b линейной регрессии y = a + b*x решается следующая система нормальных уравнений

относительно a и b: $\begin{cases} na + b * \sum x = \sum y \\ a * \sum x + b * \sum x^2 = \sum y * x \end{cases}$

Проведём расчёт, записав промежуточные данные в таблицу:

Таблица 5 – Промежуточные данные разработанной модели безопасности

x	y	x^2	y^2	x*y
0,4	0,42	0,36	0,1764	0,252
0,26	0,21	0,5476	0,0441	0,1554
0,72	0,83	0,0784	0,6889	0,2324
0,95	0,86	0,0025	0,7396	0,043
0,31	0,43	0,4761	0,1849	0,2967
0,17	0,15	0,6889	0,0225	0,1245
0,53	0,67	0,2209	0,4489	0,3149
0,42	0,53	0,3364	0,2809	0,3074
0,89	0,82	0,0121	0,6724	0,0902
0,18	0,17	0,6724	0,0289	0,1394

Для наших данных система уравнений имеет вид 10a + 5,17*b = 5,09 5,17*a + 3,395*b = 1,956

Получаем эмпирические коэффициенты регрессии, что a = 0,9925, b = -0,9352, тогда уравнение регрессии имеет вид y = -0,9352*x + 0,9925

В нашем примере мы получили результаты, что в среднем при увеличении параметра x на 1 ед, приводит к увеличению y на - 0,935 ед. Это говорит о том, что связь обратная и успех обратно зависит от уровня компетентности, чем выше компетентность, тем ниже успех атаки.

3.3 Анализ модели анализа защищенности персонала информационной системы от социоинженерных атак

Проведём аналогичный анализ для модели анализа защищённости персонала информационной системы от социоинженерных атак.

Проанализируем, как сильно влияет на успех атаки изначальная функция пользователя, зависящая от уязвимостей, но не учитывающая

психологические особенности пользователя. Данные для данной модели описаны в таблице 6.

Таблица 6 – Начальные данные для модели анализа защищенности персонала информационной системы

Пользователи	Вероятность успеха атаки, y	$S_q(V_l, K_i)$, x
S_1	0,45	0,6
S_2	0,69	0,4
S_3	0,31	0,4
S_4	0,04	0,24
S_5	0,12	0,18
S_6	0,08	0,2
S_7	0,95	0,67
S_8	0,74	0,68
S_9	0,66	0,53
S_{10}	0,22	0,31

Так же решим систему нормальных уравнений

$$\begin{cases} na + b * \sum x = \sum y \\ a * \sum x + b * \sum x^2 = \sum y * x \end{cases}$$

Воспользовавшись данными из предварительно заполненной таблицы 6

Таблица 6 – Промежуточные данные для для модели анализа защищенности персонала информационной системы

x	y	x^2	y^2	x*y
0,45	0,6	0,2025	0,36	0,27
0,69	0,4	0,4763	0,16	0,276
0,31	0,4	0,0961	0,16	0,124
0,04	0,24	0,0016	0,0576	0,0096
0,12	0,18	0,0144	0,0324	0,0216
0,08	0,2	0,0064	0,04	0,016
0,95	0,67	0,9025	0,4489	0,6365
0,74	0,68	0,5476	0,4624	0,5032
0,66	0,53	0,4356	0,2809	0,3498
0,22	0,31	0,0484	0,0961	0,0682

Для наших данных система уравнений имеет вид

10a+4.26*b=4.21

4.26*a + 2.731*b = 2.275

Получаем эмпирические коэффициенты регрессии, что a = 0,1972, b = 0,5253, тогда уравнение регрессии имеет вид y = 0,5253*x + 0,1972

В нашем примере мы получили результаты, что в среднем при увеличении параметра x на 1 ед, приводит к увеличению y на 0,525 ед. Это говорит о том, что связь прямая и успех напрямую зависит от $S_q(V_l, K_i)$, чем выше больше уязвимостей у пользователя, тем выше успех атаки.

3.4 Сравнение результатов и выводы

Для более наглядного сравнения результатов переведём обратную связь зависимости успеха атаки от компетентности, в прямую. Для этого представим параметр x как Km – 1, перезаполним таблицу, проведём расчёты и по полученным расчётам построим график зависимости успеха от компетентности. Для второй модели, аналогично, построим график зависимости успеха от функции уязвимости пользователя. Результаты графиков приведены ниже на рисунках 3,4.

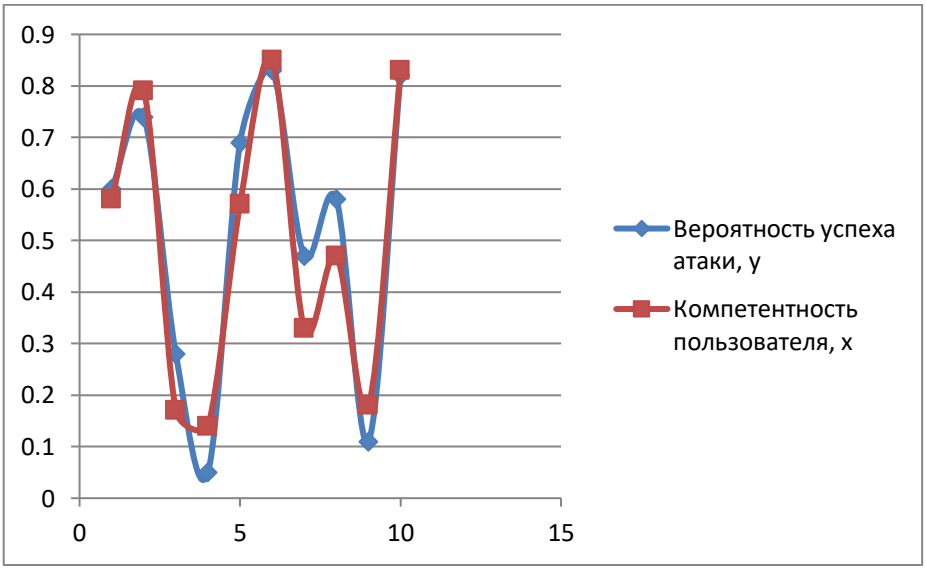

Рисунок 3 – График зависимости вероятности успеха атаки от компетенции пользователя

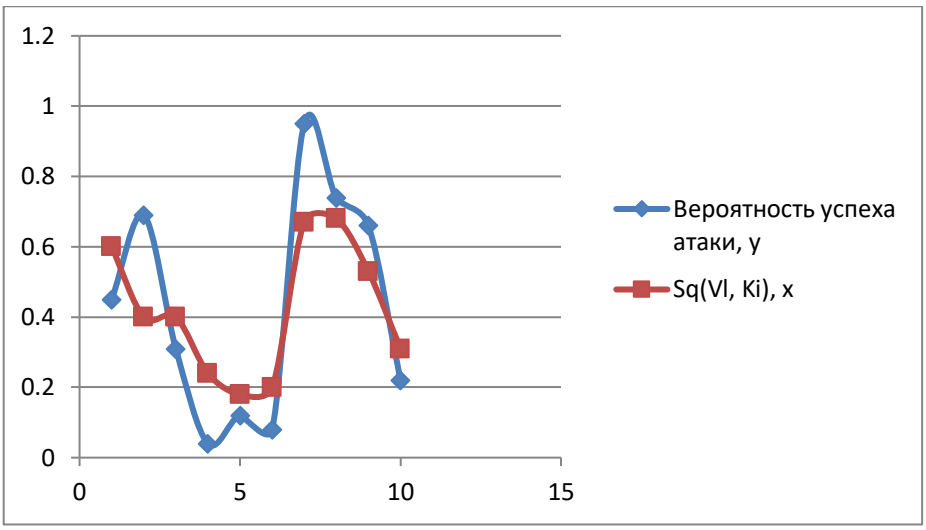

Рисунок 4 – График зависимости вероятности успеха атаки от функции уязвимости

Проведя регрессионный анализ для изначальной модели и усовершенствованной введением в неё уровня компетентности, и сравнением графиков зависимостей, можно заметить, что в случае без учёта человеческого фактора функция без учёта компетентности даёт менее точную оценку, нежели модель с учётом человеческого фактора. В первом случае 1 ед для успеха атаки меняется при изменении функции уязвимости на 0.525 ед, в то время как 1 ед для успеха атаки изменяется при изменении функции компетентности на 0.953, что указывает на более сильную зависимость, а следовательно более точную оценку. Исходя из этого, стоит сделать вывод, что человеческий фактор это именно та компонента, которой не хватало в вышеописанных моделях и это именно то, чего не хватает при составлении моделей безопасности сейчас.

ЗАКЛЮЧЕНИЕ

В данной работе была изучены две модели безопасности информационной системы. Был проведён их анализ, на основе которого было сделано утверждение, что у каждой модели имеется один и тот же недостаток – они не учитывают человеческий фактор. На основе этого суждения и основ дифференциальной психологии был введён показатель компетентности пользователя, зависящий от его психологических особенностей, и разработана модель безопасности, учитывающая этот показатель. Был проведён статистический регрессионный анализ двух моделей – взятой за основу модели В.А.Абрамова и нашей, усовершенствованной, в которой учитывается компетентность. Анализ выявил, что у модели учитывающей человеческий фактор выше точность и от увеличения показателя компетентности значительно уменьшается успех социоинженерной атаки. Из всего этого можно сделать выводы, что если учитывать человеческий фактор в современных моделях безопасности информационной системы, то точно такой модели будет значительно выше, чем точности существующих моделей без учёта человеческого фактора.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Васильев К.К., Служивый М.Н. Математическое моделирование систем связи: учебное пособие, 2008, С.2-10.
2. Замятина О.М. Моделирование систем: учебное пособие, 2009, С 1-20.
3. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Информационно-управляющие системы, 2016, №. 4 (83), С.77–84.
4. Тулупьев А.Л., Азаров А.А., Пащенко А.Е. Информационная модель пользователя, находящегося под угрозой социоинженерной атаки, Тр. СПИИРАН. 2010. Вып. 2 (13), С.143–155.
5. Тулупьева Т.В., Тулупьев А.Л., Азаров А.А., Пащенко А.Е. Психологическая защита как фактор уязвимости пользователя в контексте социоинженерных атак, Тр. СПИИРАН. 2011. Вып. 18, С.74–92.
6. Новиков Д.А., Петраков С.Н. Курс теории активных систем, 1999, С.28-44.
7. Бодров В.А. Психология профессиональной пригодности, 2001, С. 4-27.
8. Юнг К.Г. Психологические типы, 1929, С.101-157.
9. Краснов И.З. Акмеологическая оценка профессиональной компетентности,2009.
10. Краснов И.З., Цыганков Н.С. Алгоритм расчёта уровня компетентности относительно требуемой деятельности человека, Научно-технический вестник Поволжья, №2, 2016 г, С.127-132.
11. Краснов И.З., Шапочкин С.О. Модель управления эффективностью деятельности организации с учетом человеческого фактора, Научно-технический вестник Поволжья, №6, 2016 г, С.152-155.
12. Ченцов С.В., Краснов И.З., Сидарас А.А. Обеспечение устойчивости информационных систем с учетом человеческого фактора. "Фундаментальные исследования" № 11 (часть 1), 2017, С.140-144.
13. Демидов Н.Е. Аналитические иерархические процессы экспертного оценивания на платформе MATLAB, 2004.

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт Космических и Информационных Технологий
Кафедра прикладной математики и компьютерной безопасности

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А. А. Кытманов
подпись
«18» 06 2018 г.

БАКАЛАВРСКАЯ РАБОТА

01.03.04 Прикладная математика

Математические модели обеспечения безопасности информационных систем с учетом человеческого фактора

Руководитель _____ доцент. И.З.Краснов
подпись, дата

Выпускник _____ А. А.Истягин
подпись, дата

Красноярск 2018