Вестник УГАТУ
Уфа : УГАТУ, 2012 Т. 16, № 3 (48). С. 187–193

УДК 004.056

Т. И. Фазлиахметов, А. И. Фрид

МОДЕЛЬ АНАЛИЗА РИСКОВ НЕСАНКЦИОНИРОВАННОЙ МОДИФИКАЦИИ МЕТРОЛОГИЧЕСКИХ ДАННЫХ В ПРОИЗВОДСТВЕННЫХ СИСТЕМАХ

В статье рассмотрена проблема обеспечения целостности метрологических данных в информационных производственных системах, а также проблема оценки рисков в таких системах. Предлагается решение проблемы повышения уровня защищенности данных, основанное на математических взаимосвязях параметров функционирования технологических объектов. Предлагается модель для оценки рисков несанкционированной модификации метрологических данных, которая используется для определения целесообразности использования предлагаемого решения. На основе данной модели и методики ГРИФ показан пример расчета риска несанкционированной модификации метрологических данных и эффект от использования предлагаемого решения. *Целостность данных*; *защита метрологических данных*; *угроза*; *вероятность реализации угрозы*; *стоимость метрологической информации*; *риск*

ВВЕДЕНИЕ

В 2010 году произошел инцидент, – была атакована промышленная система SCADA [1]. Такие системы контролируют процессы во многих отраслях производства, таких как нефте- и газодобыча, нефтепереработка, атомная энергетика и т.д. Естественно, такие комплексы имеют свои базы данных, и та информация, которая хранится в них, бывает бесценна. Более того, несанкционированное вмешательство в производственные и технологические процессы может приводить не только к экономическим потерям, снижению эффективности управления, но и, в самом худшем случае, к техногенным катастрофам. Поэтому необходима повышенная информационная безопасность (ИБ) производственных систем. Особенно пристальное внимание следует уделять защите метрологических данных от несанкционированной модификации (НСМ) их полного удаления, так как именно на их основе принимаются те или иные решения по управлению производственными процессами. И последствия этих решений могут быть катастрофическими.

Важно отметить, что данное требование относится не только к SCADA системам, но и к любым производственным системам, которые обрабатывают метрологические данные.

Таким образом, целью исследования, приведенного в работе, является повышение уровня защищенности метрологических данных. Следует отметить, что в работе рассматривается задача защиты метрологических данных только от несанкционированного изменения (обеспечение целостности информации). Для достижения поставленной цели необходимо решить следующие задачи:

- предложить метод для повышения уровня защищенности метрологических данных;
- разработать модель для оценки эффективности предлагаемого метода;
- оценить эффективность предлагаемого метода.

В настоящее время существует множество технических средств и механизмов, обеспечивающих информационную безопасность на различных уровнях защиты [2]. Однако существующие механизмы обладают рядом недостатков и могут в определенных случаях не обеспечить необходимую защиту данных. Недостатками приведенных выше средств и механизмов являются:

- анализируют лишь свойства информационных потоков и вычислительных процессов, не уделяя внимание самим данным и их «смыслу»;
- не обеспечивают защиту данных в случае, когда пользователь легально имеет к ней доступ, но действует злонамеренно или непреднамеренно искажает данные;
- не обеспечивают защиту данных в случае, когда злоумышленник получает полный доступ (проходит все уровни защиты);
- средства являются общими для информационных систем, то есть не учитывают специфику данных и область, в которой функционирует информационная система.

В связи с недостатками существующих подходов возникают следующие вопросы: как за-

Контактная информация: 8(347)273-06-72

щитить информацию, если пользователь имеет доступ к изменению данных, как защитить информацию, если злоумышленник получил доступ к изменению данных?

КОНЦЕПЦИЯ МЕТОДА

Концепция предлагаемого решения состоит в том, чтобы использовать смысловую нагрузку информации – контекст информационных потоков [3], то есть рассматривать данные не просто как поток информации, а учитывать специфику области, в которых они используются.

Применительно к информационной безопасности в производственных системах нефтегазового комплекса идея повышения уровня защищенности данных состоит в том, чтобы использовать тот факт, что метрологические данные функционально и статистически связаны между собой. Например, расход жидкости зависит от давления в трубопроводе, вязкости, температуры и других параметров. Чем больше давление в трубе, тем больше расход жидкости. Решение задачи защиты данных в этом случае может состоять в том, чтобы по другим параметрам потока, таким как давление, содержание влаги и т. д., рассчитать значение расхода и сравнить его с тем значением, которое пытаются записать на место текущего. Если рассчитанное и новое значения расходов равны или близки по значению, то принимается решение, что попыток несанкционированной модификации нет. Если эти расходы не равны, то принимается решение, что идет попытка несанкционированной модификации данных, и попытка блокируется.

РАЗРАБОТКА МОДЕЛИ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ МЕТРОЛОГИЧЕСКИХ ДАННЫХ

Для предлагаемого решения можно выделить два варианта его использования:

- как дополнительная контрмера для всех существующих средств и механизмов защиты информации на различных уровнях;
- как альтернативный вариант некоторых контрмер на том же уровне защиты, то есть как замена некоторых существующих контрмер.

Для целесообразности использования предлагаемого метода по первому варианту необходимо выполнение следующих условий:

$$Q_{\text{tool}} \le R, \quad (1)$$

$$Q_{\text{threat}} \le I, \quad (2)$$

$$Q_{\text{tool}} + Q_{\text{sol}} \le R, \quad (3)$$

где Q_{tool} – затраты на использование средств защиты информации (СЗИ); R – риск НСМ информационных ресурсов; Q_{threat} – затраты на реализацию угрозы; I – стоимость информации; Q_{sol} – затраты на реализацию предлагаемого решения.

Для целесообразности использования предлагаемого метода по второму варианту к условиям (1)–(3) добавляется условие того, что затраты на предлагаемое решение должны быть минимальными из всех затрат на реализацию альтернативных контрмер:

$$Q_{\text{sol}} = \min(Q_{\text{tool}(i)}). \quad (4)$$

Таким образом, для оценки эффективности предлагаемого метода и определения целесообразности его использования необходимо решить следующие задачи:

- анализ рисков информационной безопасности производственных систем (определение R, I, Q_{threat});
- анализ затрат при использовании существующих механизмов защиты данных (определение Q_{tool});
- анализ затрат при реализации предлагаемого метода в оперативных производственных системах (определение Q_{threat}).

В [4] дается общая модель информационной безопасности и взаимосвязь между основными понятиями безопасности. Однако данная модель не дает представление о количественной взаимосвязи характеристик ИБ, приведенных выше, а показывает лишь их функциональную взаимосвязь. Кроме того, она не учитывает характер активов, на которые направлена защита. На основе этой модели предлагается модель для оценки эффективности обеспечения целостности метрологических данных в производственных системах, представленная на рис. 1.

На данной модели активами, на которые направлены угрозы, являются метрологические данные, входящие в состав информационной системы. Эти данные представляют собой значения различных параметров, описывающих функционирование какого-либо производственного объекта. Активы имеют две характеристики, влияющие на уровень риска R (f_5, f_6): K – коэффициент разрушительности; I – стоимость информации (в этом случае стоимость метрологических данных).

Информационная система имеет уязвимости, на которые направлены угрозы. Каждая угроза характеризуется тремя параметрами: P – вероятность реализации угрозы; F – частота угрозы за год; Q_{threat} – затраты на реализацию угрозы.

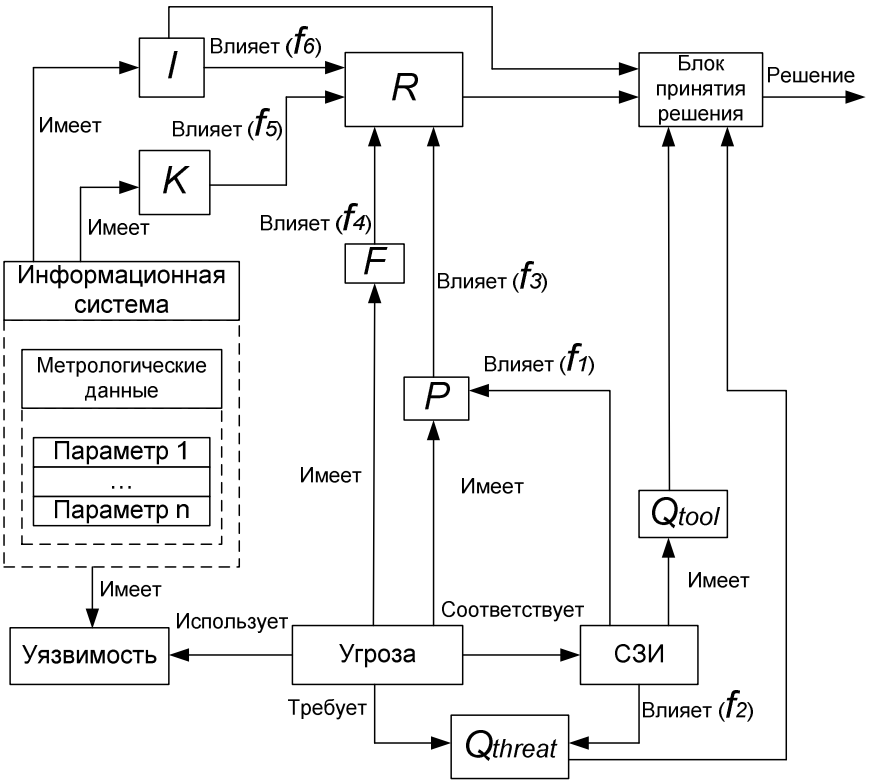

Рис. 1. Модель для анализа рисков несанкционированной модификации метрологических данных

P и F влияют на R (f_4, f_5). Каждой угрозе соответствуют свои СЗИ, которые влияют на P и Q_{threat} (f_1, f_2) [2]. Сами СЗИ характеризуются затратами на их реализацию – Q_{tool}.

Таким образом, для оценки эффективности предлагаемого решения необходимо определить перечисленные выше характеристики компонентов модели, а также их взаимосвязи ($f_1 - f_6$).

Для определения зависимостей $f_3 - f_6$ используется формула, приведенная в [2]:

$$R = I \cdot K \cdot P \cdot F. \qquad (5)$$

Зависимость f_1 определяется:

- экспертным путем;
- статистически;
- путем тестирования СЗИ;
- специфическими методами.

Зависимость f_2 определяется стоимостью СЗИ.

Стоимость информации I представляет собой стоимость изменения значения какого-либо параметра. Для расчета I необходимо ввести следующие характеристики параметра:

VP – текущее значение параметра;

VP_{new} – новое значение параметра – то значение, на которое делается попытка изменить VP;

S – стоимость единицы измерения параметра;

C – количество коммерческих производственных объектов.

Тогда I одного параметра можно определить по формуле:

$$I = (VP - VP_{\text{new}}) \cdot S \cdot C. \qquad (6)$$

ПРИМЕР РАСЧЕТА РИСКОВ НСМ МЕТРОЛОГИЧЕСКИХ ДАННЫХ

Анализ угроз и уязвимостей

Чтобы оценить эффективность предлагаемого решения, приведем пример расчета рисков информационной безопасности до и после его использования. Следует отметить, что здесь не рассматриваются вопросы, связанные с использованием показателей Q_{tool} и Q_{threat}, а производится лишь демонстрация расчета рисков. Расчет рисков производится на основе методики ГРИФ «Алгоритм: модель анализа угроз и уязвимостей» [5].

Пусть имеется информационная система, состоящая из рабочих станций с установленным прикладным программным обеспечением для работы с метрологической информацией.

Метрологические данные хранятся на сервере БД, которая находится под управлением СУБД Oracle 10. Для каждого конкретного числа, значения какого-либо параметра, по алгоритму MD5 рассчитывается хеш-функция, кото-

рая проверяется при использовании этого числа в приложении.

В качестве операционных систем используется Windows XP (на рабочих станциях) и Windows Server (на сервере БД) 2008. В качестве СЗИ, в частности, можно использовать продукцию под маркой McAfee: McAfee VirusScan Enterprise версии 8.7.0i (включая McAfee Anti-Spyware).

Вход в приложение осуществляется по логину и паролю, т. е. имеет авторизацию. В самом приложении не имеется возможность редактирования данных, непосредственно пришедших с автоматизированных систем измерения, т. е. метрологические данные остаются в БД в неизменном виде. Однако логин и пароль, использующиеся для авторизации в приложении, также могут быть использоваться для авторизации непосредственно в СУБД (например, при использовании утилит для работы с БД). Разграничение доступа к данным реализовано средствами самой БД.

В системе зарегистрировано несколько пользователей, каждый из которых потенциально может быть злоумышленником. Для простоты расчетов всех пользователей можно выделить в группы в зависимости от доступа к метрологическим данным и служебной информации (метаданные). Выделенные группы показаны в табл. 1.

Таблица 1

Группы пользователей

Группа пользователей	Доступ к метрологическим данным	Доступ к метаданным
Администратор	Полный	Полный
Специалист цеха	Полный	Чтение
Начальник отдела	Чтение	Чтение

Исходя из описания системы и моделей злоумышленника, можно сформировать список угроз и уязвимостей для каждой из моделей злоумышленника. Списки угроз представлены в табл. 2–4.

Вероятности реализации угроз определены по результатам тестов, приведенных в [6], [7] и [8]. McAfee Anti-Spyware смог определить 11,11 % шпионских программ, а McAfee VirusScan Enterprise смог определить 90,59 % вредоносного ПО. Вероятность последней угрозы группы «Администратор» выбрана исходя из доли злоумышленников среди всех администраторов системы. Предполагается, что их количество относительно мало.

Таблица 2

Анализ угроз для группы пользователей «Администратор»

Угроза	Уязвимость	*P*
Преодоление контроля целостности данных по хеш-функции	Недостатки алгоритма расчета хеш-функции	0,754
НСМ МД в памяти компьютеров до сохранения их в БД	Устаревшие базы антивирусной защиты	0, 094
Изменение метаданных или настроек работы приложения	Полный доступ к метаданным и настройкам работы ПО	0,001

Таблица 3

Анализ угроз для группы пользователей «Специалист цеха»

Угроза	Уязвимость	*P*
Преодоление контроля целостности данных по хеш-функции	Недостатки алгоритма расчета хеш-функции	0,754
НСМ МД в памяти компьютеров до сохранения их в БД	Устаревшие базы антивирусной защиты	0, 094

Таблица 4

Анализ угроз для группы пользователей «Начальник отдела»

Угроза	Уязвимость	*P*
Перехват логина и пароля пользователя, имеющего право на редактирование метрологических данных	Уязвимости в операционной системе	0,889
Преодоление контроля целостности данных по хеш-функции	Недостатки алгоритма расчета хеш-функции	0,754
НСМ МД в памяти компьютеров до сохранения их в БД	Устаревшие базы антивирусной защиты	0, 094

Для расчета общей вероятности реализации угроз предлагается представить уязвимости и угрозы в виде графа, представленного на рис. 2.

Ресурс представляет собой ценный актив предприятия, на который направлена угроза. Барьер представляет собой СЗИ. *P* – вероятность прохождения соответствующего барьера

или вероятность использования уязвимости. Если между уязвимостью и ресурсом нет барьера и не указана вероятность, то вероятность принимается равной 1. Уязвимость, находящаяся до барьера, – это уязвимость самого СЗИ или уязвимость, с помощью которой можно преодолеть данный барьер.

Графы угроз и уязвимостей для каждой группы пользователей показаны на рис. 3–5.

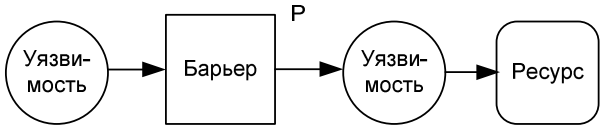

Рис. 2. Граф угроз и уязвимостей

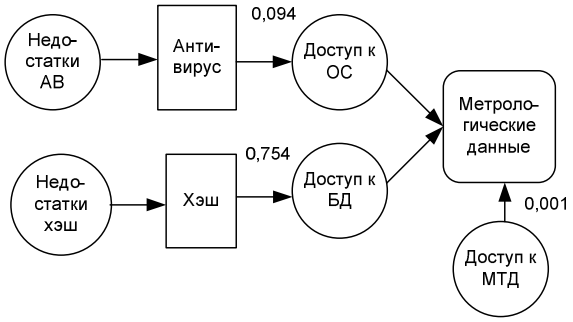

Рис. 3. Граф угроз и уязвимостей для группы «Администратор»

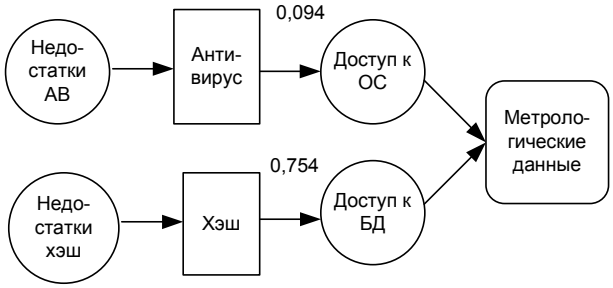

Рис. 4. Граф угроз и уязвимостей для группы «Специалист цеха»

Для расчета общей вероятности применяются следующие правила:

1. Общая вероятность параллельных угроз вычисляется по формуле, приведенной в ГРИФ:

$$P_{\text{total}} = 1 - \prod_{i=1}^{n} (1 - P_i), \qquad (7)$$

где P_i – вероятность реализации i-й угрозы;

n – количество параллельных угроз.

2. Общая вероятность последовательных угроз вычисляется по формуле:

$$P_{\text{total}} = \sum_{i=1}^{n} (1 - P_i). \qquad (8)$$

3. Общая вероятность по всем группам пользователей вычисляется аналогично п. 1.

Анализ рисков до и после введения предлагаемого метода

В качестве технологического объекта, по которому злоумышленник пытается изменить данные, возьмем один трубопровод со средним расходом нефти 500 тонн/ч. В качестве изменяемого параметра – расход нефти, так как именно он представляет материальную ценность.

Итак, злоумышленник хочет уменьшить значение расхода на 10%, то есть на 50 тонн/ч. Пусть стоимость одной тонны нефти равна 70 $. По формуле (6) рассчитаем потери компании за один час при успешной реализации данного действия:

$$I_{\text{hour}} = 50 \cdot 70 \cdot 1 = 3500 \text{ \$}. \qquad (9)$$

Далее рассчитаем годовые потери компании:

$$I = 3500 \cdot 24 \cdot 365 = 30660000 \text{ \$}. \qquad (10)$$

Результаты вычислений общих вероятностей по формулам (7) и (8) показаны в табл. 5.

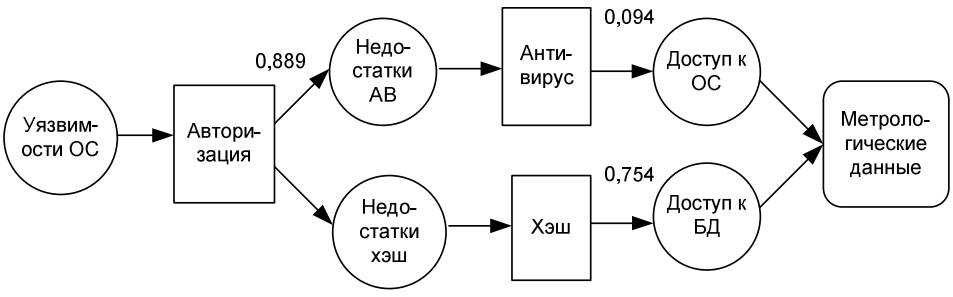

Рис.5. Граф угроз и уязвимостей для группы «Начальник отдела»

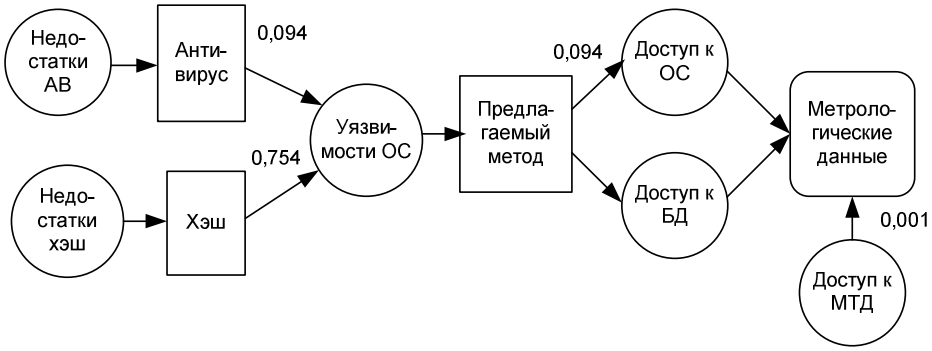

Рис.6. Граф угроз и уязвимостей для группы «Администратор»

Таблица 5

Общая вероятность до введения предлагаемого метода

Группа	Вероятность реализации угрозы по группе пользователей	Общая вероятность реализации угроз, P_{total}
Администратор	0,777	0,985
Специалист цеха	0,777	
Начальник отдела	0,691	

По формуле (5) рассчитаем риск. Коэффициенты K и F в данном случае примем равными 1, так как они учитываются при расчете общего уровня угроз в методике ГРИФ:

$$R = 30660000 \cdot 0{,}985 = 30200100 \text{ \$}. \quad (11)$$

Теперь рассчитаем риск после введения предлагаемого решения. Так как ни одно решение не может гарантировать стопроцентную защиту данных, то после введения предлагаемого решения появляется новая угроза обхода данной защиты. После введения предлагаемого механизма защиты данных для каждого злоумышленника добавляется еще одна угроза, представленная в табл. 6.

Таблица 6

Дополнительная угроза после введения предлагаемого метода

Угроза	Уязвимость	P
Преодоление механизма защиты данных, основанного на математической взаимосвязи данных	Уязвимости в операционной системе	0, 094

Граф угроз и уязвимостей для группы «Администратор» примет вид как на рис. 6. Остальные графы изменятся аналогично.

Результаты вычислений общих вероятностей после введения предлагаемого решения показаны в табл. 7.

Таблица 7

Общая вероятность после введения предлагаемого метода

Группа	Вероятность реализации угрозы по группе пользователей	Общая вероятность реализации угрозы, P_{total}
Администратор	0,073	0,204
Специалист цеха	0,073	
Начальник отдела	0,064	

Аналогично формуле (11) рассчитаем риск после введения предлагаемого метода:

$$R_{new} = 30660000 \cdot 0{,}204 = 6254640 \text{\$} \ . \quad (12)$$

ВЫВОДЫ

В работе предлагается метод защиты метрологических данных, основанный на их математической взаимосвязи. Метод отличается от существующих тем, что он учитывает «смысл» данных, а также специфику предметной области данных.

Предлагается модель для оценки риска несанкционированной модификации метрологических данных. Производится анализ риска до и после введения предлагаемого метода. Анализ показывает, что внедрение предлагаемого метода защиты метрологических данных может привести к существенному снижению риска. В данном случае применение предлагаемого решения позволила снизить уровень риска примерно в 4,8 раз.

СПИСОК ЛИТЕРАТУРЫ

1. **Синцов А.** Шпионский ярлык // Хакер. М.: ООО «Гейм Лэнд». 2010. № 9. С. 54–57.

2. **Нестеров С. А**. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft [Электронный ресурс]. http://www.intuit.ru/department/itmngt/riskanms/

3. **Websence**. Protecting Essential Information: Securing the Foundation of the Internet Business Platform. 2008 [Электронный ресурс]. http://www.websense.com/assets/white-papers/whitepaper_prot_ess_info_ 0809_uk.pdf

4. **ГОСТ Р ИСО/МЭК 15408-2002** «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий». 2002.

5. **«ООО «Диджитал Секьюрити».** Описание методики ГРИФ «Алгоритм: модель анализа угроз и уязвимостей». [Электронный ресурс]. http://www.dsec.ru/download/threats_vuln.pdf

6. **Красноступ Н. Д., Кудин Д. В.** Исследование эффективности средств защиты от шпионских программ. 2006. [Электронный ресурс]. http://www.bezpeka.com/ru/lib/sec/gen/art533.html

7. **Philippe Oechslin**. Making a faster cryptanalytic time-memory trade-off // The 23rd Annual International Cryptology Conference, CRYPTO’03: vol. 2729. 2003. P. 617–630.

8. **Интернет портал «Клуб сисадминов».** Тест антивирусов №5. 2009 г. [Электронный ресурс]. http://www.admin-club.net/index/0-19.

ОБ АВТОРАХ

Фазлиахметов Тимур Ильгизович, асп. каф. вычисл. техники и защиты информации. Дипл. магистр техники и технологии по информатике и вычисл. технике (УГАТУ, 2009). Иссл. в обл. инф. безопасности.

Фрид Аркадий Исаакович, проф. каф. вычисл. техники и защиты информации. Дипл. инженер-электромеханик (УАИ, 1968). Д-р техн. наук по управлению в техн. системах (УГАТУ 2000). Иссл. в обл. управления сложн. системами в условиях неопределенности.