ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Сентябрь 2017 Том 5 № 3 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
September 2017 Vol. 5 Iss. 3 ISSN 2307-1303 http://www.itt.sut.ru

МОДЕЛЬ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ УПРАВЛЕНИЯ ВОДОСНАБЖЕНИЕМ ДЛЯ АНАЛИЗА ИНЦИДЕНТОВ БЕЗОПАСНОСТИ

В. А. Десницкий[1,2,3*]

[1] СПИИРАН, Санкт-Петербург, 199178, Российская Федерация
[2] СПбГУТ, Санкт-Петербург, 193232, Российская Федерация
[3] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
* Адрес для переписки: desnitsky@comsec.spb.ru

Аннотация
Статья посвящена вопросам моделирования защищенной программно-аппаратной инфраструктуры киберфизической системы управления водоснабжением. **Предмет исследования.** В работе раскрывается разработанная автором модель киберфизической системы управления водоснабжением, как основа для анализа возможных действий нарушителя и моделирования конкретных событий и инцидентов безопасности. **Метод.** Применяются методы аналитического моделирования и системного анализа для определения инцидентов безопасности с возможностью последующей выработки контрмер. **Основные результаты.** Проведен анализ критически-важных характеристик, предложена модель целевой киберфизической системы управления водоснабжением. В работе проводится моделирование атак на систему управления водоснабжением, на основе которой производятся анализ инцидентов безопасности. **Практическая значимость.** Разработанная модель направлена на выявление инцидентов безопасности и повышение уровня защищенности систем управления водоснабжением от многошаговых атакующих воздействий.

Ключевые слова
защищенные киберфизические системы, модель нарушителя, инциденты безопасности.

Информация о статье
УДК 004.55
Язык статьи – русский.
Поступила в редакцию 07.07.17, принята к печати 01.09.17.

Ссылка для цитирования: Десницкий В. А. Модель киберфизической системы управления водоснабжением для анализа инцидентов безопасности // Информационные технологии и телекоммуникации. 2017. Том 5. № 3. С. 93–102.

A MODELING AND ANALYSIS OF SECURITY INCIDENTS IN A CYBER-PHYSICAL SYSTEM FOR WATER SUPPLY MANAGEMENT

V. Desnitsky [1,2,3*]

[1] SPIIRAS, St. Petersburg, 199178, Russian Federation
[2] SPbSUT, St. Petersburg, 193232, Russian Federation
[3] ITMO University, St. Petersburg, 197101, Russian Federation
* Corresponding author: desnitsky@comsec.spb.ru

Abstract—The paper comprises modeling of secure hardware and software infrastructure of a cyber-physical system for water supply management. **Research subject.** The developed model of a system for water supply management is exposed as a basis for an analysis of possible intruder actions and modeling particular security events and incidents. **Method.** Methods of analytical modeling and system analysis are applied to determine security incidents, assuming subsequent production of countermeasures. **Core results.** An analysis of critically important characteristics and modeling of a target cyber-physical system are carried out. A model of a system for water supply management is proposed, attacks on the system are modeled. Analysis of security incidents is performed. **Practical relevance.** The developed model is targeted on revelation of security incidents and increasing the security level of systems for water supply management against multi-step attacks.

Keywords—secure cyber-physical systems, intruder, security incidents.

Article info
Article in Russian.
Received 07.07.17, accepted 01.09.17.

For citation: Desnitsky V.: A Modeling and Analysis of Security Incidents in a Cyber-Physical System for Water Supply Management // Telecom IT. 2017. Vol. 5. Iss. 3. pp. 93–102 (in Russian).

Введение

Современные системы водоснабжения используются для распределения и накопления ресурсов в период избытка поступающей воды, питания гидроэлектростанций, полива, контроля уровня внутренних водных путей, в целях ирригации и др. Автоматизация систем управления, наличие программно-аппаратных уязвимостей, а также их критически важный характер обуславливает необходимость обеспечения повышенных требований к защищенности таких систем и предоставляемых ими сервисов. При этом разнородные используемые датчики физических характеристик, исполнительные устройства, программно-аппаратные интерфейсы, такие как RS-232, RFID, XBee, Wi-Fi и др. могут служить точками доступа потенциального нарушителя к элементам и функциям системы, компрометация которых позволяет путем последовательного повышение привилегий успешно осуществлять сложные многошаговые киберфизические атаки. Анализ физических и программно-информационных событий в системе

в рамках процессов динамического мониторинга на основе анализа действий нарушителя и правил корреляции информации позволит выявлять критически важные инциденты киберфизической безопасности, а также повысить уровень защищенности целевых систем.

Цель настоящего исследования — проведение анализа инцидентов киберфизической безопасности комплексной программно-технической системы управления водоснабжением на основе моделирования инфраструктуры системы водоснабжения и киберфизических процессов в ней. Для достижения цели в работе решаются следующие задачи: анализ характеристик целевой системы управления водоснабжением; разработка модели и программно-аппаратного прототипа системы управления водоснабжением; моделирование атак на базе разработанного программно-аппаратного прототипа и анализ инцидентов киберфизической безопасности. К отличительным особенностям работы относится использование в рамках предложенной модели унифицированных интерфейсов представления данных от гетерогенных источников системы управления водоснабжением, используемых в рамках компонента адаптера данных, а также их интеграция в рамках базы архивных данных в целях обеспечения процессов мониторинга.

1. Анализ характеристик целевой системы

Разновидности и функциональное наполнение систем управления водоснабжения и особенности их инфраструктур определяют способы управления, процессы мониторинга ресурсов, бизнес-процессы и уровень ее защищенности, так как в работе участвуют различные компоненты, сенсоры и устройства с отличающимися требованиями и расчётными нагрузками [1]. Можно выделить следующие элементы типовой системы:

- управляющие программно-аппаратные компоненты — микроконтроллеры с заданными цифровыми и аналоговыми интерфейсами;
- датчики, отвечающие за измерения, связанные с конкретными физическими процессами, которые позволяют получить числовую или бинарную характеристику физических факторов системы, необходимых для осуществления мониторинга процессов водоснабжения;
- шлюзы, которые регулируют величину протока воды путем открывания и закрывания затворов;
- связующие проводные и беспроводные каналы связи для передачи служебной и бизнес-информации системы;
- терминальные машины операторов для автоматизированного наблюдения и контроля за процессами системы;
- компоненты мониторинга системы, включающие анализатор инцидентов киберфизической безопасности — компоненты сбора и хранения данных, интерфейс взаимодействия с человеком, а также систему видеонаблюдения, систему контроля и управления доступом, систему пожарной и охранной сигнализации и др.

На рис. 1 схематично показаны используемые в работе датчики, в том числе датчики уровня воды, инклинаторы и наклономеры, используемые для измерения горизонтальных (продольных) движений земной коры, наклона и поворота стен, способных приводить к разрушению стен и опор, датчики

для измерения изменений размеров трещин и разломов, датчики измерения изменений расстояния между стыками блоков системы, датчики давления, Пьезометры, Турбидиметры, Термометры.

Рис. 1. Датчики системы управления водоснабжением

Деятельность систем управления водоснабжения необходимо поддерживать путём непрерывного мониторинга ключевых параметров, таких как состояние окружающей среды, геофизических и геотехнических параметров, который может осуществлять путём установки множества датчиков. Датчики способны самоорганизовываться для создания ячеистой сети, что позволяет более эффективно передавать собранную информацию на устройства сбора и обработки данных [2]. Реализация такого непрерывного мониторинга позволяет повысить уровень защищенности системы, при этом разнородность приведенных устройств и компонентов определяет технологическую сложность объединения и контроля защищенности процессов системы управления водоснабжением.

2. Модель системы управления водоснабжением

Физическая модель системы управления водоснабжением включает ряд гидротехнических приспособлений — емкостей для воды, сенсоров, переключателей, шлангов, работающих в связке с микроконтроллером, которые на физическом уровне позволяют промоделировать процессы протекания воды, открытие и закрытие затворов, превышение уровня воды установленных ограничений, а также программно-информационную часть системы, ответственную за сбор, обработку, анализ и отображение оператору основных критически-важных событий и инцидентов безопасности системы.

Как объект управления инцидентами система интегрирует в себе технические, информационные и организационные средства, реализуя на основе микроконтроллера механизмы управления инцидентами безопасности с учетом текущей политики безопасности и средств пользовательского интерфейса с возможностью отображения в реальном времени оперативных данных. Модель системы позволяет также проводить на ее основе эксперименты, связанные с моделированием сложных, растянутых во времени и происходящих на различных уровнях атакующих воздействий.

Предполагается, что модель системы должна обеспечивать требуемые целевые процессы как на физическом уровне — в части контроля уровня воды, уровня потока воды, поддержания определённого уровня воды в резервуаре, так и на программно-информационном уровне — в части сбора, хранения, обработки данных, полученных от датчиков, оповещения, составления отчётов, контроля и управления системой удалённо. Модель системы управления водоснабжением также включает механизмы определения некорректного функционирования вследствие действий нарушителя или неправильного использования инфраструктуры системы и реагирования с формированием инцидентов безопасности и выдачей рекомендаций для решения выявленных проблем. При этом в качестве основных в процессе проектирования системы используются функциональные и нефункциональные требования, формулируемые с использованием системы количественных и качественных показателей [3]. Формулируются требования к отдельным компонентам системы с использованием характеристик их совместимости между собой, а также нефункциональных характеристик производительности, энергоэффективности и др.

На рис. 2 приведена структурная модель системы управления водоснабжением, описывающие основные компоненты системы и ее архитектурные особенности. Устройства ввода/вывода включают специализированные датчики и исполнительные устройства. Датчики отвечают за получение измерений, связанных с конкретными физическими процессами. Их измерительные сигналы преобразуются в цифровые данные с помощью RTU-модулей (*Remote Terminal Unit*) — устройства связи с объектом. Исполнительные устройства отвечают за преобразование цифрового сигнала в физическое воздействие, с целью контроля, прямо или косвенно, других физических объектов, которые работают в связке с микроконтроллером. При этом адаптер данных обеспечивает связь с системой мониторинга с помощью разнородных слоёв передачи данных, работая с различными физическими носителями информации и технологиями проводной и беспроводной связи.

Устройства управления включают инженерные рабочие станции, базы данных и пользовательский интерфейс. Центр управления SCADA отвечает за оценку, обработку, хранение собираемых с датчиков данных. Он соединён с компонентами нижнего уровня с помощью главного терминала, и доступен оператору через специализированный интерфейс. База архивных данных позволяет хранить события, оповещения системы безопасности и собранные данные измерений, а также распространять их по всей системе или её частям. В частности, данные включают в себя информацию с датчиков, данные о работе операторов, административные логи. База данных используется также в статистическом анализе, диагностике и расследовании инцидентов безопасности в целях долгосрочного мониторинга инфраструктуры системы.

Пользовательский интерфейс позволяет оператору контролировать процессы и проверять статус системы с использованием графических индикаторов, таких как всплывающие окна, мигающие зоны, текстовые сообщения и другие формы визуализации информации. К отличительным особенностям предложенной модели относятся использованием унифицированных интерфейсов представления данных от гетерогенных источников системы управления водоснабжением, используемых в рамках компонента адаптера данных, а также их интеграция в рамках базы архивных данных в целях обеспечения процессов

мониторинга. Разработанный программно-аппаратный прототип системы управления водоснабжением базируется на микроконтроллерах Arduino Mega 2560 и Raspberry Pi, аналоговых угловых датчиках уровня воды, датчиках протока воды, моторизованных шаровых кранах, а также портативного погружного электронасоса, смонтированных на двух соединяющихся резервуарах воды и моделирующих полный цикл работы водяной системы с возможностью удаленного мониторинга в динамике состояния датчиков и установки параметров исполнительных устройств.

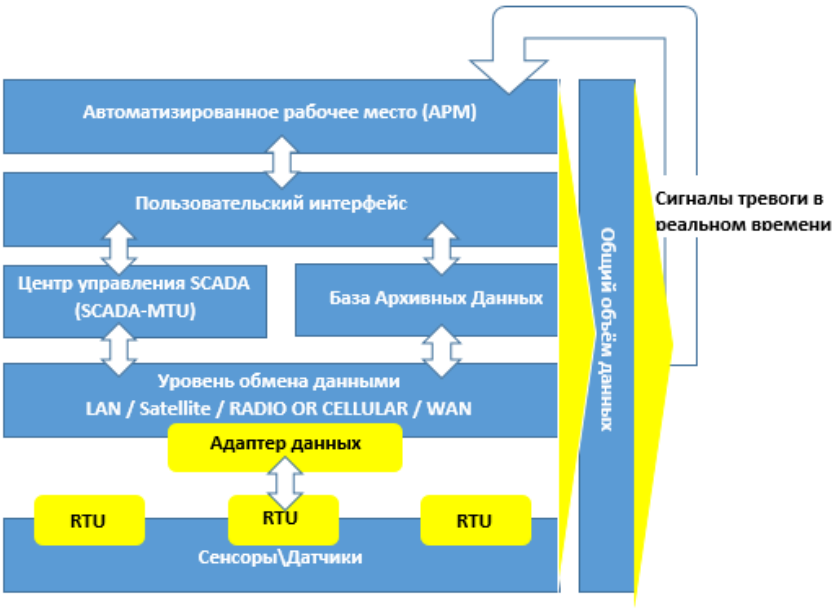

Рис. 2. Модель системы управления водоснабжением

3. Моделирование атак на систему управления водоснабжением

Атаки на систему управления водоснабжением моделируются с использованием следующих двух классификаций нарушителя, пытающегося скомпрометировать инфраструктуру целевой системы или ее сервисы: по типу доступа к инфраструктуре системы управления водоснабжением [4] и по возможностям нарушителя [5]. Задаются следующие пять типов нарушителя:

- *тип 0* — нарушитель не имеет прямого доступа к инфраструктуре или сервисам системы управления водоснабжения, нарушитель применяет приемы социальной инженерии;
- тип 1 — нарушитель взаимодействует с инфраструктурой или сервисами системы управления водоснабжением опосредованно, осуществляя непрямой доступ к ним;
- тип 2 — нарушитель воздействует на инфраструктуру системы управления или её сервисы напрямую, находясь при этом на некотором расстоянии от защищаемого помещения;
- *тип 3* — нарушитель имеет физический доступ к инфраструктуре системы управления водоснабжением, но не имеет возможности исследовать и модифицировать её внутренние электронные компоненты;

- *тип 4* — нарушитель имеет полный доступ к инфраструктуре системы управления водоснабжением и всем её микросхемам, и внутренним интерфейсам.

При этом нарушитель может иметь один из следующих трех уровней возможностей, определяющий организационно-техническую сложность атакующих воздействий, которые может воспроизводить нарушитель [6]:

- *уровень 1* — нарушитель эксплуатирует находящиеся в открытом доступе программно-аппаратные инструменты и уже известные уязвимости;
- *уровень 2* — нарушитель способен выявлять и эксплуатировать ранее неизвестные уязвимости и разрабатывать новые программно-аппаратные инструменты для воздействия на целевое. систему;
- *уровень 3* — нарушитель уровня 2, характеризующийся вдобавок наличием неограниченных программно-аппаратных и финансовых ресурсов для осуществления атак.

Тогда как нарушитель типа 0 опирается в основном на приемы социальной инженерии, для нарушителей типа 1, 2, 3 и 4 социальная инженерия может представлять собой некоторый предваряющую стадию атаки, связанную с анализом поведения персонала системы управления водоснабжением, способствующую ускорению атаки или величины ущерба от нее. К мерам противодействия таким атакам можно отнести выполнение персоналом заданных политик безопасности, внедрение механизма выявления и контроля аномальных данных и др.

Атакующие воздействия на элементы системы водоснабжения требуют наличия открытых коммуникационных интерфейсов для осуществления взаимодействия с элементами системы [7]. Атакующий способен перехватывать потоки данных на основе атак типа "человек посередине" на интерфейсы Ethernet, Wi-Fi (тип 1 нарушителя), RFID или XBee (тип 2 нарушителя), анализировать программные сервисы устройств системы и производить поиск слабых мест в программном обеспечении.

Нарушители типа 1 и типа 2 могут также осуществлять атаки на основе эксплуатации уязвимостей конкретных компонентов системы водоснабжения, в том числе уязвимости микроконтроллеров Arduino, универсальных сетевых атак, атак истощения энергоресурсов и пр.

Действия нарушителя типа 3 предполагают наличие его непосредственного воздействия, как на информационно-физический объект, в том числе подачу некорректных данных на serial-интерфейсы, атаку по сторонним каналам, атаки внедрения ложного устройства, многошаговые комбинированные атаки, включающие одновременные физические воздействия на сенсоры, исполнительные устройства и программно-информационные воздействия.

Нарушитель типа 4 рассматривает систему как на набор взаимосвязанных микроконтоллеров, сенсоров, исполнительных модулей и связующего сетевого оборудования. Нарушитель может производить декомпиляцию программного кода, воздействовать на данные и вычислительные процессы физически, в том числе с использованием электронных осциллографов и микроскопов. В качестве примеров рассмотрим следующие два инцидента.

Пример 1. Инцидент некорректности значений сенсоров системы: выявлены противоречия между данными от сенсора уровня воды в резервуаре и сенсора давления, каждый из которых позволяет судить об объеме находящейся

в нем воды. Уровень воды - ключевой параметр системы управления водоснабжением. В предположении, что атакующий воздействовал на сенсор уровня воды с целью формирования некорректных данных о состоянии системы, датчик давления, являясь менее доступным физически в рамках реальной инфраструктуры системы управления водоснабжением, может рассматриваться в качестве контрольного.

Пример 2. Инцидент несоответствия команд оператора, инициированных на программно-информационной уровне и показаниями датчиков. Оператором системы управления водоснабжением дана команда на открытие затвора в условиях того, что уровень воды располагается выше данного затвор. Дальнейшие показания сенсоров давления, сенсоров протока и сенсоров уровня воды не зафиксировали ожидаемых изменений. В соответствии с этим создаётся инцидент безопасности и формируется уведомление оператора о необходимости визуальной проверки уровня воды и проверки датчиков на предмет корректности их работы.

4. Анализ инцидентов безопасности

Рассмотрены возможные инциденты безопасности системы управления водоснабжением, сформулированы правила корреляции инцидентов безопасности, а также проведены моделирование и выявление этих событий на разработанном прототипе модели системы управления водоснабжением. Целевая система реагирует на следующие события: изменение уровня воды в резервуаре; изменение давления воды в резервуаре; изменение потока воды через шлюз; изменение состояния затвора. При любом из этих событий, система проводит аналитическую обработку данных в части их корреляции и формирования инцидентов безопасности.

Инцидент безопасности формулируется в виде пары (I, t_0), где I — набор взаимосвязанных событий, произошедших в системе за временной промежуток t_0. Формирование инцидента свидетельствует о наличие действий атакующего, направленных на нарушение одного или нескольких требований информационной безопасности. В общем виде правило корреляции событий имеет следующий вид: $(\{ev\_sw_i)\}_i \cup \{ev\_ph_i\}, t) \rightarrow Type_{Inc}$, где ev_sw_i — набор событий программно-информационного характера, в ev_ph_j — события физического характера, выполнение которых в рамках фиксированного временного промежутка t, определяет наличие инцидента заданного типа $Type_{Inc}$.

В качестве примера следующее правило корреляции определяет инцидент несоответствия показаний датчиков уровня воды, являющихся результатом атаки с параллельным физическим воздействием на датчик уровня воды и программно-информационным воздействием на уровне пользовательского интерфейса на основе перебора пароля оператора методом грубой силы: $((l_1 == false), (l_2 == true), ep, opn) \rightarrow inc$, где несрабатывание датчика уровня водs l_1 при сработавшем датчик l_2 и событии ep несанкционированного получения доступа к управлению системой и события opn — открытия затвора обуславливает инцидент возможного затопления водяного резервуара.

Злоумышленник получает возможность влиять на показания сенсора датчика уровня воды с целью формирования некорректных данных о состоянии системы управления водоснабжением, тем самым вводя систему в заблуждение

о реальных физических характеристиках. В ходе атаки злоумышленник подменяет данные скомпрометированного сенсора уровня воды с целью инициировать алгоритм реагирования на инцидент переполнения воды в резервуаре, и тем самым, открыв затворы, спровоцировать сброс воды. В результате полученные от скомпрометированного датчика данные будут указывать на увеличение уровня воды в резервуаре до критического уровня. Проведенные эксперименты на базе разработанного программно-аппаратного прототипа системы управления водоснабжением с моделированием на натурной модели действий нарушителя показали выполнимость целей мониторинга путем успешного выявления и последующего уведомления оператора о выявленном инциденте информационной безопасности.

Заключение

В работе проведен анализ критически-важных характеристик и предложена модель киберфизической системы управления водоснабжением. Проводятся моделирование атак на систему управления водоснабжением и анализ инцидентов безопасности. Работа выполнена при финансовой поддержке РФФИ (проекты 15-07-07451, 16-29-09482 офи_м) и бюджетных тем № 0073-2015-0004.

Литература

1. Wu J., Zhang Y., Liang X. Design of Wireless Dam Security Information System // International Conference on Measuring Technology and Mechatronics Automation. 2010. pp. 1072–1076.

2. Doğan R., Erdem E. Temperature and humidity control of the tunnels in the dam using wireless sensor networks // 19th International Conference on Intelligent Engineering Systems (INES). 2015. pp. 379–383.

3. Desnitsky V., Kotenko I. Design and Verification of Protected Systems with Integrated Devices Based on Expert Knowledge // Automatic Control and Computer Sciences. 2015. Vol. 49. Iss. 8. pp. 648–652.

4. Rae A. J., Wildman L. P. A Taxonomy of Attacks on Secure Devices // Australian Information Warfare and IT Security. 2003. pp. 251–264.

5. Abraham D.G., Dolan G.M., Double G.P., Stevens J.V. Transaction security system // IBM Systems Journal. 1991. Vol. 30. Iss. 2. pp. 206–228.

6. Десницкий В. А., Чечулин А. А., Котенко И. В., Левшун Д. С., Коломеец М. В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. № 5 (48). С. 5–31.

7. Desnitsky V., Kotenko I. Nogin S. Detection of Anomalies in Data for Monitoring of Security Components in the Internet of Things // XVIII International Conference on Soft Computing and Measurements (SCM). 2015. pp. 189–192.

References

1. Wu J., Zhang Y., Liang X. Design of Wireless Dam Security Information System // International Conference on Measuring Technology and Mechatronics Automation. 2010. pp. 1072–1076.

2. Doğan R., Erdem E. Temperature and humidity control of the tunnels in the dam using wireless sensor networks // 19th International Conference on Intelligent Engineering Systems (INES). 2015. pp. 379–383.

3. Desnitsky V., Kotenko I. Design and Verification of Protected Systems with Integrated Devices Based on Expert Knowledge // Automatic Control and Computer Sciences. 2015. Vol. 49. Iss. 8. pp. 648–652.

4. Rae A. J., Wildman L. P. A Taxonomy of Attacks on Secure Devices // Australian Information Warfare and IT Security. 2003. pp. 251–264.

5. Abraham D. G., Dolan G. M., Double G. P., Stevens J. V. Transaction security system // IBM Systems Journal. 1991. Vol. 30. Iss. 2. pp. 206–228.

6. Desnitsky V., Chechulin A., Kotenko I., Levshun D., Kolomeec M. Combined Design Technique for Secure Embedded Devices Exemplified by a Perimeter Protec-tion System // SPIIRAS Proceedings. 2016. No. 5 (48). pp. 5–31.

7. Desnitsky V., Kotenko I. Nogin S. Detection of Anomalies in Data for Monitoring of Security Components in the Internet of Things // XVIII International Conference on Soft Computing and Measurements (SCM). 2015. pp. 189–192.

Десницкий Василий Алексеевич – кандидат технических наук,
старший научный сотрудник, СПИИРАН,
Санкт-Петербург, 199178, Российская Федерация;
доцент, СПбГУТ, Санкт-Петербург, 193232,
Российская Федерация; инженер,
Университет ИТМО, Санкт-Петербург, 197101,
Российская Федерация, desnitsky@comsec.spb.ru

Desnitsky Vasily – Candidate of Engineering, Senior Research Officer,
SPIIRAS, St. Petersburg, 199178, Russian Federation;
Associate Professor, SPbSUT, St. Petersburg,
193232, Russian Federation; engineer,
ITMO University, St. Petersburg, 197101,
Russian Federation, desnitsky@comsec.spb.ru