

## ПРОФЕССИОНАЛИЗАЦИЯ УПРАВЛЕНЧЕСКОГО ОБРАЗОВАНИЯ


### Внедрение методологии быстрой оценки объектов критическая инфраструктура для учреждений образования

**Николай Николаевич Лансере**

аспирант

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича  
Санкт-Петербург, Россия


krasov@inbox.ru

 0000-0000-0000-0000

Поступила в редакцию 17.02.2022

Принята 19.03.2022

Опубликована 05.04.2022

 10.25726/e0560-7007-4832-f

#### Аннотация

В статье разработана и внедрена в программный комплекс системы ЕАИС методика оценки результатов освоения образовательных программ в области информационной безопасности. Она основана на теории нечетких множеств. Метод позволяет производить интегральный учет как количественных, так и качественных факторов адаптивного тестирования в рамках промежуточной аттестации освоения студентом дисциплины образовательной программы в области информационной безопасности. В рамках накопительной балльно-рейтинговой системы использование теории нечетких множеств позволяет накапливать баллы по 100-балльной шкале по всем видам учебной работы и формировать итоговый балл по каждой дисциплине образовательной программы в области информационной безопасности в зависимости от максимально возможных баллов, установленных для каждого объема выполненной работы.

#### Ключевые слова

WordPress, Атаки, Сканнер, Парсер, SQL, Brute Force, XSS, DDoS

#### Введение

В дошкольном возрасте начинает складываться самосознание ребёнка, его мировоззрение и стремительное развитие цифровых и интернет - технологий привело к формированию глобального информационного общества и цифровой экономики. Информационно – телекоммуникационные технологии проникли практически во все сферы: предпринимательскую деятельность, коммуникацию и предоставление услуг во всех отраслях, включая транспорт, финансовую сферу, обрабатывающий сектор, образование, здравоохранение, сельское хозяйство и другие отрасли, розничную торговлю, средства массовой информации, сферу развлечений и ведение бизнеса. Благодаря этому происходит глобальная трансформация экономики и социальной сферы. Ускоряются темпы мирового экономического развития, повышается производительность труда в существующих отраслях, формируются новые рынки и отрасли. И чем активнее идет развитие информационно телекоммуникационных технологий, тем серьезнее становятся угрозы безопасности информации.

#### Материалы и методы исследования

Для примера, как на первый взгляд незначительная ошибка разработчика программного обеспечения может привести к крупным убыткам. 2018 год, известный сетевой магазин (Азбука вкуса) запускает бонусную программу, при регистрации в которой клиент получает 50 бонусов, эквивалентных

50 рублям. Покупки в магазине можно оплачивать полностью бонусами. В личном кабинете есть возможность перевода бонусов с аккаунта на аккаунт без каких-либо ограничений, этой уязвимостью и воспользовались злоумышленники. Существует множество сервисов для предоставления за небольшую плату виртуальных телефонных номеров для приема смс сообщений. Таким образом с использованием не хитрого программного обеспечения регистрировалось большое число «левых» аккаунтов, после чего средства собирались на «основном» аккаунте, а торговая сеть несла убытки.

2020 год сайт РЖД запустил программу лояльности «РЖД Бонус», с простыми условиями, клиент приглашал пройти регистрацию по ссылке своего знакомого и после регистрации оба получали по 400 баллов. Разработчиками была допущена серьезная ошибка, а именно при регистрации нового аккаунта не требовалось его верификации, новые аккаунты можно было регистрировать на одинаковые паспортные данные, чаще всего ненастоящие, что очень сильно упростило написание программы для регистрации аккаунтов. Таким образом злоумышленники могли передвигаться на поездах с минимальными затратами, а организация несла убытки. Как видно из представленных примеров очень важно учитывать все возможные риски при проектировании и эксплуатации. Убытки организаций от действий злоумышленников меркнут по сравнению с возможными убытками и уроном, который может произойти при деструктивном воздействии на автоматизированные системы управления технологическими процессами на критически важных объектах (АСУ ТП КВО).

### **Результаты и обсуждение**

История появления АСУ ТП уходит корнями в далекие 1756 год, когда российский механик Н.И. Ползунов разработал регулятор питания парового котла водой и в 1784 год, когда англичанин Д. Уатт разработал регулятор скорости паровой машины. Длительное время регуляторы паровой машины были основными видами автоматических устройств управления в промышленности. Следующее бурное развитие теории и практики автоматического регулирования получили в тридцатые и сороковые годы XX столетия. С появлением электронных вычислительных машин (ЭВМ), и быстрый рост их технических характеристик (производительности, объемов памяти, надежности) позволили использовать такие машины в промышленности для автоматизации процессов обработки информации и решения задач управления. Одной из первых промышленных АСУ ТП, где электронные вычислительные машины применялись в режиме формирования уставок аналоговым регуляторам, является построенная в 1959 году в США система управления нефтеперегонным процессом. В дальнейшем переход на новую элементную базу и появление интегральных микросхем позволили на порядок снизить стоимость единицы вычислительной мощности ЭВМ и повысить ее надежность. Прародителями создания современных АСУ ТП стали создание локальных вычислительных сетей и разработка программируемого логического контроллера. В настоящее время мы видим децентрализованные распределенные автоматизированные системы управления, пример которой представлен на рис. 1.

Из представленной на рисунке 1 схемы видно, что АСУ ТП имеет три уровня:

- 1) верхний уровень – уровень операторского управления, куда обычно входят операторские, инженерные автоматизированные рабочие места, промышленные серверы (SCADA – серверы) с установленным на них общесистемным и прикладным программным обеспечением, телекоммуникационное оборудование;
- 2) средний уровень – уровень автоматического управления, где располагаются программируемые логические контроллеры, иные технические средства с установленным программным обеспечением, получающие данные с нижнего (полевого) уровня, передающие данные на верхний уровень, также промышленная сеть передачи данных;
- 3) нижний (полевой) уровень – уровень ввода (вывода) данных исполнительных устройств, куда включаются датчики, исполнительные механизмы, другие аппаратные устройства с установленными в них микропрограммами и машинными контроллерами.

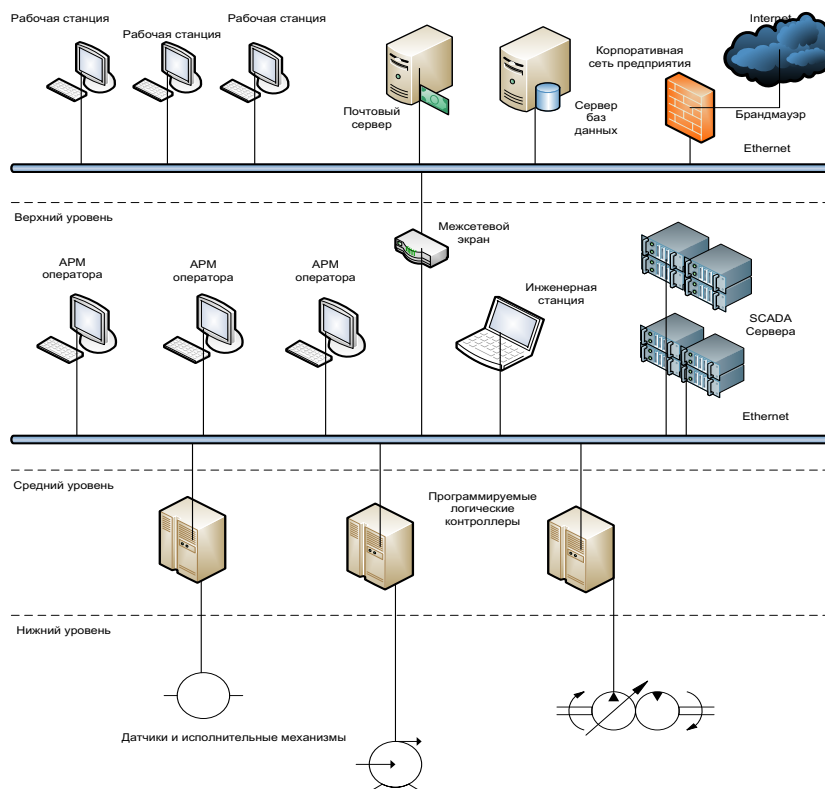


Рисунок 1. Схема АСУ ТП

На схеме так же можно видеть, что корпоративная сеть предприятия, имеющая выход в сеть Интернет, подключена к промышленной сети АСУ ТП. Еще лет 10 назад воздушный зазор между промышленными сетями и другими сетями предприятия был простым решением для минимизации угроз. Однако, на сегодняшний день постоянно растет оперативность получения разного рода отчетности о состоянии предприятия для быстрого принятия решений, тем самым корпоративные сети все больше интегрируются в промышленные сети. Системы управления производством, такие как MES, ERP, работающие в корпоративной сети контролируют весь процесс управления производством. Доступ в Интернет из промышленных сетей не всегда, может быть, из-за слабых ограничений. Очень часто – это вынужденная необходимость. Обособленные части промышленных сетей могут находиться в труднодоступных местах, не требовать постоянного обслуживания, мониторинг осуществляется по каналам связи. Эксплуатирующий персонал посещает, как правило, такие объекты с целью плановых проверок или в экстренных случаях. Необходимо отметить, что техническое сопровождение таких объектов очень часто выполняется работниками подрядных, а порой и субподрядных организаций. Такая работа часто осуществляется с использованием удаленного доступа к промышленной сети заказчика из корпоративной сети подрядной организации. В зависимости от ограничений и обстоятельств каждой конкретной ситуации работник подрядчика имеет возможность подключения к промышленной сети заказчика, находясь в любом месте, где есть доступная сеть для выхода в Интернет. Работник, подключающийся из-за пределов промышленной сети предприятия заказчика, часто имеет высокие права доступа на уровне локальной системы или на уровне всей сети. Такой пользователь имеет возможность случайно или намеренно заразить компьютеры промышленной сети. Таким образом промышленные сети становятся все больше похожими на корпоративные и соответственно появляются угрозы как в корпоративных сетях.

Рассмотрим наиболее актуальные угрозы для современных АСУ ТП.

1. Незащищенный канал технической поддержки
2. Незащищенное интернет-соединение
3. Неучтенные отчуждаемые носители информации

Участники хакерской группировки FIN7 использовали почту США для отправки USB-накопителей с вредоносным программным обеспечением сотрудникам американских компаний, в том числе из оборонной и транспортной отраслей. Злоумышленники рассчитывают на доверчивость людей и то, что они будут использовать полученные в качестве подарка накопители на рабочих местах. Согласно имеющимся данным, чаще всего флешки с вредоносным ПО распространялись от имени Министерства здравоохранения США и некоторых социальных служб. Для большей убедительности злоумышленники снабжали посылки описанием содержимого накопителя, утверждая, что на нём хранятся важные данные касательно эпидемии коронавирусной инфекции и актуальные рекомендации для граждан. В некоторых случаях вредоносные USB-накопители доставлялись в декоративной подарочной упаковке, как если бы они были отправлены через Amazon, и дополнялись поддельными благотворительным письмом и подарочной картой.

4. Настройки межсетевых шлюзов
5. Неучтенные переносные компьютеры
6. Изменение программ программируемых логических контроллеров

Сведения о результате категорирования включаются в специальную форму, утверждённую ФСТЭК России (Приказ ФСТЭК №236 22 декабря 2017). Отдельно по каждому объекту и направляются в ФСТЭК России (Постановление, 2018; Ф3, 2017).

При проведении категорирования, организации как правило путают понятия:

- Анализ потенциальных угроз, проводимый при проектировании системы обеспечения безопасности значимого объекта в соответствии с приказом ФСТЭК России №239 от 25 декабря 2017.
- Оценка последствий инцидента с участием объекта КИИ, которая приводится при категорировании.

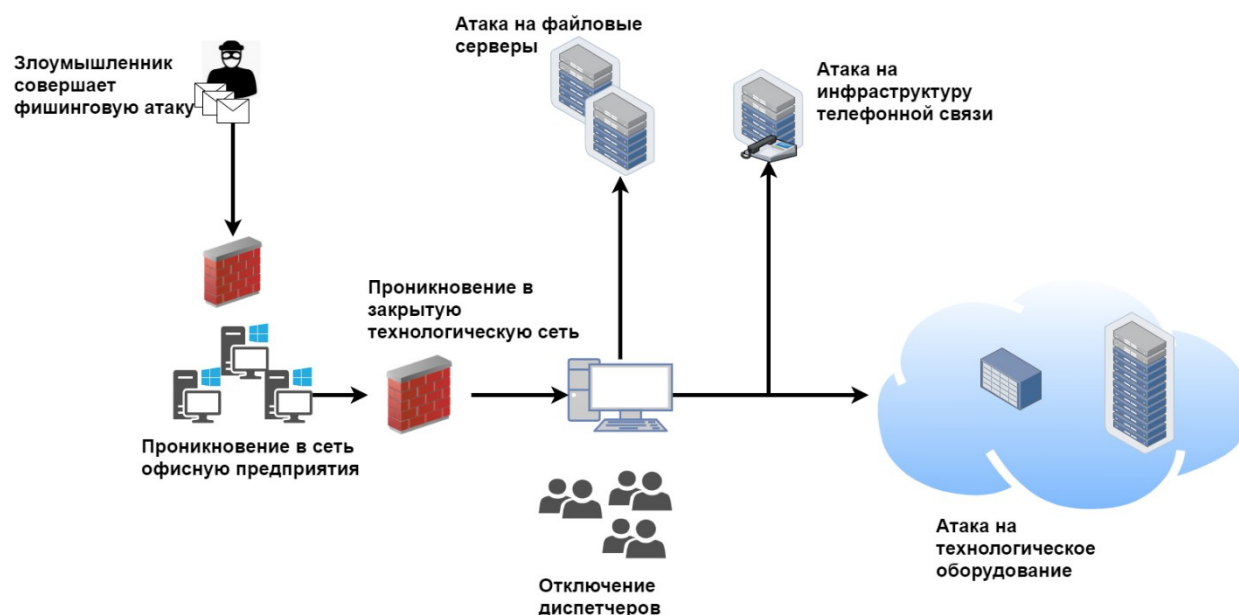


Рисунок 2. Возможные векторы атак на предприятие

В одном из указанных случаев решается задача выбора основных мер обеспечения безопасности и способов их реализации. Для выбора реализации меры защиты, нужно оценивать вероятные способы реализации атак, для этого законом предписано использовать банк данных угроз и уязвимостей ФСТЭК России (Дущин, 2010; Котенко, 2012; Штеренберг, 2016). Для того что бы оценить последствия нарушения работы объекта КИИ такая детализация не требуется и является бесполезной.

Если рассматривать на примере системы теплообеспечения. На стадии категорирования, известен технологический процесс: котёл нагревает теплоноситель, насосы закачивают холодную воду

в котёл, а горячую – в трубы теплотрассы, подача теплоносителя в отдельные части теплотрасс реализуется задвижками, давление контролируют специальные датчики, превышение определённых показателей приведёт в действие аварийный останов. Перечисленные компоненты управляются автоматизированной системой.

Во время категорирования принимается в качестве аксиомы, если не обеспечивать защиту системы от действий третьих лиц, то такие лица могут воздействовать на отдельные элементы системы. Исходя из этого, эксперты ставят себя на место злоумышленника и оценивают возможные сценарии его действий делая упор на причинение максимального ущерба. К примеру, нарушитель потенциально может отключить аварийный останов, перекрыть задвижку котла и увеличить до максимума мощность насоса. Что бы проверить вероятность события не требуется оценивать, насколько возможно внедрить вредоносное ПО или изменить данные программы управления или различные угрозы, указанные в банке данных ФСТЭК России. Достаточно того, что системы управления позволят злоумышленнику, выполнить перечисленные действия, и это может подтвердить компетентный специалист из отдела эксплуатации (Красов, 2019; Котенко, 2012; Штеренберг, 2016).

Категорирование объектов КИИ – Форма оценки рисков безопасности объектов IT-инфраструктур используемых в важных для государства и общества сферах экономики. Уникальность данного процесса вызвана тем, что объекты могут принадлежать частным организациям и физическим лицам, но при этом создавать серьёзные угрозы для общества и государства.

### **Заключение**

Процесс категорирования объектов КИИ можно сравнить с определением уровней защищённости информационных систем персональных данных. Проводится в соответствии с Постановлением правительства РФ от 01.11.2012 №1119, просматривается эволюция в подходе регулятора к созданию требований. Свойства информации (Конфиденциальность, целостность, доступность) не рассматриваются как самостоятельная ценность, которая требует защиты. В случае с КИИ требуется оценивать какой реальный урон может нанести злоумышленник, влияя на информационные или технологические процессы. Такой метод оценки не использовался до 2017 года в практике российской информационной безопасности. Таким образом важность категорирования заключается в том, что коммерческие компании и промышленные предприятия, впервые объективно начали оценивать защищённость информационных систем и систем управления. После проведения категорирования руководство большинства компаний начало пересматривать свою политику в области защиты информации увидев фактическую беззащитность своих инфраструктур от внешних угроз.

### **Список литературы**

1. Душин, С.Е., Красов А.В., Литвинов Ю.В. Моделирование систем и комплексов / Санкт-Петербург, 2010.
2. Котенко И.В., Дойникова Е.В., Чечулин А.А. Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения // Защита информации. Инсайд. 2012. № 4 (46). С. 54-66.
3. Красов А.В., Косов Н.А., Холоденко В.Ю.. Исследование методов провизининга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-journal. 2019. № 13-2 (37). С. 243-247.
4. Красов А.В., Левин М.В., Цветков А.Ю. Управление сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. 2015. № 1. С. 141-146.
5. Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И.Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // Т-Сотм: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36-40.

6. Миняев А.А., Красов А.В., Сахаров Д.В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 29-33.
7. Постановление правительства РФ от 8 февраля 2018 г. n 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры российской федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры российской Федерации и их значений»
8. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 n 187-фз
9. Федеральный закон «О персональных данных» от 27.07.2006 n 152-фз 9. Федеральная служба по техническому и экспортному контролю приказ от 22 декабря 2017 г. n 236 об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (в ред. приказа ФСТЭК России от 21 марта 2019 г. n 59)
10. Штеренберг С.И., Полтавцева М.А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59-68. [19:49]
11. Штеренберг С.И., Штеренберг И.Г. Вероятностные методы построения элементов самообучения адаптивных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. № 1. С. 53-56.
12. Shterenberg S.I., Poltavtseva M.A. A distributed intrusion detection system with protection from an internal intruder // Automatic Control and Computer Sciences. 2018. Т. 52. № 8. С. 945-953.


### **Implementation of the methodology of rapid assessment of critical infrastructure facilities for educational institutions**

**Nikolai N. Lancere**

graduate student

St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruевич St. Petersburg, Russia


krasov@inbox.ru

 0000-0000-0000-0000

Received 17.02.2022

Accepted 19.03.2022

Published 05.04.2022

 10.25726/e0560-7007-4832-f

#### **Abstract**

In the article, a methodology for evaluating the results of mastering educational programs in the field of information security has been developed and introduced into the software package of the EAIS system. It is based on the theory of fuzzy sets. The method allows for integral accounting of both quantitative and qualitative factors of adaptive testing within the framework of the intermediate certification of the student's mastery of the discipline of the educational program in the field of information security. Within the framework of the cumulative point-rating system, the use of fuzzy set theory allows you to accumulate points on a 100-point scale for all types of academic work and form a final score for each discipline of the educational program in the field of information security, depending on the maximum possible points set for each volume of work performed.

### Keywords

WordPress, Атаки, Сканнер, Парсер, SQL, Brute Force, XSS, DDoS

### References

1. Dushin, S.E., Krasov A.V., Litvinov Ju.V. Modelirovanie sistem i kompleksov / Sankt-Peterburg, 2010.
2. Kotenko I.V., Dojnikova E.V., Chechulin A.A. Obshee perechislenie i klassifikacija shablonov atak (CAPEC): opisaniye i primery primeneniya // Zashhita informacii. Insajd. 2012. № 4 (46). S. 54-66.
3. Krasov A.V., Kosov N.A., Holodenko V.Ju.. Issledovanie metodov provizhininga bezopasnoj seti na mul'tivendornom oborudovanii s ispol'zovaniem sredstv avtomatizirovannoj konfiguracii // Colloquium-journal. 2019. № 13-2 (37). S. 243-247.
4. Krasov A.V., Levin M.V., Cvetkov A.Ju. Upravlenie setjami peredachi dannyh s izmenjajushhejsja nagruzkoy // Vserossijskaja nauchnaja konferencija po problemam upravleniya v tehniceskikh sistemah. 2015. № 1. S. 141-146.
5. Krasov A.V., Shterenberg S.I., Fahrutdinov R.M., Ryzhakov D.V., Pestov I.E. Analiz informacionnoj bezopasnosti predpriyatija na osnove sbora dannyh pol'zovatelej s otkrytyh resursov i monitoringa informacionnyh resursov s ispol'zovaniem mashinnogo obuchenija // T-Comm: Telekommunikacii i transport. 2018. T. 12. № 10. S. 36-40.
6. Minjaev A.A., Krasov A.V., Saharov D.V. Metod ocenki jeffektivnosti sistemy zashhity informacii territorial'no-raspredelennyh informacionnyh sistem personal'nyh dannyh // Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tehnologii i dizajna. Serija 1: Estestvennye i tehnicieskie nauki. 2020. № 1. S. 29-33.
7. Postanovlenie pravitel'stva RF ot 8 fevralja 2018 g. n 127 «Ob utverzhdenii pravil kategorirovaniya ob#ektov kriticheskoj informacionnoj infrastruktury rossijskoj federacii, a takzhe perechnja pokazatelej kriteriev znachimosti ob#ektov kriticheskoj informacionnoj infrastruktury rossijskoj Federacii i ih znachenij»
8. Federal'nyj zakon «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii» ot 26.07.2017 n 187-fz
9. Federal'nyj zakon «O personal'nyh dannyh» ot 27.07.2006 n 152-fz 9. Federal'naja sluzhba po tehniceskomu i jeksportnomu kontrolju prikaz ot 22 dekabrja 2017 g. n 236 ob utverzhdenii formy napravlenija svedenij o rezul'tatah prisvoeniya ob#ektu kriticheskoj informacionnoj infrastruktury odnoj iz kategorij znachimosti libo ob otsutstvii neobhodimosti prisvoeniya emu odnoj iz takih kategorij (v red. prikaza FSTJeK Rossii ot 21 marta 2019 g. n 59)
10. Shterenberg S.I., Poltavceva M.A. Raspredelennaja sistema obnaruzhenija vtorzhenij s zashhitoy ot vnutrennego narushitelja // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2018. № 2. S. 59-68. [19:49]
11. Shterenberg S.I., Shterenberg I.G. Veroyatnostnye metody postroeniya jelementov samoobuchenija adaptivnyh informacionnyh sistem // Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tehnologii i dizajna. Serija 1: Estestvennye i tehnicieskie nauki. 2016. № 1. S. 53-56.
12. Shterenberg S.I., Poltavtseva M.A. A distributed intrusion detection system with protection from an internal intruder // Automatic Control and Computer Sciences. 2018. T. 52. № 8. S. 945-953.