СПЕЦИАЛИЗИРОВАННЫЙ КОМПЬЮТЕР С АППАРАТНОЙ ЗАЩИТОЙ ДАННЫХ M-TRUST: ПЛАТФОРМА ДЛЯ ЗАЩИЩЕННЫХ РЕШЕНИЙ

Выполнение требований 187-ФЗ и связанных с ним подзаконных актов сопряжено с очень большим количеством организационных мероприятий, которые необходимо провести в кратчайшие сроки. На этом фоне необходимые технические меры не кажутся проблемой, тем более что принципиально задачи технической защиты информации и способы их решения профессионалам хорошо понятны. Однако при переходе к планированию выясняется, что с реализацией этих способов на практике все пока не так благополучно, как в теории.

Это связано с тем, что объекты защиты информации всех типов (технические средства, данные, информационные технологии, каналы передачи данных), в КИИ крайне разнообразны, намного разнообразнее, чем в среднем в защищенных корпоративных или государственных информационных системах (см. табл. 1).

Таблица 1. Особенности объектов защиты информации в КИИ

Объекты защиты информации	«обычные» защищенные ИС	КИИ
Технические средства	Сервера, ПК, терминалы	То же, плюс управляющие элементы КИИ, разнообразные

		датчики и контроллеры
Данные	Файлы и данные	То же, плюс сигналы управления, данные измерений и контроля
Каналы	Ethernet	То же, плюс WiFi, BlueTooth, LTE и др.
Информационные технологии	Прикладное ПО и общесистемное ПО	То же, плюс ПО управления технологическими процессами

Что особенно важно – все это разнообразие практически не может быть унифицировано, а значит,

мероприятия по защите КИИ должны повлечь за собой применение столь же разношерстных средств защиты информации, которые необходимо спроектировать, внедрить и сопровождать. Все это грозит весьма ощутимыми расходами.

Особенно выпукло картина выглядит на примере защиты сетевого взаимодействия объектов КИИ: защищено должно быть все, а не только информационный уровень системы. Обменивающиеся по сети разнообразными данными и сигналами технические средства объектов КИИ не только сами по себе разнообразны, но и располагаться могут весьма нетривиальным для обычных информационных систем образом – не только на стационарных, но и на мобильных и даже подвижных объектах[1].

При этом *на всех* местах выработки должны защищаться *все* сигналы и *все* каналы передачи данных.

В подавляющем большинстве КИИ непременной частью системы защиты сетевого взаимодействия являются средства криптографической защиты

[1] Хотя необходимо признать, что и стационарные объекты могут ощутимо различаться – от центрального офиса до станции общественного транспорта или, скажем, маяка, но все же размещение мобильных (банкомат, инфокиоск), а особенно – подвижных объектов (поезд, автомобиль инкассации, скорая помощь, корабль) отличается еще большей непредсказуемостью.

информации (СКЗИ), поскольку, как уже упоминалось, некоторые объекты КИИ взаимодействуют по незащищенным сетям общего доступа, причем с использованием стандартных цифровых каналов типа WiFi, BlueTooth и LTE. Изменение порядка взаимодействия с построением выделенных защищенных каналов не всегда возможно в принципе, а когда и возможно – то влечет за собой весьма продолжительные и дорогостоящие работы, несопоставимые с внедрением СКЗИ[2]. Со стороны СКЗИ же, в свою очередь, предъявляются требования к среде функционирования криптографии (СФК), условиям хранения и применения ключей и т. п.

Отсюда недвусмысленно вытекает набор свойств, которыми должна характеризоваться платформа средства защиты сетевого взаимодействия между объектами КИИ:

1) возможность создавать и поддерживать доверенную вычислительную среду,

2) возможность работы с неизвлекаемым ключом в автоматическом режиме,

3) возможность установки различных СКЗИ при соблюдении условий сертификации на высокие классы,

4) возможность работы с различными каналами связи по различным протоколам, при необходимости – параллельно,

---

[2] Откровенно говоря, даже не смешно представить себе такую постановку задачи для стоящего «в чистом поле» банкомата.

5) возможность коммутации с различным оборудованием объекта КИИ без модификации последнего.

Отдельно необходимо остановиться на том, что все эти характеристики касаются именно аппаратной платформы, а не программной реализации на ней конкретного решения.

Не оставаясь на уровне аксиоматики (приоритет аппаратной реализации защитных функций давно не нуждается в доказательствах), приведем самые очевидные аргументы.

Фактически, в части защиты сетевого взаимодействия все специфичное в требованиях к КИИ сводится к тому, что

> при взаимодействии с использованием сетей общего доступа *каждый узел* должен быть защищен СКЗИ *высокого класса*.

Все остальное – следствия из этого обстоятельства.

Детали сертификационных требований приведены в справочном разделе в конце этой брошюры.

Некоторые следствия, вытекающие из необходимости защиты всех узлов сети рассмотрим на примере защиты банкоматов.

Для оборудования каждого узла СКЗИ, сертифицированным на высокий класс, неприемлемо

использовать установленный на технические средства программный VPN. Даже в случае, если для него создана и поддерживается СФК, это недопустимо потому, что при обслуживании в ПО этого компьютера могут быть внесены изменения, нарушающие СФК, а проведение в каждом случае соответствующих проверок – просто невозможно организационно. Более того, в случае с рядом специфических объектов КИИ вообще возможна ситуация, что непредсказуемые изменения – например, замена компьютера на свой, улучшенный – будут произведены, например, при работах вообще не с компьютером, а с какими-то другими техническими средствами объекта – например, с диспенсером банкомата: объекты КИИ зачастую обслуживаются большим количеством технического персонала, среди которого может скрываться злоумышленник.

Ситуация выглядит несколько лучше при использовании аппаратного шлюза, однако, использование импортных устройств неприемлемо по причине их несоответствия требованиям регуляторов, а отечественные сертифицированные устройства в этом качестве, как правило, не используются. Причины на это, в общем, объективные – цена и габариты.



Не то что бы их нельзя было установить в каждый банкомат, электричку, машину инкассации, скорую помощь и инфокиоск, но они дороги, избыточны по своим характеристикам, очень велики по размеру и зачастую подвержены множеству уже хорошо разработанных и постоянно появляющихся новых атак.

Еще одно требование регулятора к СКЗИ высокого класса – неизвлекамый ключ. Казалось бы, эта тема должна быть раскрыта в современных СКЗИ в полной мере, однако и здесь есть важные для применения в КИИ особенности.

«Неизвлекаемость» – свойство, описывающее связь ключа с некоторым его физическим хранилищем, то есть говоря о том, что ключ неизвлекаем, необходимо уточнять, *откуда*. Неизвлекаемые ключи как правило неизвлекаемы из токена, который, как правило – USB-устройство, смарт-карта или «таблетка» Touch Memory. Читая документы на СКЗИ высоких классов сертификации для защиты канала, мы видим, что «требование неизвлекаемости ключа выполняется применением токена…». Это добросовестное выполнение требования, однако, токен с неизвлекаемым ключом – это инструмент решения совсем другой задачи, существенно отличающейся от защиты сетевого взаимодействия объектов КИИ. Токен предназначен для того, чтобы ключ *пользователя* был *отчуждаем* от СВТ, на котором пользователь

осуществляет те или иные операции с ключом. В описываемом же случае отчуждаемость не только избыточна, но и вредна: с одной стороны, она делает возможными сценарии атак с подменой или иными вариантами компрометации ключа за счет отчуждаемости его носителя, а с другой, подключенное к порту USB-устройство резко снижает надежность решения – при вибрации, ударах, нагревании и прочих особенностях условий, в которых работают технические средства на объектах КИИ.

Модуль работы с неизвлекаемом ключом должен быть реализован как часть резидентного компонента безопасности, размещенного непосредственно на плате компьютера, а не как отчуждаемый персональный носитель ключа.

Задачи коммутации и использования широкого спектра каналов и протоколов связаны уже не с требованиями регуляторов, а с техническими особенностями объектов КИИ. необходимо поддержать множество различных интерфейсов, то есть тоже требуют аппаратных решений.

Всем этим требованиям отвечает специализированный компьютер с аппаратной защитой данных m-TrusT.

Его особенностями являются:

- Новая гарвардская архитектура, обеспечивающая вирусный иммунитет

- аппаратная поддержка реализации доверенной загрузки
- функциональная замкнутость среды
- аппаратное обеспечение целостности
- аппаратное резидентное решение по неизвлекаемости ключа
- аппаратный ДСЧ.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ПОЛЕЗНУЮ МОДЕЛЬ

№ 191690

СПЕЦИАЛИЗИРОВАННЫЙ КОМПЬЮТЕР С АППАРАТНОЙ ЗАЩИТОЙ ДАННЫХ

Патентообладатели: *Закрытое акционерное общество "Особое Конструкторское Бюро Систем Автоматизированного Проектирования" (RU), Пярин Виктор Анатольевич (RU), Общество с ограниченной ответственностью "Сангар" (RU)*

Авторы: *Батраков Антон Юрьевич (RU), Коняйский Валерий Аркадьевич (RU), Счастный Дмитрий Юрьевич (RU), Пярин Виктор Анатольевич (RU)*

Заявка № 2019115393

Приоритет полезной модели 20 мая 2019 г.

Дата государственной регистрации в Государственном реестре полезных моделей Российской Федерации 15 августа 2019 г.

Срок действия исключительного права на полезную модель истекает 20 мая 2029 г.

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Однако, кроме архитектурного решения, необходимо определить также форм-фактор и эксплуатационные требования, с соблюдением которых нужно изготовить компьютер.

Если во все уже функционирующие объекты КИИ внедрить средства защиты, которые будут обеспечивать:

1) криптографическую защиту ***всей*** передаваемой информации;

2) информационное взаимодействие ***всех*** объектов КИИ;

3) возможность использования ***разнообразных*** цифровых каналов (WiFi, BlueTooth, и др.);

4) информационное взаимодействие с ***разнообразной*** каналообразующей аппаратурой (RS232, RS435 и др.)

и все это – для ***всех*** типов технических средств, то при традиционном подходе это приведет к:

1) серьезной ***переработке проектных решений***;

2) ***модернизации*** исправного и еще не выработавшего свой ресурс оборудования;

3) ***восстановлению системы после сбоев***, вызванных модернизацией, которая может привести к частичному или полному нарушению функционирования системы.

Защита выльется в серьезные финансовые затраты.

Но вариантов исполнения требований 187-ФЗ несколько. Можно:

1) провести модернизацию объектов КИИ;

2) для каждого объекта КИИ разработать, изготовить и сертифицировать собственное множество аппаратных СКЗИ;

3) создать специальную аппаратуру, обладающую всеми необходимыми свойствами, и особенностью которой будет простейшая модернизация к любым объектам и каналам, не требующая проведения повторной сертификации.

Очевидно, что:

- первый вариант очень дорогой и длительный,
- второй – дорогой и очень длительный,

Причем в обоих случаях приведение системы в соответствие с требованиями закона и подзаконных актов тем дороже, чем выше разнообразие технических средств в системе.

- третий – полностью приемлем, если цена решения будет доступной.

Адаптация СЗИ к техническим средствам объектов КИИ позволит сохранить инвестиции в КИИ.

Однако адаптация СЗИ, а особенно – СКЗИ – это повторная сертификация. Замкнутый круг?

Нет, инженерная задача.

Решается задача путем декомпозиции: разделения СЗИ на то, что должно быть неизменным, чтобы не требовалось повторной сертификации, и то, что может меняться для того, чтобы интегрироваться с очередным техническим средством на очередном объекте КИИ.

Для разработки решения по лучшему варианту нужно выделить аппаратное ядро, а встраивание выполнять за счет создания несложных интерфейсных плат, обеспечивающих транспорт и необходимый форм-фактор, но не связанных с выполнением криптографических функций.

Ядро проектируется как универсальное, множество интерфейсных плат может быть огромно, форм-факторы разнообразны и зависят только от особенностей объектов КИИ.

Такое решение создано – это защищенная интеграционная платформа МК-И.

МК-И – это микрокомпьютер Новой гарвардской архитектуры m-TrusT и интерфейсная плата для его коммутации с сетевой инфраструктурой, которая может включать в себя самые разные типы оборудования. Поэтому интерфейсные платы делаются различными, а сам микрокомпьютер m-TrusT – универсальный, его форм-фактор не зависит от предполагаемого места установки.

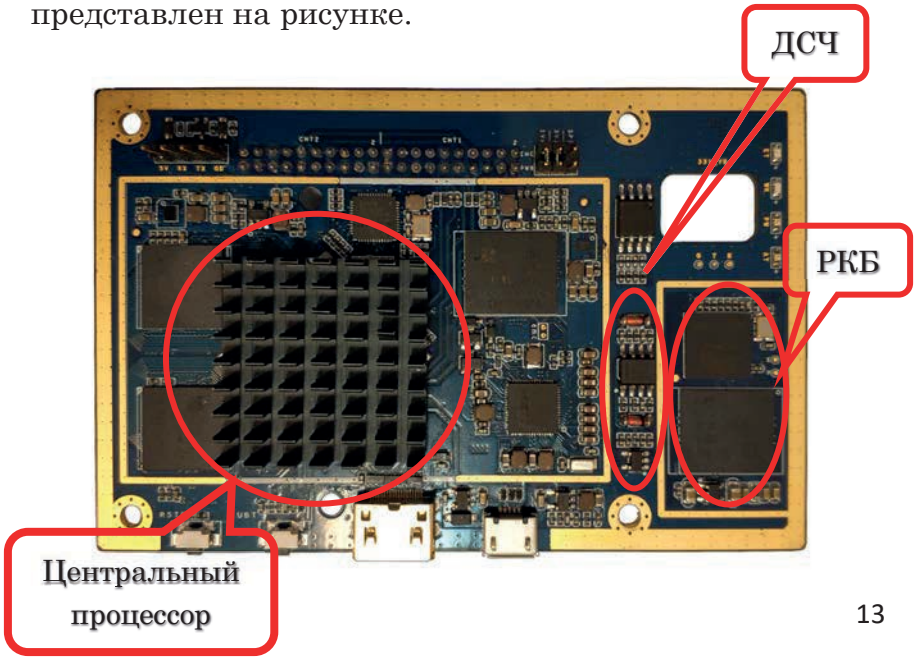
Важно это потому, что изменения интерфейсной части не влияют на вычислительную часть компьютера, а это снимает основные сложности, вызываемые адаптацией серийного продукта – возможное внесение новых ошибок или дефектов, необходимость повторных проверок или сертификации и т. п. Ядро универсально, а интерфейсные платы обеспечивают только транспорт.

Каждый микрокомпьютер «m-TrusT» является точкой сбора информационных и/или управляющих сигналов от объектов КИИ, их шифрования для передачи по каналам связи, а также приема зашифрованных сигналов из каналов связи и их расшифровкой.

Типовые характеристики микрокомпьютеров:

- Габаритные размеры: 65 х 80 мм;
- Процессор: Quad-core ARM Cortex-A17, up to 1.8 GHz;
- ОЗУ: 2 Гб DDR3;
- ПЗУ: 16 Гб NAND-flash;
- microUSB;
- microHDMI.

Общий вид микрокомпьютера m-TrusT представлен на рисунке.



Микрокомпьютер не подключается напрямую ни к чему, кроме собственной интерфейсной платы, поэтому его состав не сложен и постоянен. Интерфейсная плата же нужна как раз для того, чтобы корректно подключиться к тому или иному конкретному ПКО и каналообразующей аппаратуре различных типов.

Наличие собственной ОС и вычислительных ресурсов позволяет обеспечить достаточную для защиты сетевого взаимодействия производительность[3] и высокий уровень защищенности. Особенностями m-TrusT является наличие датчика случайных чисел и размещение ПО в памяти с физически устанавливаемым доступом read only (только чтение), что исключает вредоносное воздействие на ПО и обеспечивает неизменность среды функционирования средств криптографической защиты информации. Ресурсы m-TrusT позволяют обеспечить СФК, позволяющую сертифицировать вариант исполнения СКЗИ на m-TrusT на класс КС3. Помимо Новой гарвардской архитектуры защищенность платформы обеспечивается РКБ и СДЗ, сертифицированным ФСТЭК России.

Встроенное СКЗИ может быть любым сертифицированным[4].

---

[3] Возможна защищенная передача видеосигнала с камер без ощутимого снижения качества изображения.

[4] Например, в решении «fin-TrusT» для защиты сетевого взаимодействия в финансовой организации встроенное СКЗИ – DCrypt от компании ТСС.

Итак, коммутировать микрокомпьютер m-TrusT в «разрыв» между ПКО различного назначения и каналом связи позволяет интерфейсная плата. Как уже упоминалось – разнообразие оборудования, взаимодействующего по сети (ПК, скорая помощь, банкомат, электричка, информационный киоск, машина инкассации, терминал оплаты etc), является ключевой характеристикой инфраструктуры, поэтому интерфейсные платы должны быть ***разными***, чтобы коммутировать ***одно и то же*** СЗИ (то есть не *совместимые*, не *похожие*, а именно *одинаковые* СЗИ) с разными ПКО. Например, она может быть такой, как на рисунке:

- Габаритные размеры: 90 х 105 мм;
- Соединитель типа Розетка 87758-2016 MOLEX;
- Разъем USB Type A;
- Разъем Ethernet;
- Разъем питания от источника постоянного напряжения 5 вольт.

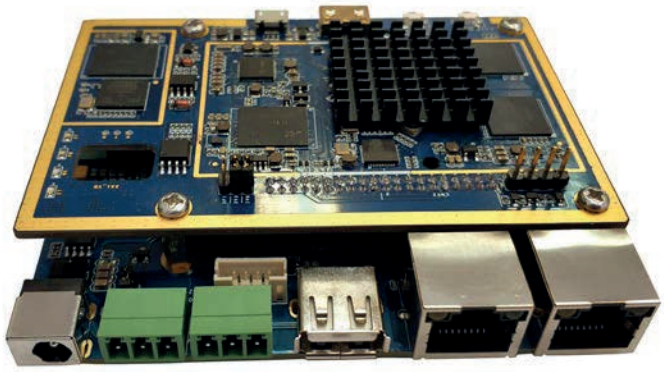
Интерфейсная плата №2

- Габаритные размеры 90 х 110 мм;
- Соединитель типа Розетка 87758-2016 MOLEX;
- USB-хаб;
- Разъем USB Type A;
- 2 разъема Ethernet ;
- Разъем RS-232, подключенный через преобразователь USB-RS-232;

• Разъем RS-485, подключенный через преобразователь USB-RS-485;

• Разъем для micro-SD карты;

• Разъем питания от источника постоянного напряжения 5 вольт.



На следующем рисунке показан другой вариант интерфейсной платы с меньшим количеством интерфейсных разъемов:

• Габаритные размеры: 90 х 105 мм

• Соединитель типа Розетка 87758-2016 MOLEX

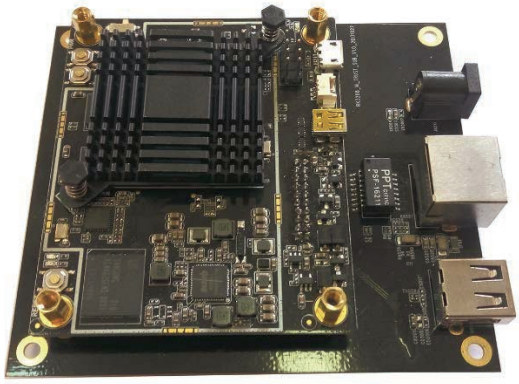
• Разъем USB Type A

• Разъем Ethernet

• Разъем питания от источника постоянного напряжения 5 вольт.

Возможна разработка интерфейсных плат для других типов разъемов. С учетом уже имеющегося опыта внедрения на транспорте и кредитно-финансовой сфере, мы уверенно говорим о том, что эта

задача решается с положительным результатом в разумные сроки.

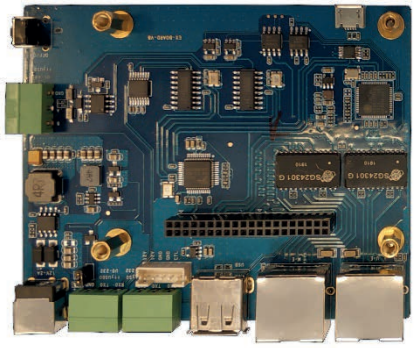


Для некоторых объектов, как показала практика, удобным может быть исполнение в едином корпусе, например, если частого переоборудования не требуется, а техническое средство функционирует вне помещения, где внешние условия могут быть разнообразными и не всегда благоприятными. В этом случае корпус снижает возможное воздействие внешних условий.

Разумеется, за счет описанных особенностей МК-И, построенное на нем решение может поддержать любой из вариантов связи объектов, или даже все их одновременно, причем с дублированием каждого канала (несколько каналов Ethernet, несколько sim-карт для мобильного Интернета и т. д.), с тем чтобы во время работы использовать тот, что доступен в данный момент и в данном месте.

Такое средство защиты универсально – на все технические средства всех объектов системы

внедряется одно и то же СЗИ без внесения каких-либо изменений в само защищаемое оборудование. Эта универсальность обеспечивается интерфейсными платами.



Еще раз подчеркнем, что такая платформа *уже создана*, запатентована[5], решения, построенные на ней сертифицированы, внедряются и применяются в реальных функционирующих КИИ. Ее преимущества – кроме сертифицированных ФСТЭК и ФСБ России встроенных средств защиты и «вирусного иммунитета» – достаточная производительность при низкой цене.

[5] Описание полезной модели к патенту Вы можете увидеть в конце этой брошюры.

ОСНОВНЫЕ ОСОБЕННОСТИ, ОБЕСПЕЧИВАЮЩИЕ ЗАЩИЩЕННОСТЬ РЕШЕНИЯ

Самое главное свойство платформы – полная доверенная загрузка, то есть доверенная загрузка не только ОС, но и начальная загрузка устройства полностью контролируемая, с пошаговым обеспечением целостности, позволяющим поддерживать среда функционирования криптографии.

Процессор устройства сконфигурирован таким образом, чтобы старт загрузки всегда производился из памяти, аппаратно защищенной от перезаписи (физически переведенной в режим read only). Из этой памяти стартует загрузчик, который проверяет целостность модуля, который, стартовав, производит настройку СДЗ. Последний в свою очередь контролирует старт ОС. Эта схема обеспечивает пошаговый контроль загрузки, который позволяет сделать старт микрокомпьютера доверенным на всем его протяжении.

Доверенная загрузка поддерживается программным комплексом Аккорд-МКТ, сертифицированным ФСТЭК.

Функциональная замкнутость среды поддерживается комплексом Аккорд-Х, сертифицированным ФСТЭК.

СИСТЕМА СЕРТИФИ
СРЕДСТВ ЗАЩИТЫ ИНФ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНО
№ РОСС RU.0001.0

СЕРТИФИКАТ СООТВЕ
№ 3936

Выдан 10 мая 2018 г.
Действителен до 10 мая 2021 г.

Настоящий сертификат удостоверяет, что модуль д
МКТ», разработанный и производимый ЗАО «ОКБ САПР»
условиями ТУ 501410-071-37222406-2016, является програ
загрузки, соответствует требованиям документов «Требо
загрузки» (ФСТЭК России, 2013) и «Профиль защиты средс
базовой системы ввода-вывода четвертого класса защиты. ИТ
2013) при выполнении указаний по эксплуатации,
37222406.501410.071 ФО.

Сертификат выдан на основании результатов с
проведенных испытательной лабораторией ООО «ЦБИ» (аттес
№ СЗИ RU.0001.01БИ00.Б004) - техническое заключени
заключения от 04.04.2018 органа по сертификации ФАУ «Г
(аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А

Заявитель: ЗАО «ОКБ САПР» (ИНН 7725739137)
Адрес: 117525, г. Москва, ул. Автозаводская, д. 1
Телефон: (499) 235-6265

Контроль маркирования знаками соответствия с
и инспекционный контроль её соответствия требованиям доку
сертификате, осуществляется испытательной лабораторией ОО

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭ

Настоящий сертификат внесен в Государственный реестр сертифицирова
18 мая 2018 г.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3079

Выдан 30 января 2014 г.
Действителен до 30 января 2017 г.
Срок действия продлен до 30 января 2020 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс средств защиты информации** от несанкционированного доступа «Аккорд-Х», разработанный и производимый ЗАО «ОКБ САПР» в соответствии с техническими условиями ТУ 4012-026-11443195-2008, функционирующий в средах операционных систем, указанных в формуляре 11443195.4012.026-ФО, является программно-техническим средством защиты информации от несанкционированного доступа, реализующим функции идентификации и аутентификации, управления доступом, очистки памяти, регистрации событий безопасности, контроля целостности, соответствует требованиям руководящих документов «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 2 уровню контроля, «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 3 классу защищенности и технических условий при выполнении ограничений по применению, указанных в формуляре.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Центр безопасности информации», (аттестат аккредитации от 30.03.2006 № СЗИ RU.117.Е08.025) – техническое заключение от 13.12.2013, и экспертного заключения от 27.12.2013 органа по сертификации ЗАО «Лаборатория ППШ» (аттестат аккредитации от 29.09.2007 № СЗИ RU.054.А97.010) и результатов инспекционного контроля, проведенного испытательной лабораторией ООО «Центр безопасности информации» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001) - техническое заключение от 28.02.2017.

Заявитель: ЗАО «Особое Конструкторское Бюро Систем Автоматизированного Проектирования» (ИНН 7725739137)
Адрес: 115280, г. Москва, ул. Автозаводская, д.1
Телефон: (499) 235-6265

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящих документов и технических условий, указанных в настоящем сертификате, осуществляется испытательной лабораторией ООО «Центр безопасности информации».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

А.Куц

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
30 января 2014 г.

А также:

- физический датчик случайных чисел – двухплечевое решение с использованием диодов 2Г103А9, по схеме «Дебют», имеет положительное заключение ФСБ;

- криптографическое API поддержки аппаратного неизвлекаемого ключа платформы m-TrusT имеет положительное заключение ФСБ;

- специализированный компьютер с аппаратной защитой данных m-TrusT сертифицирован ФСБ как платформа для СКЗИ DCrypt на класс КС3.

Как любой универсальный защищенный компьютер, m-TrusT может использоваться для реализации всех технических мер обеспечения безопасности значимых объектов КИИ, включая ИАФ, УПД, ОПС, ЗНИ, АУД, АВЗ, СОВ, ОЦЛ, ОДТ, ОПО. Наиболее же эффективно использовать m-TrusT для обеспечения группы мер ЗИС.

При использовании m-TrusT в составе ИС важно соответствие требованиям регулятора его собственных свойств. Этому посвящена таблица 2. В таблице 3 же приведены те меры, которые обеспечиваются с помощью m-TrusT в системах КИИ.

Таблица 2. Соответствие m-TrusT техническим мерам Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных приказом ФСТЭК России от 25 декабря 2017 г. № 239

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Соответствие m-TrusT требованиям ФСТЭК	Примечание
I. Идентификация и аутентификация (ИАФ)			Меры ИАФ.0. ИАФ.3, ИАФ.4 являются организационными. Мера ИАФ.6 – необязательная.
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	
ИАФ.2	Идентификация и аутентификация устройств	+	

ИАФ.5	Идентификация и аутентификация внешних пользователей	+	
ИАФ.7	Защита аутентификационной информации при передаче	+	
II. Управление доступом (УПД)			Меры УПД.0, УПД.4, УПД.5 являются организационными. Меры УПД.7, УПД.8, УПД.12 – необязательные.
УПД.1	Управление учетными записями пользователей	*	Не имеет пользователей т. к. обычно работает в автоматическом режиме
УПД.2	Реализация модели управления доступом	*	Управление доступом осуществляется ключевой системой
УПД.3	Доверенная загрузка	+	
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	
УПД.9	Ограничение числа параллельных сеансов доступа	*	Ограничивается ключевой системой

УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	
УПД.13	Реализация защищенного удаленного доступа	+	Защита удаленного доступа обеспечивается СКЗИ
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	
III. Ограничение программной среды (ОПС)			Меры ОПС.0 и ОПС.2 являются организационными. Мера ОПС.3 – необязательная.
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+	

IV. Защита машинных носителей информации (ЗНИ)			Меры ЗНИ.0 - ЗНИ.2 являются организационными. Меры ЗНИ.3 и ЗНИ.4 – необязательные.
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	**	Отсутствует возможность подключения съемных машинных носителей информации. В системе обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.6	Контроль ввода (вывода) информации на съемные машинные носители информации	**	Отсутствует возможность подключения съемных машинных носителей информации. Обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.7	Контроль подключения съемных машинных носителей информации	**	Отсутствует возможность подключения съемных машинных носителей информации. Обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	-	

V. Аудит безопасности (АУД)			Меры АУД.0 – АУД.2, АУД.10 и АУД.11 являются организационными.
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	Обеспечивается собственной системой времени
АУД.4	Регистрация событий безопасности	+	
АУД.5	Контроль и анализ сетевого трафика	-	
АУД.6	Защита информации о событиях безопасности	+	
АУД.7	Мониторинг безопасности	+	
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	
АУД.9	Анализ действий отдельных пользователей	-	

VI. Антивирусная защита (АВЗ)			Меры АВЗ.0 и АВЗ.5 являются организационными.
АВЗ.1	Реализация антивирусной защиты	+	
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	-	Электронная почта и внешние сервисы не используются
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов	-	
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	-	Не требуется
VII. Предотвращение вторжений (компьютерных атак) (СОВ)			Мера СОВ.0 является организационной.
СОВ.1	Обнаружение и предотвращение компьютерных атак	**	Обеспечивается внешними средствами СОВ

СОВ.2	Обновление базы решающих правил	**	Обеспечивается внешними средствами СОВ
VIII. Обеспечение целостности (ОЦЛ)			Мера ОЦЛ.0 является организационной. Меры ОЦЛ.2 и ЗНИ.6 – необязательные.
ОЦЛ.1	Контроль целостности программного обеспечения	+	
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему	+	
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	+	
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	+	

IX. Обеспечение доступности (ОДТ)			Меры ОТД.0 – ОТД.2 являются организационными. Мера ОТД.7 – необязательная.
ОДТ.4	Резервное копирование информации	**	В соответствии с политикой информационной безопасности
ОДТ.5	Обеспечение возможности восстановления информации	**	В соответствии с политикой информационной безопасности
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	Обеспечивается архитектурой
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	-	

X. Защита технических средств и систем (ЗТС)			Меры ЗТС.0, ЗТС.2 – ЗТС.5 являются организационными. Меры ЗТС.1 и ЗТС.6 – необязательные.
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			Меры ЗИС.0 – ЗИС.5, ЗИС.8 являются организационными. Меры ЗИС.7, ЗИС.9 – ЗИС.12, ЗИС14, ЗИС.15, ЗИС.17, ЗИС.18, ЗИС.22 – ЗИС.26, ЗИС.28 – ЗИС.31, ЗИС.36, ЗИС.37 – необязательные.
ЗИС.6	Управление сетевыми потоками	+	Обеспечивается ключевой системой
ЗИС.13	Защита неизменяемых данных	+	
ЗИС.16	Защита от спама	+	
ЗИС.19	Защита информации при ее передаче по каналам связи	+	
ЗИС.20	Обеспечение доверенных канала, маршрута	+	
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+	

ЗИС.27	Обеспечение подлинности сетевых соединений	+	
ЗИС.32	Защита беспроводных соединений	+	
ЗИС.33	Исключение доступа через общие ресурсы	+	
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+	
ЗИС.35	Управление сетевыми соединениями	+	
ЗИС.38	Защита информации при использовании мобильных устройств	+	
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	-	

XII. Реагирование на компьютерные инциденты (ИНЦ)			Все меры этой группы – организационные.
XIII. Управление конфигурацией (УКФ)			Все меры этой группы – организационные.
XIV. Управление обновлениями программного обеспечения (ОПО)			Меры ОПО.0, ОПО.1 и ОПО.3 являются организационными.
ОПО.2	Контроль целостности обновлений программного обеспечения	+	
ОПО.4	Установка обновлений программного обеспечения	+	
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)			Все меры этой группы – организационные.
XVI. Обеспечение действий в нештатных ситуациях (ДНС)			Все меры этой группы – организационные.
XVII. Информирование и обучение персонала (ИПО)			Все меры этой группы – организационные.

* - при использовании в ИС без СКЗИ мера осуществляется установкой СПО СЗИ

** - при использовании в ИС при установке СПО СЗИ

Таблица 3. Применение m-TrusT для защиты значимых объектов КИИ

Обозначение и номер меры	Меры обеспечения безопасности
ЗИС.19	Защита информации при ее передаче по каналам связи
ЗИС.20	Обеспечение доверенных канала, маршрута
ЗИС.27	Обеспечение подлинности сетевых соединений
ЗИС.32	Защита беспроводных соединений
ЗИС.33	Исключение доступа через общие ресурсы
ЗИС.35	Управление сетевыми соединениями

При этом m-TrusT обеспечивает существенные преимущества, в том числе:

1. Работа в автоматическом режиме, что существенно снижает нагрузку на организационно-технические меры при эксплуатации СКЗИ

2. Изменение форм-фактора без повторной сертификации изделия, что значительно сокращает сроки работ по защите КИИ

3. Обеспечивается работа с любыми каналами связи, используемыми в КИИ

4. Обеспечивается защита КИИ без глубокой переработки ее структуры, что сильно сокращает затраты на проведение мероприятий.

ОСОБЫЕ ВАРИАНТЫ

Немало уже написано о том, что встраиваемость в разнообразные технические средства различных объектов разных КИИ обеспечивается интерфейсными платами. Разработка интерфейсной платы под конкретное оборудование не занимает много времени и не влияет на защитные свойства и функции платформы.

В то же время не на всех объектах КИИ это требуется – некоторые из них могут быть офисными или серверными объектами, в таких случаях гораздо уместнее и соответствующее исполнение платформы для СЗИ. Для таких объектов платформа изготавливается для размещения в стойку или на столе.

Именно поэтому мы утверждаем, что m-TrusT – универсальное решение. Использование в качестве платформы для средства защиты сетевого

взаимодействия в КИИ специализированного компьютера с аппаратной защитой данных m-TrusT позволяет учитывать все особенности оборудования объектов КИИ и без затрат на перепроектирование и восстановление от сопутствующих сбоев, в кратчайшие сроки выполнить требования 187-ФЗ, сохранив при этом существующую структуру и логику функционирования.

Адаптация СЗИ к системе и к ее конкретному объекту – это не задача эксплуатирующей организации, это задача производителя СЗИ. И она решена.

ОСОБЫЕ УСЛОВИЯ ФУНКЦИОНИРОВАНИЯ

Для систем класса АСУТП и КИИ особое значение имеют климатические условия. Специализированные компьютеры m-TrusT могут изготавливаться для категорий C (castom), I (industrial), M (military). Стандартное решение – I.

П Р О Т О К О Л
климатических испытаний модуля m-TrusT на базе RK3399

Место испытаний: НИИАС, г. Москва, Нижегородская ул., 27, стр. 1
Стенд для испытаний: Климатическая испытательная камера Tabai MC-81. Оборудование имеет поверку до 12.2019 г.
Оборудование для испытаний:

1. МПУЛ-И с установленным m-TrusT RK3399 (далее МПУЛ)
2. Док-станция с установленным m-TrusT RK3399 (далее док-станция)

Техническими условиями на МПУЛ-И установлены температурные границы от -20° до +50°.

Методика испытаний:

1. Охлаждение выключенного оборудования до -30°. Включение, проверка работоспособности.
2. Охлаждение выключенного оборудования до -40°. Включение, проверка работоспособности.
3. Нагрев включенного оборудования до +50°. Выключение, включение, проверка работоспособности.
4. Нагрев включенного оборудования до +60°. Выключение, включение, проверка работоспособности.

Температура считывается программно с двух датчиков на m-TrusT, температура среды определяется по датчику климатической камеры.

Результаты испытаний:

1. Охлаждение, удерживание температуры -30° в течении 1 часа, включение оборудования, температура на датчиках после включения МПУЛ -18°, док-станция -27°. После включения оборудование работало в штатном режиме.
2. Охлаждение, удерживание температуры -40° в течении 30 минут, включение оборудования, температура на датчиках после включения МПУЛ -30°, док-станция -38°. После включения оборудование работало в штатном режиме.
3. Нагрев оборудования до +50° и удерживание в течении 1 часа. Выключение-включение оборудования, температура МПУЛ +75°, док-станция +54°. После включения оборудование работало в штатном режиме.
4. Загрузка процессора m-TrusT на 100% в течении 5 минут при температуре +50°. Выключение-включение оборудования, температура МПУЛ 85°, док-станция 66°. После включения оборудование работало в штатном режиме.
5. Нагрев оборудования до +60 и удерживание в течении 1 часа. Выключение-включение оборудования, температура МПУЛ +92°, док-станция +66°. После включения оборудование работало в штатном режиме.
6. Загрузка процессора m-TrusT на 100% в течении 5 минут при температуре +60°. Выключение-включение оборудования, температура МПУЛ +100°, док-станция 76°. После включения оборудование работало в штатном режиме.

РЕШЕНИЯ НА БАЗЕ M-TRUST

Архитектура платформы с интерфейсной платой обуславливает возможность построения на базе специализированного компьютера с аппаратной защитой данных m-TrusT широкого спектра инфраструктурных решений.

Безопасный город

Нас окружают камеры, данные с которых оказывают непосредственное влияние на принятие множества критически важных или просто значимых для конкретных граждан решений. Изображение с этих камер передается по каналам передачи данных общего пользования, вмешательство в этот процесс «человека посередине» не представляет для злоумышленника сложности.

Такая атака дает злоумышленнику возможность подменять данные на те, что позволят ему решить какие-то свои задачи, либо, что не менее опасно, особенно в условиях движения к биометрической идентификации, – накапливать данные о гражданах в целях дальнейшего использования в собственных целях.

Встраивание в камеры СКЗИ на платформе m-TrusT сделает процесс сбора данных с камер защищенным с максимально возможным сохранением инвестиций. Стоимость оборудования камер СКЗИ

будет ощутимо ниже замены всех камер на такие, в которые по умолчанию встроены средства шифрования аналогичного класса защиты. «Безопасный» город становится безопасным.

Умный дом

Умный дом сейчас едва ли не в большей степени ассоциируется с опасностью, чем с прогрессом. Приборы, взаимодействующие по сети в лучшем случае разовьют искусственный интеллект и взбунтуются (это оптимистический сценарий, потому что случится это очень нескоро), а в худшем – попадут под управление не собственного хозяина, а его недоброжелателя. Можно рисовать много сценариев развития этой ситуации – как смешных, так и страшных. Оставив эту задачу сценаристам, можно решить проблему радикально – защитить взаимодействие вещей, поскольку от него зависят люди.

При этом сценарии m-TrusT со специализированной платой расширения становится концентратором потоков информационного взаимодействия в системах IoT (так называемого «Интернета вещей»). Преступник больше не сможет отключить ваш холодильник и включить кипяток в душе. Умный дом становится безопасным.

Надежный банк

Криптошлюз для защиты сетевого взаимодействия технических средств финансовой организации fin-TrusT уже упоминался выше. С помощью криптошлюзов fin-TrusT защищаются коммуникации между подразделениями и офисами банков, банком и процессинговым центром, процессинговым центром и банкоматами. Выполняются требования законодательства, блокируются уязвимости во взаимодействии в финансовой сфере.

Если рассматривать в качестве примера объекта КИИ банкомат, то там сегодня все устроено на первый взгляд довольно просто. В его составе есть диспенсер (в нем лежат деньги и из него деньги выдаются), компьютер и периферийное оборудование. Компьютер взаимодействует с процессинговым центром (например, по IP-протоколу), и USB-кабелями соединен с диспенсером и другим периферийным оборудованием.

При работе с банкоматом с пластиковой карты считывается ее номер, с клавиатуры – PIN, все это передается в процессинговый центр, где и выполняется авторизация. Если все в порядке – проверяется запрашиваемая сумма. Затем компьютером банкомата формируется команда на выдачу денег, которая передается в диспенсер. Из защитных механизмов здесь используется только один – диспенсер размещен в сейфе.

Такого очень упрощенного описания уже достаточно, чтобы понять «Что делать?». Надо защитить каналы – как от процессингового центра к компьютеру, так и от компьютера к диспенсеру, и обеспечить целостность программно-аппаратной среды компьютера. Сделать это в соответствии с 187-ФЗ, нетравматично для функционирования системы и с сохранением инвестиций можно именно с помощью решения fin-TrusT на платформе специализированного компьютера с аппаратной защитой данных m-TrusT.

Финансовые коммуникации становятся безопасными.

Безопасный транспорт

Представим себе железную дорогу как некоторый обобщенный эталонный макет транспорта вообще.

Если рассматривать ее с точки зрения сетевого взаимодействия объектов КИИ (это лишь одно из большого числа крайне интересных проявлений этого феномена, однако именно ему посвящена эта брошюра), то мы увидим три глобальных типа объектов: подвижные составы, станционное оборудование и некоторый центральный вычислительный центр (ведь мы рассматриваем условную модель, а не конкретную КИИ).

Основное взаимодействие происходит между подвижными составами и центральным

вычислительным центром (назовем его ЦВЦ). Он рассылает расписание, аккумулирует данные от подвижных составов и рассылает сделанные на основании этих данных корректировки. Станционное оборудование также отправляет в ЦВЦ данные о движении подвижных составов и получает корректировки расписания, которые передает подвижным составам, а также выполняет различные вспомогательные функции, прописывать которые на уровне такой контурной обрисовки условной транспортной системы нет смысла. Подвижные составы также параллельно взаимодействуют со станционным оборудованием и с ЦВЦ, отправляя данные о своем движении и получая указания и корректировки. Очевидно, что нарушения этого взаимодействия может иметь крайне неприятные последствия, и так же очевидно, что средства защиты этого взаимодействия должны быть унифицированы, но в то же время адаптированы к работе в совершенно разных условиях. Бортовой компьютер подвижного состава работает в условиях вибрации и нагревания, и в целом он абсолютно не похож на ПК или сервер. На станциях оборудование представляет собой стойку серверов, ЦВЦ – это ЦОД с серверами огромной производительности. То есть это задача для платформы m-TrusT. Реализация СКЗИ на m-TrusT, с одной стороны, не имеет никаких ограничений по работе «навстречу» с реализациями этого же СКЗИ на любых других

платформах, а с другой – позволяет организовать защищенное взаимодействие параллельно по разным каналам. Транспорт становится безопасным.

Умная энергетика

Объекты энергетики рассмотрим на примере электрических подстанций. Это объекты, предназначенные для приема, преобразования и распределения электричества. Многие из них расположены «в чистом поле» – на открытых пространствах, вдалеке от какой-либо инфраструктуры, и функционируют относительно автономно.

Такие объекты неизбежно вызывают повышенный интерес злоумышленников, о чем писал еще А. П. Чехов[6]. Подключение к подстанции с целью решения каких-то бытовых задач, предельно опасна, так как объект не имеет ресурсов, позволяющих различать легальные и нелегальные запросы. Негативный эффект от таких действий не исчерпывается бесконтрольным потреблением электроэнергии. Цифровые подстанции, имеющие в составе управляющего комплекса противоаварийную систему, могут расценить изменение нагрузки как аварию и включить противоаварийную автоматику – в этом

[6] Чехов А. П. Злоумышленник // Полное собрание сочинений и писем в 30-ти томах. Сочинения. Том 4. М., «Наука», 1984.

случае целевые функции подстанции могут быть не выполнены в нужный момент, а к чему конкретно это приведет – зависит от того, в рамках какой инфраструктуры и для чего предназначена данная конкретная электроустановка.

Средство защиты, которое позволит отличать аутентифицированный и гарантированно неизмененный управляющий сигнал от воздействия «народных умельцев», позволит избежать этих негативных событий. Оно может быть построено на платформе m-TrusT. Для этого разработана специальная интерфейсная плата, позволяющая устанавливать м-траст в корпусе под DIN-рейку.

Умное производство

Сетевое взаимодействие технических средств объектов на производстве (классическое АСУТП) характеризуется рядом важных особенностей:

- основной защищаемой информацией является технологическая (обеспечивающая управление технологическими или чувствительно важными процессами), программно-техническая (программы системного и прикладного характера, обеспечивающие функционирование системы), командная (управляющая) и измерительная информация;

- предъявляются жесткие требования к времени и порядку выполнения автоматизированных функций;

- во взаимодействие включены разнородные, территориально и пространственно распределенные элементы, в которых реализуются разнообразные информационные технологии, это взаимодействие предельно далеко от документооборота на офисных ПК;

- крайне нежелательны отключения систем для проведения мероприятий по обеспечению безопасности информации;

- крайне опасны последствия вывода из строя и (или) нарушения функционирования системы (и здесь уже речь идет об опасности для жизни и здоровья, а не просто ущерб каким-либо интересам большого числа граждан).

Большая часть этих особенностей определяет по существу лишь одно требование общего характера к используемым СЗИ – они должны создаваться с повышенным вниманием к качеству на всех этапах – от проектирования для производства. Как правило, гарантия особенно высокого качества связана с более высокой ценой продукта, а значит, данный сегмент должен быть крайне привлекательным для производителя, что, в свою очередь, обеспечит конкуренцию, та повысит общий уровень качества и т. д.

Однако, иметь в своей продуктовой линейке варианты исполнения СЗИ с огромным разнообразием интерфейсов, в том числе довольно экзотических, производителю сложно и не выгодно, ведь

многотысячные продажи делают стандартные интерфейсы, свойственные офисным компьютерам. Аналогично обстоит дело с форматами данных, с файловыми системами, с поддержкой подключаемого оборудования. Поэтому эксплуатирующая или подрядная организация при создании проекта подсистемы защиты информации вынуждена использовать то, что есть, и за ту цену, которую назначит подчас единственных поставщик, а не то, что соответствует высоким требованиям к качеству, надежности и живучести.

Однако и это еще не все. Особенность многих производств сегодня состоит еще в одном очень существенном обстоятельстве: их управляющие инфраструктурные элементы находятся за рубежом. А это означает, что при неблагоприятных внешнеполитических обстоятельствах эти элементы могут стать рычагами управления не только производственными процессами. Система безопасности таких объектов должна строится в предположении, что центр управления может перестать быть доверенным источником, и его команды должны интеллектуально обрабатываться, а не просто без искажений передаваться на исполнение.

На платформе специализированного компьютера с аппаратной защитой данных m-TrusT можно построить такую систему.

Умный учет

Приборы учета всегда представляли собой цель для «улучшений» как со стороны недобросовестных пользователей учитываемых ресурсов, так и со стороны недобросовестных взимателей платы за эти ресурсы. Самого разного рода «скручивания» и «накручивания» самого разного рода счетчиков возникло, вероятно, одновременно с самими счетчиками. Каждый, то брал в аренду автомобиль, который надо вернуть «с тем же количеством топлива», наверняка замечал, что датчик топлива ведет себя удивительно, а Интернет полнится советами по обходу любых счетчиков – от воды до трафика.

«Умные» приборы учета имеют два существенных отличия:

1) ими можно управлять удаленно, без непосредственного «личного» контакта с каждым, и

2) они несут в себе функциональность не только непосредственно учета, но и управления.

Это совершенно логично – закончился лимит, превышена просрочка по оплате, или наступило еще какое-то заранее назначенное граничным событие – и в установленном порядке отключается подача того, использование чего считает «умный» счетчик. Никакого произвола или человеческого фактора.

За исключением того, что подать эту команду может хакер. А учитывая природу учитываемых

ресурсов, трудно преувеличить общественную значимость ситуации, которую сможет создать злоумышленник, буде в его планах резкое повышение уровня социальной напряженности.

Сделать «умный» учет безопасным можно за счет использования решений на платформе m-TrusT.

Защищенный бизнес

В защите нуждаются не только КИИ. Потребность в защите собственной информационной инфраструктуры, даже если она не является критической с точки зрения государства, все более осознана бизнесом – и уже не только крупным. И для таких информационных систем особенно важным становится баланс цены и качества. Создавая систему защиты «для себя», одинаково неверно переплачивать за правильное название (с какой бы точки зрения «правильным» оно ни было бы) и избыточную функциональность, ни покупать за небольшие деньги ненадежную защиту.

Криптомаршрутизаторы объектового уровня на платформе m-TrusT могут стать как раз тем решением, которое необходимо бизнесу – одного устройства будет достаточно на небольшой офис, оно не займет места, не требует специальных условий размещения и работает прозрачно для пользователей.

ПАТЕНТНОЕ ОПИСАНИЕ

СПЕЦИАЛИЗИРОВАННЫЙ КОМПЬЮТЕР С АППАРАТНОЙ ЗАЩИТОЙ ДАННЫХ

Реферат:

Компьютер содержит недоступный извне механический коммутатор, устанавливающий для запоминающего устройства, хранящего критичные данные, режим Read Only. Задача полезной модели – повышение уровня защищенности со снижением нагрузки на организационно-технические мероприятия – решена тем, что он содержит блок неизвлекаемого ключа, содержащий, в свою очередь, физический датчик случайных чисел (ФДСЧ) и микроконтроллер с внутренней памятью, запрограммированный на исполнение процедур генерации неизвлекаемого ключа подписи на основе случайной последовательности байт, полученных с ФДСЧ, его записи во внутреннюю память, вычисление ключа проверки подписи, соответствующего неизвлекаемому ключу, выработки сессионного ключа на основе случайной последовательности байт, полученных с ФДСЧ, выработки ключа защиты ключей на основании ранее выработанных неизвлекаемого ключа подписи и ключа ее проверки, зашифровывания на данном ключе сессионного ключа, а также последующее расшифровывание сессионного ключа на ключе

защиты ключей, выработанном, в свою очередь, на основе неизвлекаемого ключа подписи и ключа ее проверки.

Полезная модель относится к области компьютерной техники и информационных технологий и может быть использована там, где требуются защищенные компьютерные средства ограниченной функциональности, поддерживающие заданные криптографические процедуры, в особенности, электронной подписи (ЭП) – например, в качестве бортовых компьютеров сетей оперативно-технологической связи железнодорожного транспорта.

Можно считать доказанным, что в подобных случаях целесообразно применять компьютеры с аппаратной защитой данных, которая обеспечивает более высокий уровень защищенности – в отличие от программной защиты – по отношению к хакерским атакам. Подобные компьютеры содержат, по меньшей мере, один элемент электрической схемы, управляющий доступом в режиме записи к перепрограммируемому запоминающему устройству, хранящему критичные данные – в частности, специализированную операционную систему [1]. Наиболее близким к полезной модели является компьютер, в котором упомянутый элемент представляет собой недоступный извне

механический коммутатор, устанавливающий для запоминающего устройства, хранящего критичные данные, режим RO (Read Only) [2].

Однако поддержание компьютером криптографических процедур, стандартизованных для подобных применений, требует правильной (т. е. корректной и в то же время простой) организации работы с ключевыми данными – а этот вопрос для известных компьютеров с аппаратной защитой данных до настоящего времени так и не нашел удовлетворительного решения. В частности, в вышеуказанном примере задача работы с ключами шифрования возлагалась бы на машиниста локомотива, в обязанности которого входило бы их периодическое обновление путем подключения к каналам ввода-вывода бортового компьютера съемного носителя ключевой информации. Это повысило бы нагрузку на организационно-технические мероприятия на железнодорожном транспорте и снизило бы уровень защищенности, поскольку эти ключи должны быть генерированы где-то извне, съемный носитель с ними вручен машинисту, который – естественно – должен быть соответствующим образом подготовлен к выполнению таких специальных работ, затем машинист должен доставить носитель до локомотива, и, наконец, произвести процедуру обновления. Не говоря об усложнении учетных и

контрольных операций, на каждый отрезок этой цепочки оказывает негативное влияние человеческий фактор, что является недостатком компьютера, требующего такого порядка работы с ключами.

С другой стороны, в последние годы для криптографических токенов и чипов смарт-карт был предложен и успешно реализован принцип неизвлекаемости ключей, состоящий в том, что ключ шифрования и/или ключ подписи никогда не покидает пределов чипа, внутри которого он был сгенерирован. Это позволяет исключить экспорт ключей, поскольку все внешние функции (запрос на сертификат, проверка ЭП и т.п.) можно исполнить при помощи ключей проверки подписи (открытых ключей) [3].

Задачей полезной модели является повышение уровня защищенности, обеспечиваемого компьютером, и снижение нагрузки на организационно-технические мероприятия. Техническим результатом является получение более простого в эксплуатации и лучше защищенного компьютера.

Указанный результат достигнут раскрываемой ниже аппаратной реализацией принципа неизвлекаемости ключей шифрования, адаптированной к специализированному компьютеру с аппаратной защитой данных.

А именно, в специализированном компьютере с аппаратной защитой данных, содержащем недоступный извне механический коммутатор, устанавливающий для запоминающего устройства, хранящего критичные данные, режим RO, новым является то, что он дополнительно содержит блок неизвлекаемого ключа, содержащий, в свою очередь, физический датчик случайных чисел (ФДСЧ) и микроконтроллер с внутренней памятью, запрограммированный на исполнение следующих процедур:

генерации неизвлекаемого ключа подписи на основе случайной последовательности байт, полученных с ФДСЧ, его записи во внутреннюю память, и вычисление ключа проверки подписи, соответствующего неизвлекаемому ключу;

выработки сессионного ключа на основе случайной последовательности байт, полученных с ФДСЧ, и выработки ключа защиты ключей на основании ранее выработанных неизвлекаемого ключа подписи и ключа ее проверки, и зашифровывания на данном ключе сессионного ключа;

расшифровывание сессионного ключа на ключе защиты ключей, выработанном, в свою очередь, на основе неизвлекаемого ключа подписи и ключа ее проверки.

Данные отличия обеспечивают достижение указанного результата, поскольку при эксплуатации такого компьютера процедура обновления закрытых ключей, периодически проводимая с участием человека, больше не требуется. Такое решение промышленно применимо, т. к. оно соответствует действующим отечественным и международным нормативам [4, 5].

ИСТОЧНИКИ ИНФОРМАЦИИ

1. Патент России на полезную модель №138562.

2. Патент России на полезную модель №118773.

3. Сабанов А.Г. О неизвлекаемости закрытых ключей. «Защита информации. Инсайд» №2, март-апрель 2015.

4. ГОСТ Р ИСО/МЭК 9594-8-98.

5. ISO/IEC 13888-3:2009.

Формула полезной модели

Специализированный компьютер с аппаратной защитой данных, содержащий недоступный извне механический коммутатор, устанавливающий для запоминающего устройства, хранящего критичные данные, режим Read Only, отличающийся тем, что он содержит блок неизвлекаемого ключа, содержащий, в свою очередь, физический датчик случайных чисел (ФДСЧ) и микроконтроллер с внутренней памятью, запрограммированный на исполнение процедур генерации неизвлекаемого ключа подписи на основе

случайной последовательности байт, полученных с ФДСЧ, его записи во внутреннюю память, вычисление ключа проверки подписи, соответствующего неизвлекаемому ключу, выработки сессионного ключа на основе случайной последовательности байт, полученных с ФДСЧ, выработки ключа защиты ключей на основании ранее выработанных неизвлекаемого ключа подписи и ключа ее проверки, зашифровывания на данном ключе сессионного ключа, а также последующее расшифровывание сессионного ключа на ключе защиты ключей, выработанном, в свою очередь, на основе неизвлекаемого ключа подписи и ключа ее проверки.

КРАТКИЙ ОБЗОР НОРМАТИВНОЙ БАЗЫ ПО КРИТИЧЕСКИМ ИНФОРМАЦИОННЫМ ИНФРАСТРУКТУРАМ

Основные документы

Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – 187-ФЗ) [1], вступивший в силу с 1 января 2018 г. регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура, КИИ) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. Под безопасностью критической информационной инфраструктуры в 187-ФЗ понимается состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак. Под компьютерной атакой понимается целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами

информации. Под объектами критической информационной инфраструктуры понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры (ст. 2, п. 7 187-ФЗ). В свою очередь субъектами критической информационной инфраструктуры являются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей (ст. 2, п. 8 187-ФЗ).

Таким образом, 187-ФЗ и его подзаконные акты можно и нужно применять для обеспечения безопасности функционирования систем электронного банкинга.

Рассмотрим основные положения этих документов.

Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 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» [2]. Вводится перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, а также определяется порядок категорирования этих объектов. Категорирование осуществляется субъектами критической информационной инфраструктуры в отношении принадлежащих им на праве собственности, аренды или ином законном основании объектов критической информационной инфраструктуры, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры. Устанавливаются 3 категории значимости. Самая высокая категория – первая, самая низкая – третья. Определен перечень исходных данных для категорирования. Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом критической

информационной инфраструктуры перечня объектов. Перечень объектов в течение 5 рабочих дней после утверждения направляется в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры (ФСТЭК России). Определен перечень сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости (либо об отсутствии необходимости присвоения ему одной из таких категорий), направляемых в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры. Форма направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий утверждена **приказом ФСТЭК России от 22 декабря 2017 г. № 236** [3].

Следует отметить, что проект данного постановления Правительства Российской Федерации был согласован с Центральным Банком Российской Федерации.

По информации ФСТЭК России в настоящее время насчитывается более 250 систем банковской сферы и иных сфер финансового рынка, подлежащих категорированию в качестве объектов критической

информационной инфраструктуры. Как минимум половина из этих систем так или иначе относится к системам электронного банкинга, и доля их будет только увеличиваться.

Основными проблемными вопросами категорирования, с которыми приходится сталкиваться субъекту критической информационной инфраструктуры, являются:

- определение принадлежности к субъектам критической информационной инфраструктуры;
- определение критических процессов;
- определение перечня объектов критической информационной инфраструктуры, подлежащих категорированию;
- определение необходимости согласования перечня объектов критической информационной инфраструктуры с государственным органом или российским юридическим лицом;
- подготовка сведений о результатах категорирования объектов критической информационной инфраструктуры.

Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования утверждены **приказом ФСТЭК России от 21 декабря 2017 г. № 235** [4]. Документ определяет требования к силам, программным и программно-аппаратным средствам обеспечения

безопасности значимых объектов критической информационной инфраструктуры, к организационно-распорядительным документам, к функционированию системы безопасности в части организации работ.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры утверждены **приказом ФСТЭК России от 25 декабря 2017 г. № 239** [5]. Документом в зависимости от категории значимости и угроз безопасности информации определены следующие организационные и технические меры, подлежащие реализации:

идентификация и аутентификация;

управление доступом;

ограничение программной среды;

защита машинных носителей информации;

аудит безопасности;

антивирусная защита;

предотвращение вторжений (компьютерных атак);

обеспечение целостности;

обеспечение доступности;

защита технических средств и систем;

защита информационной (автоматизированной) системы и

ее компонентов;

планирование мероприятий по обеспечению безопасности;

управление конфигурацией;

управление обновлениями программного обеспечения;

реагирование на инциденты информационной безопасности;

обеспечение действий в нештатных (непредвиденных) ситуациях;

информирование и обучение персонала.

Средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации, применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической информационной инфраструктуры самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации.

В случае использования в значимом объекте сертифицированных на соответствие требованиям по безопасности информации средств защиты информации (это 6 видов средств защиты: межсетевые экраны, системы обнаружения вторжений, средства антивирусной защиты, средства доверенной загрузки,

средства контроля съемных машинных носителей информации, операционные системы):

а) в значимых объектах 1 категории применяются средства защиты информации не ниже 4 класса защиты, а также средства вычислительной техники не ниже 5 класса;

б) в значимых объектах 2 категории применяются средства защиты информации не ниже 5 класса защиты, а также средства вычислительной техники не ниже 5 класса;

в) в значимых объектах 3 категории применяются средства защиты информации 6 класса защиты, а также средства вычислительной техники не ниже 5 класса.

При этом в значимых объектах 1 категории значимости применяются сертифицированные средства защиты информации, соответствующие (вместо 4-го уровня НДВ) 4 или более высокому уровню доверия. В значимых объектах 2 категории значимости применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В значимых объектах 3 категории значимости применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.

В случае если значимый объект является государственной информационной системой или информационной системой персональных данных,

меры по обеспечению безопасности значимого объекта и меры защиты информации (персональных данных) принимаются в соответствии с более высокой категорией значимости, классом защищенности или уровнем защищенности персональных данных.

Таким образом, объекты КИИ (автоматизированные и информационные системы в их составе) подлежат защите также, как ГИС и ИСПДн *высоких классов защищенности.*

Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры» [6]. Правилами устанавливается порядок осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, и его территориальными органами мероприятий по государственному контролю в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Государственный контроль осуществляется путём проведения плановых и внеплановых выездных проверок. Проверка проводится должностными лицами органа государственного контроля, которые указаны в приказе

органа государственного контроля о проведении проверки. Срок проведения плановой проверки не должен превышать 20 рабочих дней. Срок проведения внеплановой проверки не должен превышать 10 рабочих дней. Информация об организации проверок, в том числе об их планировании, о проведении и результатах таких проверок, в органы прокуратуры не направляется, за исключением информации о результатах проверок, проведённых на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

Другие документы

Необходимо упомянуть также еще ряд документов ФСТЭК России и ФСБ России.

Приказ ФСТЭК России от 06.12.2017 №227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [7].

Приказ ФСТЭК России от 11.12.2017 №229 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской

Федерации» [8]. Содержание этих документов очевидно из названий.

Приказ ФСБ России от 24 июля 2018 г. N 366 «О Национальном координационном центре по компьютерным инцидентам» [9]. Инициирует создание Национального координационного центра по компьютерным инцидентам (НКЦКИ), определяет его задачи и права.

Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации...» [10]. Устанавливает набор параметров инцидентов для передачи в НКЦКИ (не позднее 24 часов с момента их обнаружения) и способы передачи информации.

Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации...» [11]. Определяет способы передачи информации об инциденте другим субъектам КИИ и получения сведений субъектами КИИ об атаках. Обмен информацией с иностранными организациями осуществляет НКЦКИ.

Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» [12]. Определяет требования к функциональным возможностям и характеристикам технических средств, необходимых для решения задач центров ГосСОПКА.

Приказ ФСБ России от 19.06.2019 № 281 «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты...» [13]. Обязывает субъекта КИИ согласовывать с НКЦКИ установку средств ГосСОПКА и уведомлять о приеме их в эксплуатацию. Определяет необходимые для согласования сведения. Срок согласования — до 45 календарных дней.

Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак...» [14]. Определяет состав плана реагирования на инциденты и принятия мер по ликвидации последствий, разрабатываемого субъектом КИИ. Обязует информировать НКЦКИ о результатах реагирования и ликвидации последствий не позднее 48 часов после завершения мероприятий.

Федеральным законом от 26.07.2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"» [15] внесены изменения, предусматривающие ответственность физических и юридических лиц:

создание, распространение и (или) использование ПО или иной компьютерной информации для неправомерного воздействия на КИИ:

- принудительные работы до 5 лет / лишение свободы до 5 лет / штраф до 1 млн руб.

Неправомерный доступ к информации КИИ, если он повлёк вред:

- принудительные работы до 5 лет / лишение свободы до 6 лет / штраф до 1 млн руб.

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой законом информации КИИ либо правил доступа, если оно повлекло причинение вреда для КИИ:

- принудительные работы до 5 лет / лишение свободы до 6 лет / запрет занимать должности до 3 лет.

Группой лиц или с использованием служебного положения:

• лишение свободы до 8 лет / запрет занимать должности до 3 лет.

Если повлекло тяжкие последствия:

• лишение свободы до 10 лет / запрет занимать должности до 5 лет.

К счастью, специалисты «на местах» не предоставлены сами себе в этой ситуации, в различных учебных центрах и центрах повышения квалификации проводятся курсы повышения квалификации по программам [16], разработанным в соответствии с **«Методическими рекомендациями по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации»** [17], утвержденными ФСТЭК России 16 апреля 2018 г., и примерной программой повышения квалификации **«Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры»** [18], утвержденной ФСТЭК России 17 декабря 2018 г. Разработка программы в соответствии с приведенными документами от ФСТЭК означает, что все положения, модули и темы программы утверждены регуляторами, и соответствуют нормативной методической базе.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 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»

3. Приказ ФСТЭК России от 22 декабря 2017 г. № 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. № 59) [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1590-prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236 (дата обращения: 16.08.2019).

4. Приказ ФСТЭК России от 11 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

5. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. приказа ФСТЭК России от 26 марта 2019 г. № 60) [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 16.08.2019).

6. Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной

инфраструктуры» [электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/287-postanovleniya/1617-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-17-fevralya-2018-g-n-163 (дата обращения: 20.08.2019).

7. Приказ ФСТЭК России от 06.12.2017 №227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1587-prikaz-fstek-rossii-ot-6-dekabrya-2017-g-n-227 (дата обращения: 16.08.2019).

8. Приказ ФСТЭК России от 11.12.2017 №229 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1475-prikaz-fstek-rossii-ot-11-dekabrya-2017-g-n-229 (дата обращения: 16.08.2019).

9. Приказ ФСБ России от 24 июля 2018 г. N 366 «О Национальном координационном центре по компьютерным инцидентам» [электронный ресурс]. URL: http://base.garant.ru/72041506/ (дата обращения: 16.08.2019).

10. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [электронный ресурс]. URL: http://base.garant.ru/72041504/ (дата обращения: 16.08.2019).

11. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской

Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» [электронный ресурс]. URL: http://base.garant.ru/72041500/ (дата обращения: 16.08.2019).

12. Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» [электронный ресурс]. URL: http://base.garant.ru/72257648/ (дата обращения: 16.08.2019).

13. Приказ ФСБ России от 19.06.2019 № 281 «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» [электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=329209&fld=134&dst=1000000001,0&rnd=0.3852266461376137#02990060630554834295 (дата обращения: 20.08.2019).

14. Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» [электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=329210&fld=134&dst=1000000001,0&rnd=0.9251330703791609#06741709231220478 (дата обращения: 20.08.2019).

15. Федеральный закон от 26.07.2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”» [электронный ресурс]. URL: https://rg.ru/2017/07/31/uk-dok.html (дата обращения: 16.08.2019).

16. Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры [электронный ресурс]. URL: http://www.okbsapr.ru/pclass-6.html (дата обращения: 24.09.2019).

17. Информационное сообщение ФСТЭК России от 23 апреля 2018 г. N 240/11/1868 «О разработанных ФСТЭК России Методических рекомендациях по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации» от 23 апреля 2018 г. N 240/11/1868 [электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obuchenie-spetsialistov/1559-informatsionnoe-soobshchenie-fstek-rossii-ot-23-aprelya-2018-g-n-240-11-1868 (дата обращения: 16.08.2019).

18. Информационное сообщение ФСТЭК России от 17 декабря 2018 г. N 240/11/5453 «О разработанной ФСТЭК России примерной программе повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры» [электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obuchenie-spetsialistov/1761-informatsionnoe-soobshchenie-fstek-rossii-ot-17-dekabrya-2018-g-n-240-11-5453 (дата обращения: 16.08.2019).