Разработка и программная реализация математических методов обеспечения защиты информации реального времени для высокотехнологичного машиностроительного оборудования

Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

Глазов Николай Егорович

Директор департамента специальных проектов

Научно-технический центр «СТАНКОИНФОРМЗАЩИТА»

1. **Исследования** в области информационной безопасности объектов критически важных инфраструктур
2. **Разработка** средств защиты информации в АСУ ТП, SCADA, оборудовании с ЧПУ
3. **Аудит** информационной безопасности промышленных объектов

Действующие лицензии


СЕРИЯ КИ 0094 НОМЕР 004666

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО РАЗРАБОТКЕ И ПРОИЗВОДСТВУ СРЕДСТВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 1078 от 18 декабря 2012 г.

Лицензия предоставлена Закрытому акционерному обществу «Научно-технический центр «Станкоинформзащита»

ОАО «НТЦ «Станкоинформзащита»)

ОГРН 1097746276385, ИНН 7715758652

Адрес места нахождения:

127572, г. Москва, ул. Абрамцевская, д. 9, корп. 1

Адрес места осуществления лицензируемой деятельности:

105082, г. Москва, ул. Большая Почтовая, д. 26, стр. 1, оф. 508


УФСБ России по городу Москве и Московской области

Серия РТ ЛИЦЕНЗИЯ № 0078517

Регистрационный номер 25458 от 21 ноября 14 г.

На осуществление лицензионного вида деятельности: проведение работ, связанных с использованием сведений, составляющих государственную тайну

Степень секретности выполняемых работ (услуг): секретно

Закрытому акционерному обществу «Научно-технический центр «Станкоинформзащита» (ЗАО «НТЦ «Станкоинформзащита»), ИНН 7715758652

Место нахождения: 127572, г. Москва, ул. Абрамцевская, д.9, корп.1

Место (места) осуществления лицензируемого вида деятельности: МОСКВА, пр. ДОНСКОЙ 5-П, д. 15, стр.8

Условия действия, ограничения: см. на обороте

Срок действия лицензии до 22 сентября 2019

Заместитель начальника Управления А.М. Колодяжный


СЕРИЯ КИ 0094

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 1912 от 18 декабря 2012 г.

Лицензия предоставлена Закрытому акционерному обществу «Научно-технический центр «Станкоинформзащита»

ОАО «НТЦ «Станкоинформзащита»)

ОГРН 1097746276385, ИНН 7715758652

Адрес места нахождения:

127572, г. Москва, ул. Абрамцевская, д. 9, корп. 1

Адрес места осуществления лицензируемой деятельности:

105082, г. Москва, ул. Большая Почтовая, д. 26, стр. 1, оф. 508

Перечень работ и услуг, на которые распространяется настоящая лицензия:

Лицензия переоформлена на основании приказа ФСТЭК России от 18 декабря 2012 г. № 295-л

Лицензия действует бессрочно

Начальник Управления И.Назаров


СЕРИЯ ГТ 0169 НОМЕР 008535

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ОСУЩЕСТВЛЕНИЕ МЕРОПРИЯТИЙ И (ИЛИ) ОКАЗАНИЕ УСЛУГ В ОБЛАСТИ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ

(в части технической защиты информации)

Регистрационный номер 3264 от 21 октября 2015 г.

Лицензия выдана Закрытому акционерному обществу «Научно-технический центр «Станкоинформзащита»

127572, г. Москва, ул. Абрамцевская, дом 9, корп. 1

ИНН 7715758652

Перечень мероприятий и услуг в области защиты государственной тайны, на которые распространяется настоящая лицензия:

проектирование объектов в защищенном исполнении (автоматизированных систем различного уровня и назначения; систем связи, приема, обработки и передачи данных; систем отображения и размещения, помещений со средствами (техническими), подлежащими защите, помещений, предназначенных для ведения секретных переговоров).

Лицензия действительна при наличии лицензий на проведение работ, связанных с использованием сведений, составляющих государственную тайну, и аттестатов соответствия на объекты информатизации.

Лицензия действительна до 21 октября

Заместитель

М.П.


МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЛИЦЕНЗИЯ

№ 13686-АТ от 10 декабря 2015 года

на осуществление разработки, производства, испытания и ремонта вооружения и техники

Виды работ (услуг), выполнение которых в составе указанного вида деятельности предоставляет

Настоящая лицензия предоставлена закрытому акционерному обществу «Научно-технический центр «Станкоинформзащита» (ЗАО «НТЦ «Станкоинформзащита»)

ОГРН 1097746276385 ИНН 7715758652


СЕРИЯ ГТ 0169 НОМЕР 008536

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ПРОВЕДЕНИЕ РАБОТ, СВЯЗАННЫХ С СОЗДАНИЕМ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Регистрационный номер 2582 от 9 августа 2015 г.

Лицензия выдана Закрытому акционерному обществу «Научно-технический центр «Станкоинформзащита»

127572, г. Москва, ул. Абрамцевская, дом 9, корп. 1

ИНН 7715758652

Перечень работ, составляющих средства защиты информации, на которые распространяется настоящая лицензия:

разработка, производство, реализация, установка, монтаж, наладка, испытания, ремонт, сервисное обслуживание:

технических средств защиты информации;

защищенных технических систем обработки информации;

технических средств контроля эффективности мер защиты информации;

программных (программно-технических) средств защиты информации;

защищенных программных (программно-технических) средств обработки информации;

программных (программно-технических) средств контроля защищенности информации.

Лицензия действительна при наличии лицензий на проведение работ, связанных с использованием сведений, составляющих государственную тайну, и аттестатов соответствия на объекты информатизации.

Лицензия действительна до 9 августа 2020 г.

Заместитель директора

А.Куц

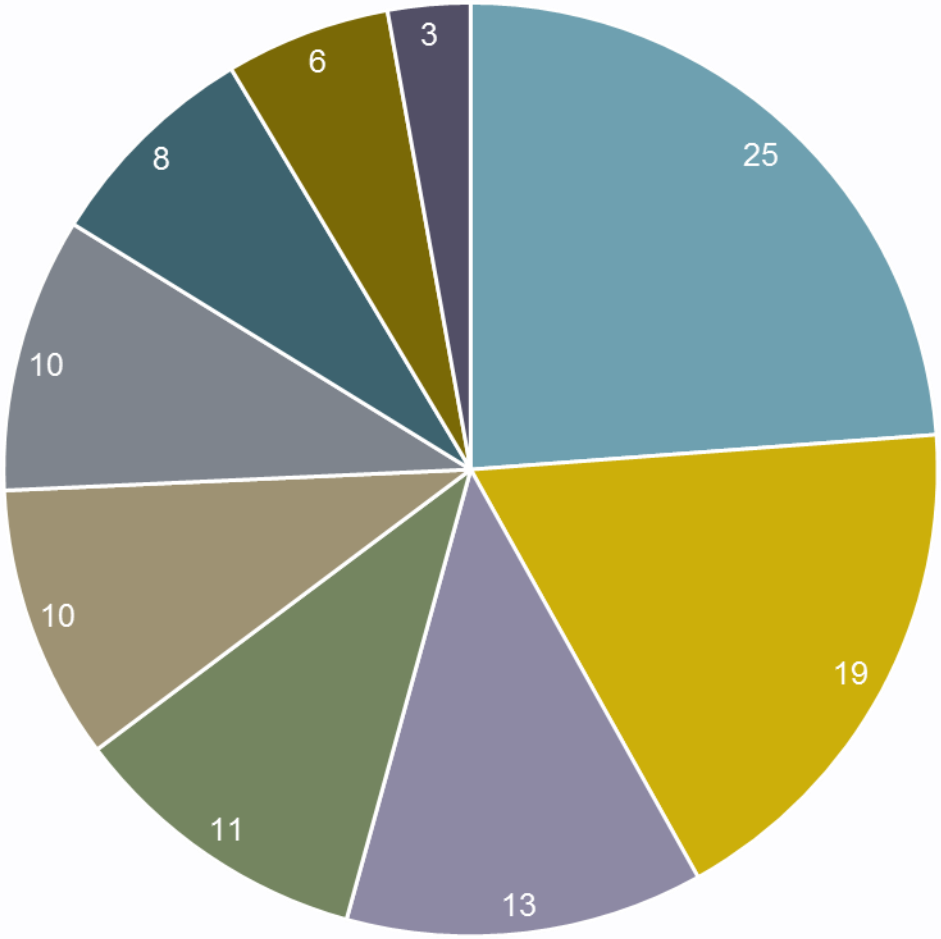
М.П.

Актуальность проблем безопасности АСУ ТП

1. Слабая защищенность технологических сетей и оборудования промышленных объектов
2. Высокая опасность последствий сбоев
3. Недостаточный уровень нормативно-правового регулирования
4. Отсутствие специализированных отечественных разработок в области безопасности АСУ ТП

Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

Виды уязвимостей АСУ ТП



- Отказ в обслуживании (DoS) (25)
- Ошибки в функции авторизации или ее отсутствие (19)
- Аварийное завершение атакуемой программы (13)
- Выполнение кода с помощью атакуемой программы (11)
- Раскрытие важной информации (10)
- Отсутствие необходимых проверок входных данных в WWW-интерфейсах (10)
- Уязвимость к фундаментальным сетевым атакам (8)
- Предопределенные данные авторизации (6)
- Слабые криптографические алгоритмы (3)

Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

Общая схема угроз промышленного объекта

Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

Цели и задачи проекта

Разработка программных средств защиты информации нового поколения, обеспечивающих необходимый уровень защиты информации в контурах, работающих в режиме реального времени.

1. Сбор и анализ информации, передаваемой с использованием типовых протоколов машиностроительного оборудования.
2. Разработка методов защиты промышленных технологических сетей, в том числе, и на уровне содержимого промышленных протоколов.
3. Реализация программных средств защиты, включая межсетевое экранирование, систему обнаружения вторжений и контроль целостности управляющего ПО, основывающихся на методах контроля промышленных протоколов.

Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

Компоненты проекта

1. **Методы и алгоритмы** защиты информации в технологических сетях промышленных объектов
2. **Специализированная архитектура** средств защиты информации
3. **Программные средства** защиты информации на промышленных объектах, включая:
   - межсетевой экран
   - система обнаружения вторжений
   - система предупреждения вторжений
   - система контроля целостности управляющих программ
4. **Методика** построения защищенной телекоммуникационной инфраструктуры промышленного объекта с использованием разработанных средств защиты

Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

Ключевые особенности

1. Обработка контролируемого трафика в режиме **реального времени**, исключающем задержки (до 5 мс) информационного обмена технологического оборудования
2. Методы и алгоритмы защиты информации осуществляют анализ **содержимого сетевого трафика**, в том числе структуру и данные, передаваемые по промышленным протоколам
3. Методы и алгоритмы защиты информации осуществляют **контроль состояния** контролируемого технологического процесса, автоматически определяя нежелательные сценарии

Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

Основные алгоритмы

Система обнаружения вторжений	
Стандартные сетевые протоколы, Simatic S7, Profinet, Modbus, EtherNet/IP, IEC 60870-5-104, DNP3	
Интеллектуальные методы	Сигнатурные методы
1. Обнаружение аномалий с поддержкой режима самообучения 2. Обработка правил с возможностью поиска нечетких совпадений 3. Проверка содержимого команд технологических операций	Формирование БД сигнатур, в т.ч. по технологическим протоколам

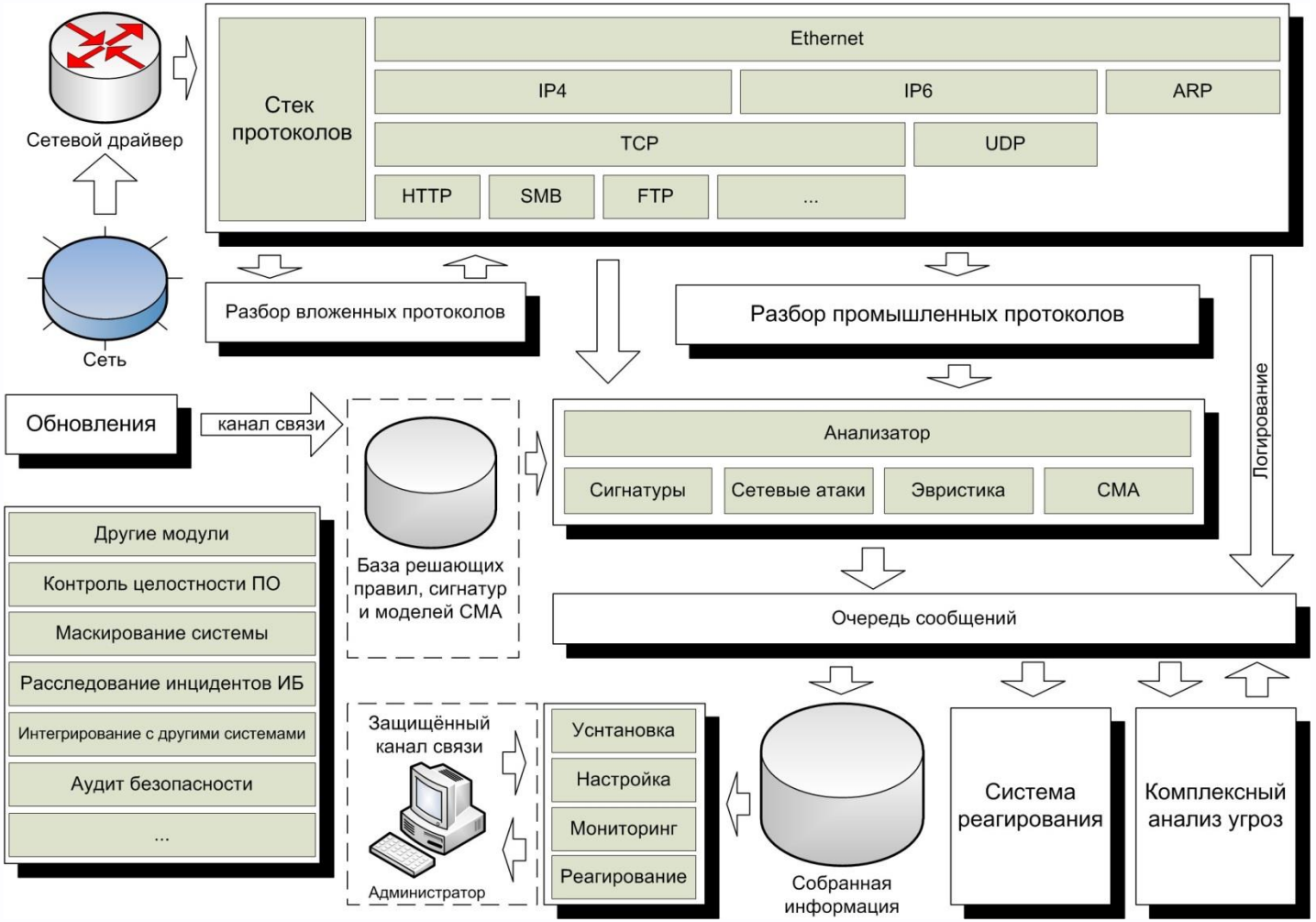
Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

Основные алгоритмы

Межсетевой экран	Контроль целостности управляющего ПО
1. Стандартный МЭ корпоративной сети 2. Функции контроля технологического трафика на основе **таблиц правил и состояний**	1. Автоматическое распознавание и извлечение управляющего ПО 2. Защищенная инфраструктура хранилища эталонных образцов ПО

Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

Схема программной платформы средств защиты информации в АСУ ТП



Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

Перспективы

ПО защиты информации в системах реального времени

Информационно-программные средства для автоматизации управления высокотехнологичным оборудованием в условиях цифрового машиностроительного производства

Реализация проекта в целом позволит:

- решить проблему **комплексирования** отечественных программно-технических средств автоматизации
- сократить технологическое отставание отечественного машиностроения за счет внедрения **оперативного управления** цифровым производством (MES, Digital Manufacturing);
- обеспечить готовность предприятий отрасли к переходу на цифровое производство;
- обеспечить унификацию технологий и решение проблем стандартизации машиностроительного производства.

Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

СПАСИБО ЗА ВНИМАНИЕ !

Исследования проводятся при финансовой поддержке Министерства образования и науки Российской Федерации. Уникальный идентификатор соглашения RFMEFI57916X0131

ЗАО «НТЦ «Станкоинформзащита»
105082, г. Москва, ул. Большая Почтовая, д.26, стр.1
Тел. (495) 790-16-60
www.ntcsiz.ru