Анна Табульда, Светлана Чернущенко

Особенности обеспечения информационной безопасности промышленных систем автоматизации в соответствии с приказом ФСТЭК № 31

Трудно переоценить важность вопроса обеспечения информационной безопасности (далее – ИБ) в целом для страны и в частности для объектов повышенной опасности, коими являются промышленные системы автоматизации.

Исключений нет: инциденты ИБ происходят в различных отраслях и сферах функционирования промышленных систем автоматизации (рис. 1) и порой приводят к катастрофическим последствиям [1, 2].

С целью урегулирования вопросов, связанных с обеспечением ИБ промышленных систем автоматизации, в нашей стране ведётся нормотворческая деятельность. Результатом данной деятельности стал вступивший в силу в 2014 году приказ ФСТЭК России № 31 [4] (далее – приказ № 31). Однако по сей день отсутствуют методические документы к приказу № 31, которые раскроют меры по защите информации, моделированию угроз, выявлению и устранению уязвимостей, реагированию на инциденты, связанные с нарушением защиты информации в АСУ ТП.

По причине их отсутствия образовался некий переходный период: сегодня при обеспечении безопасности АСУ ТП согласно требованиям приказа № 31 возникает необходимость в принятии решений по нерегламентированным вопросам. Каким образом? Например, опираясь на практики методических документов ФСТЭК, относящихся к ключевым системам информационной инфраструктуры (КСИИ) [5, 6, 7, 8] и к другим типам систем [9, 10].

Однако приказ № 31 в силу специфичности промышленных систем автоматизации обладает рядом особенностей относительно ранее выпущенных ФСТЭК документов [9, 10].

В рамках данной статьи мы рассмотрим некоторые из них, опираясь на практику применения положений приказа № 31 на объекте нефтеперерабатывающей отрасли.

Обеспечение безопасной разработки ПО

Первая особенность приказа № 31 – «уникальные» требования обеспечения безопасной разработки программного обеспечения (ОБР), которых нет в аналогичных приказах ФСТЭК. Ввиду отсутствия методических документов обратимся за ответами на вопросы о мерах защиты ОБР напря-

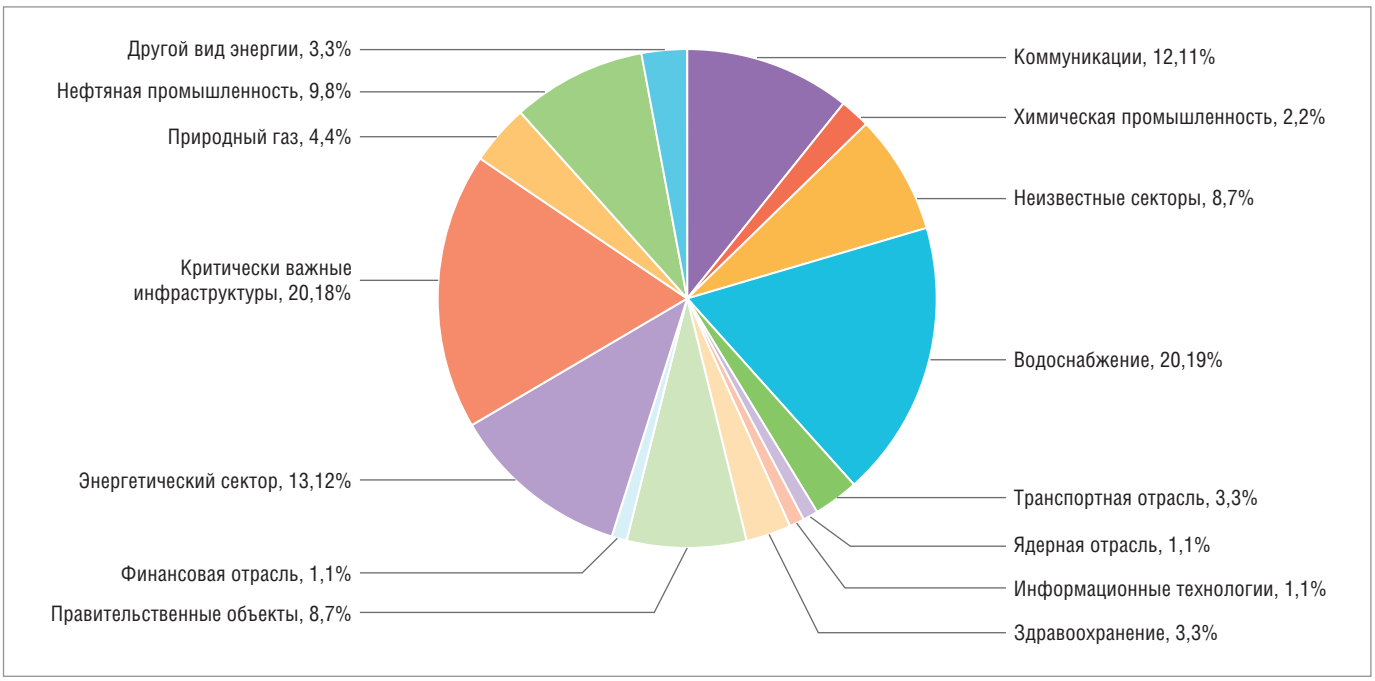


Рис. 1. Количество инцидентов ИБ в различных секторах функционирования АСУ ТП за первую половину 2015 финансового года [3]

Таблица 1

Комментарии ФСТЭК к подсистеме ОБР приказа № 31

Вопрос, касающийся подсистемы ОБР приказа № 31	Выдержка из ответа представителей ФСТЭК
Являются ли инженеры-программисты (представители оператора АСУ), разрабатывающие/дорабатывающие прикладное ПО для функционирования АСУ ТП (мнемосхемы, алгоритмы ПЛК и т.д.), разработчиками согласно терминологии приказа № 31?	К разработчикам системы защиты информации АСУ относятся в том числе инженеры-программисты, привлекаемые к разработке/доработке прикладного ПО для обеспечения безопасности информации в АСУ.
В случае самостоятельной разработки прикладного ПО операторами АСУ и необходимости выполнения ими требований к ОБР, какие из анализаторов кода можно использовать? На данный момент известные анализаторы кода не ориентированы на SCADA-пакеты и АСУ в целом (не поддерживают языки программирования ПЛК, к примеру).	Выбор автоматизированных средств, применяемых для реализации мер защиты информации по обеспечению безопасной разработки ПО, осуществляется оператором самостоятельно. В случае отсутствия автоматизированных средств анализа кода он может быть проведён методом ручного анализа.
Может ли оператор АСУ использовать ПО стороннего разработчика, который не выполняет требования ОБР.0–ОБР.6 при разработке ПО? Если да, то при каких условиях?	В процессе проектирования АСУ разработчиком должно быть выбрано ПО, соответствующее требованиям в части разработки ПО. В случае отсутствия возможности использования указанного ПО разработчиком системы защиты АСУ должны быть реализованы компенсирующие меры, связанные с применением недоверенного ПО, в соответствии с пунктом 22 требований.
Согласно п. 18.14 приказа № 31 контроль принимаемых мер по выявлению, анализу и устранению уязвимостей ПО осуществляется заказчиком и (или) оператором АСУ. Каким образом выполняется данное требование в случае, когда заказчиком или оператором АСУ не осуществляется разработка прикладного ПО, а используется прикладное ПО (SCADA-пакеты, СУБД, исполнительные системы ПЛК и т.д.) сторонних разработчиков?	Контроль принимаемых мер защиты информации по выявлению, анализу и устранению уязвимостей, в том числе прикладного ПО сторонних разработчиков, может проводиться на этапе внедрения системы защиты АСУ при анализе уязвимостей АСУ в соответствии с пунктом 15.7 требований. Кроме того, при приобретении стороннего ПО необходимо предусмотреть процедуру запроса документов, подтверждающих тестирование ПО на уязвимости при разработке.

Таблица 2

Критерии определения класса защищённости АСУ ТП

Вид информации (измерительная, управляющая и т.д.)	Нарушаемое свойство безопасности	Характер чрезвычайной ситуации	Степень ущерба	Уровень значимости	Итоговый уровень значимости	Класс защищённости АСУ ТП
Наименование 1	Целостность	Согласно таблице 3	Согласно таблице 3	= максимальной степени ущерба данного вида информации (У31/У32/У33)	= максимальному уровню значимости (У31/У32/У33)	К1 = У31 (высокий) К2 = У32 (средний) К3 =У33 (низкий)
	Доступность	Согласно таблице 3	Согласно таблице 3			
	Конфиденциальность	Согласно таблице 3	Согласно таблице 3			
Наименование N	Целостность	Согласно таблице 3	Согласно таблице 3	= максимальной степени ущерба данного вида информации (У31/У32/У33)		
	Доступность	Согласно таблице 3	Согласно таблице 3			
	Конфиденциальность	Согласно таблице 3	Согласно таблице 3			

мую к разработчикам приказа № 31. Разъяснения представителей ФСТЭК представлены в таблице 1.

Получается, что требования подсистемы ОБР предъявляются к ПО, разрабатываемому в том числе представителями оператора АСУ ТП[1], таким образом, необходима реализация определённого для конкретной АСУ ТП набора мер данной подсистемы. Плюс в том, что положениями приказа № 31 разрешено применять механизмы адаптации и уточнения требований, которые позволяют обосновать, например, использование ручного анализа кода вместо статистического или динамического, то есть возможность использования компенсирующих мер даёт возможность для каждого специфичного случая обеспечить требуемый уровень защищённости АСУ ТП.

Класс защищённости АСУ ТП

Следующая особенность заключается в распределении обязанностей участников процесса защиты АСУ ТП (заказчик/оператор/разработчик) при определении класса защищённости АСУ ТП, от которого, в том числе, зависит набор мер защиты информации в АСУ ТП, а также применяемые средства защиты информации.

При проектировании новой системы заказчик или оператор согласно приказу № 31 должен определить степень ущерба от нарушения целостности/доступности/конфиденциальности информации. Полученная степень ущерба необходима разработчику системы информационной безопасности для определения класса защищённости АСУ ТП и зависит от характера чрезвычайной ситуации.

Однако заказчик или оператор не могут предоставить требуемые данные, ведь объект по факту ещё не существует. Выход: определить характер чрезвычайной ситуации можно, либо исходя из паспортов аналогичных, уже введённых в эксплуатацию систем, либо методом экспертной оценки. Таким образом, АСУ ТП присваивается предварительный класс защищённости.

Критерии, на основании которых определяется предварительный класс защищённости АСУ ТП, представлены в таблицах 2 и 3.

Сертификация СрЗИ

Третья особенность – применение средств защиты информации (СрЗИ). Согласно информационному сообщению ФСТЭК России (№ 240/22/2748 от 25 июля 2014 г.) в АСУ ТП применяются СрЗИ, прошедшие оценку соответствия в форме, установленной заказчиком в техническом задании (ТЗ) в соответствии с ФЗ «О техническом регулировании». Однако на практике в ТЗ заказчик указывает всё ту же пресловутую фразу про оценку соответствия СрЗИ без уточнения формы. Остаётся проектировать систему защиты АСУ ТП с применением СрЗИ, прошедших оценку соответствия в форме обязательной и/или добровольной сертификации (если, например,

[1]Оператор АСУ ТП – лицо, обеспечивающее эксплуатацию автоматизированных систем управления [4].

Таблица 3

Определение степени ущерба и характера чрезвычайной ситуации

Характер чрезвычайной ситуации*	Ущерб	
	Наименование	Значение
Низкая степень ущерба		
Локальный характер	Величина материального ущерба	а) не более 100 тыс. рублей
	Число пострадавших	а) не более 10 человек
	Зона чрезвычайной ситуации	а) не выходит за пределы территории объекта
Муниципальный характер	Величина материального ущерба	б) свыше 100 тыс. рублей, но не более 5 млн рублей
	Число пострадавших	б) свыше 10 человек, но не более 50 человек
	Зона чрезвычайной ситуации	б) не выходит за пределы территории одного поселения или внутригородской территории города федерального значения
	Дополнительное условие	а также данная чрезвычайная ситуация не может быть отнесена к чрезвычайной ситуации локального характера
Средняя степень ущерба		
Межмуниципальный характер	Величина материального ущерба	б) свыше 100 тыс. рублей, но не более 5 млн рублей
	Число пострадавших	б) свыше 10 человек, но не более 50 человек
	Зона чрезвычайной ситуации	в) затрагивает территорию двух и более поселений, внутригородских территорий города федерального значения или межселенную территорию
Региональный характер	Величина материального ущерба	в) свыше 5 млн рублей, но не более 500 млн рублей
	Число пострадавших	в) свыше 50 человек, но не более 500 человек
	Зона чрезвычайной ситуации	г) не выходит за пределы территории одного субъекта Российской Федерации
Высокая степень ущерба		
Межрегиональный характер	Величина материального ущерба	в) свыше 5 млн рублей, но не более 500 млн рублей
	Число пострадавших	в) свыше 50 человек, но не более 500 человек
	Зона чрезвычайной ситуации	д) затрагивает территорию двух и более субъектов Российской Федерации
Федеральный характер	Величина материального ущерба	г) свыше 500 млн рублей
	Число пострадавших	г) свыше 500 человек
	Зона чрезвычайной ситуации	е) федерального характера

*Характер ЧС определяется в соответствии с постановлением Правительства РФ № 304 [11]

требования нормативных документов конкретной отрасли по защите информации в АСУ ТП позволяют применять СрЗИ, имеющие сертификат соответствующей системы добровольной сертификации).

Причины следующие:

- отсутствие чёткого толкования условий и результата проведения оценки соответствия в других формах;
- устоявшаяся практика применения сертифицированных СрЗИ;
- отсутствие практики применения СрЗИ, прошедших оценку соответствия в других формах (следствие из предыдущего пункта).

Ответственный за ИБ АСУ ТП

Четвёртая особенность, вызывающая горячие споры в профессиональном сообществе специалистов по ИБ промышленных систем автоматизации, – структурное подразделение или должностное лицо (работник), ответственное за защиту информации в АСУ ТП. Уйти от этого вопроса не удастся – ответственный должен быть назначен согласно приказу № 31, а вот кто им должен быть, остаётся за кадром. Давайте разбираться.

При рассмотрении предприятия через призму ИБ–АСУ ТП–ИТ обособление данных направлений в отдельные подразделения, находящиеся на одном уровне организационной иерархии, на практике расценивается как самый эффективный вариант, обеспечивающий равенство интересов трёх направлений или их обоснованную приоритезацию с учётом стратегии развития. Ответственный за ИБ промышленных систем автоматизации должен относиться к подразделению ИБ и обладать компетенциями в сфере автоматизации. Стоит учитывать также зарубежный опыт в данном вопросе: самым подходящим решением является создание по примеру NIST SP 800-82 [12] межфункциональной команды кибербезопасности, обеспечивающей плотное взаимодействие этих направлений.

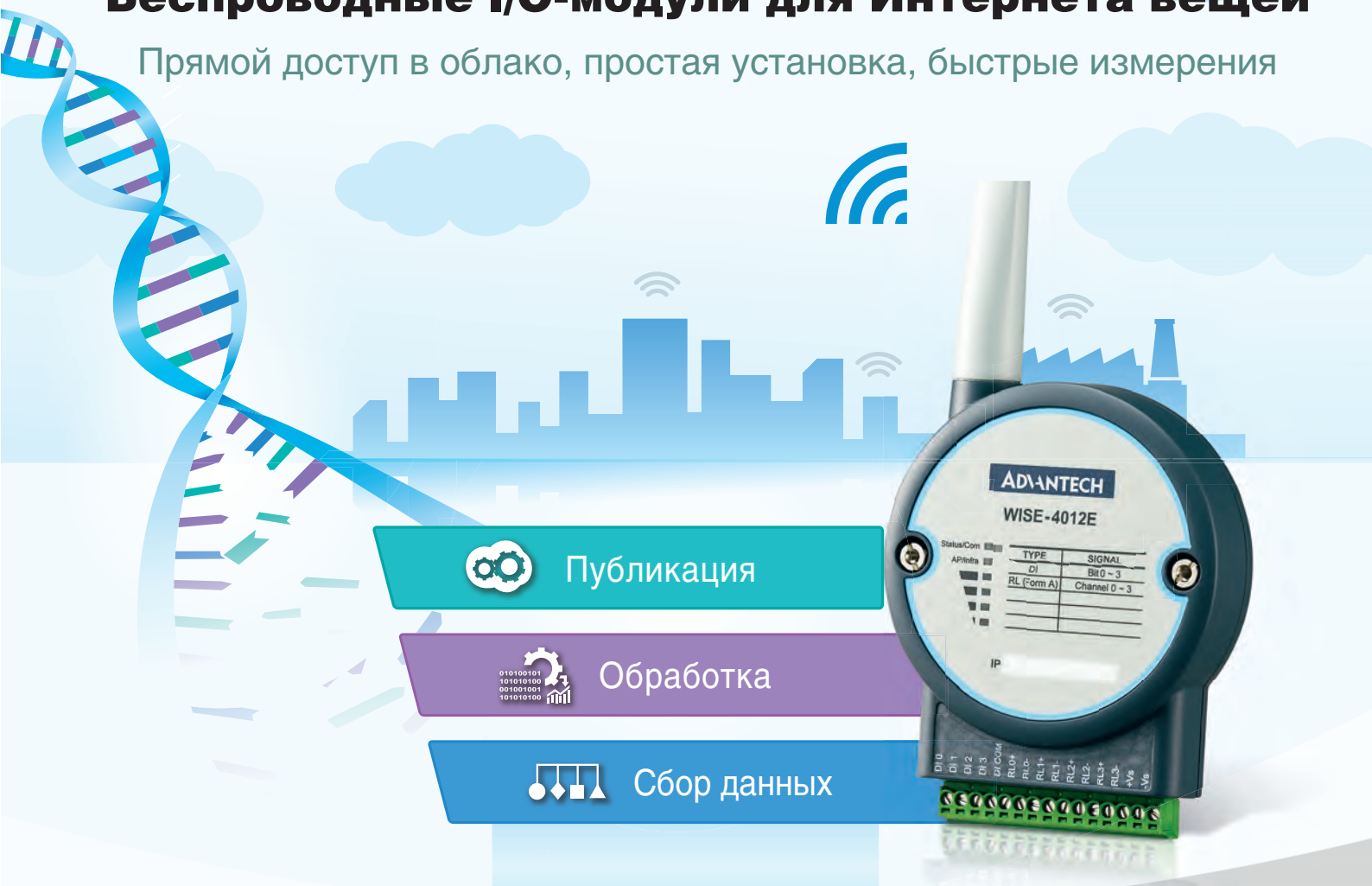
Таким образом, на примере рассмотренных особенностей обеспечения ИБ промышленных систем автоматизации в соответствии с приказом ФСТЭК № 31 становится очевидным, что с одной стороны, есть сложность и неоднозначность применения в переходный период положений приказа ФСТЭК России № 31, предъявляющего специфичные требования к защите информации в АСУ ТП, а с другой стороны, предоставляется возможность адаптации, уточнения, дополнения защитных мер, позволяющая применять компенсирующие защитные меры и обеспечивать гибкий подход к построению системы защиты информации в АСУ ТП. ●

Литература

1. Stuxnet [Электронный ресурс] // Википедия. – Режим доступа : https://ru.wikipedia.org/wiki/Stuxnet.
2. Хакеры случайно получили доступ к SCADA-системе водоочистной станции и ради интереса изменили её настройки [Электронный ресурс] // SecurityLab.ru. – Режим доступа : http://www.securitylab.ru/news/480334.php.
3. ICS-CERT Fiscal Year 2015: Mid-Year Statistics [Электронный ресурс] // ICS-CERT MONITOR. – Режим доступа : https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf.

Беспроводные I/O-модули для Интернета вещей

Прямой доступ в облако, простая установка, быстрые измерения



ADVANTECH

Enabling an Intelligent Planet

ДНК беспроводных I/O-модулей для Интернета вещей

Компания Advantech выпустила новое поколение беспроводных модулей ввода/вывода для Интернета вещей, разработанное в духе информационных технологий, которые позволяют решать различные задачи. Концепция сбора, обработки и публикации данных позволяет реализовывать различные сценарии мобильного мониторинга сигналов в одном компактном модуле. Использование стандартного Wi-Fi упрощает развертывание системы без излишних затрат на проводку и монтаж, предоставляя дополнительные возможности для сбора большего объема данных в эпоху Интернета вещей (IoT).

WISE-4012E
Набор разработчика для Интернета вещей
6-канальный беспроводной модуль ввода/вывода с комплектом разработчика

WISE-4050
Беспроводной модуль с 4 каналами дискретного ввода и 2 каналами дискретного вывода

WISE-4012
Беспроводной модуль с 4 каналами универсального ввода и 2 каналами дискретного вывода

WISE-4060
Беспроводной модуль с 4 каналами универсального ввода и 2 выходными реле

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР ПРОДУКЦИИ ADVANTECH

4. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : приказ ФСТЭК России от 14 марта 2014 г. № 31.
5. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры : утв. ФСТЭК России 18.05.2007.
6. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры : утв. ФСТЭК России 18.05.2007.
7. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры : утв. ФСТЭК России 18.05.2007.
8. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры : утв. ФСТЭК России 19.11.2007.
9. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11 фев. 2013 г. № 17.
10. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18 фев. 2013 г. № 21.
11. О классификации чрезвычайных ситуаций природного и техногенного характера : постановление Правительства Российской Федерации от 21 мая 2007 г. № 304.
12. K. Stouffer, V. Pillitteri, M. Abrams, A. Hahn. Guide to ICS Security : NIST SP 800-82 Revision 2 [Электронный ресурс] // NIST. – Режим доступа: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf/

E-mail: chernushchenko@gmail.com

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

Новости ISA

19–21 мая делегация Российской секции ISA во главе с президентом секции, проректором ГУАП Любовью Александровной Тимофеевой приняла участие в работе Исполкома округа 12 ISA (EMEA) в Милане. 20 мая в торжественной обстановке члену российской делегации Александру Владимировичу Бобовичу президентом ISA господином James Keaveney (США) была вручена премия “Automation Excellence In Academics Award”. А.В. Бобович стал первым в Европе, получившим учреждённую в 2016 году высокую профессиональную награду ISA.

23 июня на заседании Учёного совета ГУАП ректор ГУАП Юлия Анатольевна Антохина вручила студентам и аспирантам – победителям XII Европейского конкурса на лучшую студенческую научную работу ISA (ESPC-2016) дипломы и медали. Золотых медалей удостоены Александр Сорокин, Александр Чабаненко, Виталий Кузнецов, Василий Казаков, Георгий Король. Серебряные медали вручены Ефиму Головину, Александру Зеленину, Евгении Петрашкевич, Борису Осколкову, Марии Макаренко, Илье Иванову и Марии Шелест. Бронзовыми медалями отмечены работы Александра Вакуленко, Евгения Григорьева, Артемия Журавлёва, Ивана Юдина, Ярослава Баранова, Александра Кожевина, Антонины Макеевой. Приз за победу в общекомандном зачёте из рук ректора ГУАП получил президент студенческой секции ISA ГУАП аспирант Александр Чабаненко.

27 июня в атриуме Петропавловской крепости чествовали лучших выпускников высших учебных заведений Санкт-Петербурга. В XIV церемонии приняли участие вице-губернатор города Владимир Владимирович Кириллов, члены правительства, ректоры высших учебных заведений, начальники военных училищ и академий и, конечно же, сами выпускники и члены их семей. ГУАП на торжественной церемонии представляли ректор университета Ю.А. Антохина (президент Российской секции ISA 2014 года), президент университета Анатолий Аркадьевич Оводенко (Глава представительства ISA в Российской Федерации) и директор института инноватики и базовой магистерской подготовки ГУАП Елена Георгиевна Семёнова (президент Российской секции ISA 2011 года). Лучшим выпускником ГУАП 2016 года признан Алексей Курлов – активный член студенческой секции ISA ГУАП, выпускник института инноватики и базовой магистерской подготовки. За годы учёбы он зарекомендовал себя не только как студент-отличник (средний балл по итогам сессии – 5,0), но и как талантливый учёный, исследователь, практик. На его счету десятки статей и докладов в научных журналах и на конференциях, а результаты исследований магистерской диссертации Алексея нашли своё применение на практике в виде устройства, которое уже получило акт внедрения и сейчас находится на рассмотрении в Роспатенте.

Губернатор Санкт-Петербурга Г.С. Полтавченко и ректор ГУАП Ю.А. Антохина на выставке дипломных проектов

1 июля в Санкт-Петербурге прошла выставка дипломных проектов, выполненных студентами вузов Санкт-Петербурга по заданию исполнительных органов государственной власти Санкт-Петербурга «Студенты – городу 2016». Троим выпускникам ГУАП 2016 года, членам студенческой секции ISA, выигравшим конкурс, было предоставлено право выполнить дипломные проекты. По заданию Комитета по энергетике и инженерному обеспечению работу на тему «Возможности использования энергии ветра, приливов и отливов в Северо-Западном регионе РФ. Сценарные условия развития, возможности реализации проектов. Экономическое и экологическое обоснование» подготовил Артём Кашаев. Руководителем работы был Владислав Фёдорович Шишлаков, директор института инновационных технологий в электромеханике и робототехнике ГУАП, доктор технических наук, профессор. Работу на тему «Балансировка высоконагружаемых приложений с использованием проксирующих серверов» по заданию комитета по информатизации и связи выполнил Виталий Фундовой, а руководил ею кандидат технических наук, доцент Евгений Александрович Бакин, участник Всемирных студенческих приборостроительных игр ISA, бывший президент студенческой секции ISA ГУАП. По заданию Комитета по развитию транспортной инфраструктуры Санкт-Петербурга работу на тему «Перспективы развития проекта „Городские причалы Санкт-Петербурга“, проблемы, пути решения» подготовил Кирилл Гоголев. Проектом руководил кандидат технических наук, доцент Николай Николаевич Майоров (заместитель директора института аэрокосмических приборов и систем ГУАП, активный член Российской секции ISA). Губернатор Санкт-Петербурга Георгий Сергеевич Полтавченко, посетивший выставку, внимательно ознакомился с экспозицией ГУАП и поблагодарил студентов и руководителей. Ректор ГУАП Ю.А. Антохина и президент ГУАП А.А. Оводенко представили губернатору студентов и их работы.

PENTAIR

Schroff®

Платформа EuropacPRO — евромеханика высокого полёта

PROгрессивные блочные каркасы и приборные корпуса

- Безграничное разнообразие конфигураций из унифицированных компонентов
- Современный промышленный дизайн
- Высокая прочность и надёжность
- Доработка под индивидуальные требования

ОФИЦИАЛЬНЫЙ ПОСТАВЩИК ПРОДУКЦИИ SCHROFF

ProSoft® 25 лет

МОСКВА Тел.: (495) 234-0636 • Факс: (495) 234-0640 • info@prosoft.ru • www.prosoft.ru
С.-ПЕТЕРБУРГ Тел.: (812) 448-0444 • Факс: (812) 448-0339 • info@spb.prosoft.ru • www.prosoft.ru
ЕКАТЕРИНБУРГ Тел.: (343) 376-2820 • Факс: (343) 310-0106 • info@prosoftsystems.ru • www.prosoftsystems.ru