Решения Cisco по защите автоматизированных систем управления технологическими процессами

Рост инцидентов с безопасностью АСУ ТП

Сегодня, в условиях поголовной информатизации всех сфер жизни, как никогда остро встает задача обеспечения информационной безопасности критически важных объектов (КВО), ответственных за функционирование различных систем жизнеобеспечения, финансового управления, транспорта, ЖКХ, энергетики и т.п. Но если раньше такие системы создавались изолированными от Интернет и на базе проприетарных протоколов и технологий, то сейчас ситуация совершенно иная. Бизнес-необходимость требует унификации и стандартизации используемых решений, что и обуславливает массовый переход на новые поколения индустриальных сетей, использующих протокол IP, универсальные операционные системы, подключение к Интернет и т.п. Собранная за последние годы статистика уязвимостей и инцидентов в таких сетях показывает, что число проблем постоянно нарастает. Все это приводит к необходимости пересмотра подходов к защите критических важных объектов и функционирующих на них автоматизированных системах управления технологическими процессами (АСУ ТП).

История кибератак на критически важные объекты России насчитывает уже свыше четверти века, но предметно к решению этой проблемы стали подходить совсем недавно. Подтолкнуло к этому сразу несколько событий – проникновение червя Stuxnet на завод по обогащению ядерного топлива в Иране, катастрофа на Саяно-Шушенской ГЭС, террористическая атака на Баксанскую ГЭС, вредоносные программы Red October, «Маска» и ряд других, менее публичных, но не менее значимых событий. Все это привело к тому, что начиная с 2011-го года Россия, после пятилетнего перерыва вновь обратилась к теме регулирования вопросов обеспечения информационной безопасности критически важных объектов и, в частности, автоматизированных систем управления технологическими процессами.

Обзор законодательства по защите АСУ ТП

Законодательство в области обеспечения информационной безопасности АСУ ТП имеет в России давнюю историю. Первые шаги предпринимались еще в 2006-м году, когда был разработан первый законопроект по данной теме - «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры». Дальнейшие законодательные инициативы привели к появлению соответствующих разделов в «Стратегии национальной безопасности Российской Федерации до 2020 года», в законе «О безопасности объектов топливно-энергетического комплекса», а также в некоторых Постановления Правительства и Указах Президента России.

В 2012-м году Совет Безопасности РФ опубликовал подписанные Президентом России «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», которые заложили основу для формирования всей последующей нормативной базы в области защиты АСУ ТП. Именно на его базе в 2013-м году был разработаны законопроекты «О безопасности критической информационной инфраструктуры Российской Федерации» и «О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», которые должны быть приняты в конце 2014-го – начале 2015-го годов.

14 марта 2014 года был утвержден, а 30 июня 2014 года зарегистрирован в Минюсте новый приказ ФСТЭК №31 «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». Именно он обеспечивает базу для формирования организационных и технический мер защиты АСУ ТП.

Меры защиты АСУ ТП

Согласно нормативным документам ФСТЭК состав и содержание мер защиты АСУ ТП определяется владельцем или оператором такой системы в зависимости от ее класса защищенности, структурно-функциональных характеристик АСУ ТП, реализуемых информационных технологий, особенностей функционирования защищаемого технологического процесса, а также от актуальных угроз и целей защиты.
В состав мер по обеспечению безопасности, описанных в приказе ФСТЭК №31 от 14 марта 2014 года «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», входят следующие блоки требований:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранится и (или) обрабатывается защищаемая информация;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности защищаемой информации;
- обеспечение целостности АСУ ТП и защищаемой информации;
- обеспечение доступности защищаемой информации;
- защита среды виртуализации;
- защита технических средств;
- защита АСУ ТП, ее средств, систем связи и передачи данных;
- безопасная разработка прикладного и специального программного обеспечения разработчиком;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению защиты информации;
- обеспечение действий в нештатных (непредвиденных) ситуациях;
- информирование и обучение пользователей;
- анализ угроз безопасности информации и рисков от их реализации;
- выявление инцидентов и реагирование на них;
- управление конфигурацией информационной системы и ее системы защиты.

Cisco Internet of Things Group

Компания Cisco уделяет большое внимание как вопросам построения отказоустойчивых и надежных сетей АСУТП, так и сопутствующим вопросам обеспечения информационной безопасности на критически важных объектах заказчиков. С этой целью в компании много лет назад был создана специализированная группа CIAG (Critical Infrastructure Assurance Group), которая позже была реорганизована в отдельное фокусное подразделение Cisco Connected Industries Group. Совсем недавно, данное подразделение было существенно расширено и переименовано в Cisco Internet of Things Group, зоной влияния которого стали не только решения в области построения надежных и защищенных сетей на индустриальных объектах, но и все остальные сценарии межмашинного взаимодействия, описываемые термином «Всеобъемлющий Интернет».
Эксперты компании Cisco на протяжении последнего десятилетия активно участвуют в работе различных консультационных и экспертных советов, а также рабочих групп, занимающихся безопасностью критически важных объектов в различных отраслях экономики. В частности, сотрудники Cisco участвуют в работе:

- National Infrastructure Advisory Council (NIAC),
- NIAC Vulnerability Framework Committee
- AGA-12
- ISA SP99
- DNP
- ODVA

- Process Control Security Requirements Forum
- IEC TC 57 WG 15
- NCMS Manufacturing Trust
- Network Reliability and Interoperability Council (NRIC)
- Partnership for Critical Infrastructure Security

Все это позволяет нам предлагать решения, учитывающие специфику той или иной отрасли или сегмента рынка.

Архитектура Cisco для защиты АСУ ТП

Сеть АСУ ТП имеет четко выраженные отличия от корпоративных сетей передачи данных:

- Малейший простой в работе сети АСУ ТП может привести к остановке сложного технологического процесса.
- Последствия отказа сети АСУ ТП могу быть катастрофическими:
    - гибель людей,
    - техногенные катастрофы,
    - экологические бедствия.
- Очень часто в сетях АСУ ТП до сих пор используются проприетарные технологические протоколы производителей оборудования АСУ ТП, которые таят в себе сложно обнаруживаемые уязвимости, которые тяжело вовремя закрывать производителям традиционных систем обеспечения информационной безопасности и производителям самого оборудования АСУ ТП.
- Сеть АСУ ТП должна быть максимально доступной, порой даже в ущерб безопасности. Ложные срабатывания (False-Positives), влекущие за собой отключение сегментов сети или перебои в обеспечении штатного функционирования технологических процессов недопустимы.
- Обмен данными с корпоративной сетью с целью функционирования MES, ERP и других систем, а также предоставления удаленного доступа и управления сетью АСУ ТП со стороны подрядчиков, в том числе и через Интернет, не может быть блокирован и поэтому должен выполняться по строгим правилам построения, так называемый, буферных, демилитаризованных зон, и в полном соответствии с отраслевыми стандартами и рекомендациями.

Учитывая все вышеупомянутые и другие особенности, характерные сетям АСУ ТП, компания Cisco совместно с одним из мировых лидеров производства индустриального оборудования Rockwell Automation разработала подробную детализированную архитектуру Conwerged Plantwide Ethernet, описывающая все нюансы создания индустриальных сетей, включая и вопросы обеспечения их безопасности. В рамках этой архитектуры учтены и требования по отказоустойчивости, и ограничения со стороны построения топологий, и протоколы, используемые индустриальным оборудованием, и многие другие вопросы.

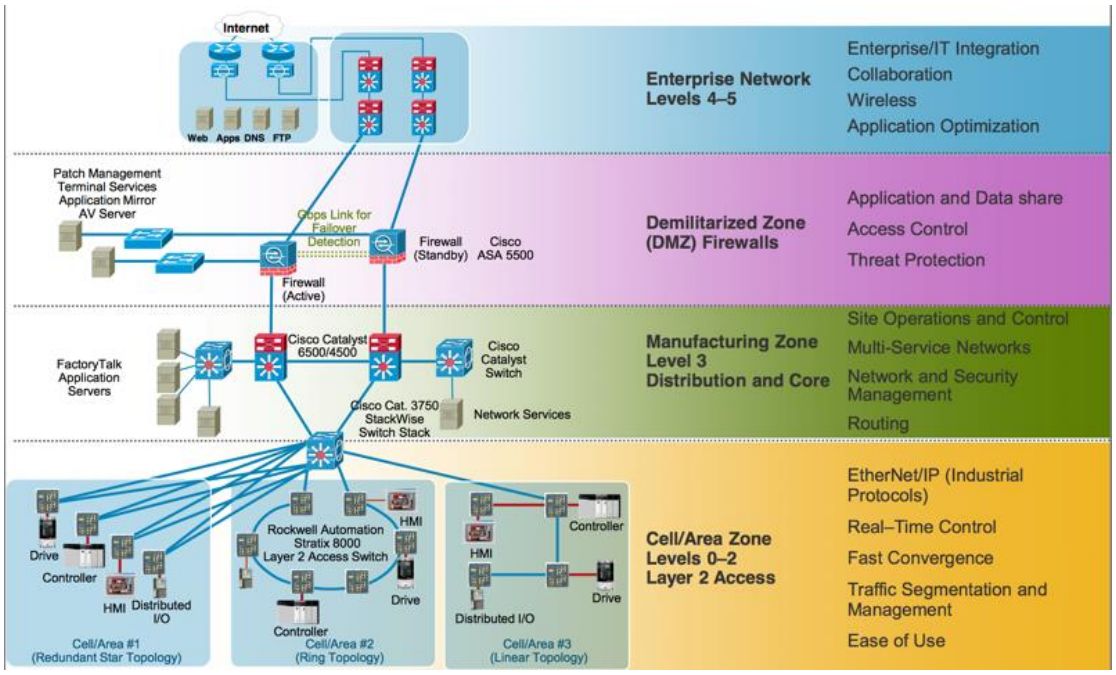

Рисунок 1. Уровни архитектуры Converged Plantwide Ethernet

Модель обеспечения безопасности, разработанная Cisco

Повышенное внимание к вопросам информационной безопасности АСУ ТП вызывается переходом индустриальных решений с проприетарных протоколов на TCP/IP и активным внедрением новых технологий (включая удаленный доступ и беспроводные решения) в процесс обработки и передачи управляющих команд, а также хранения диагностической и другой исторической информации. Проблемой являются также и изощренные, целенаправленные атаки, целью которых становится нарушение штатного режима функционирования технологических процессов, которое может привести даже к экологическим катастрофам и человеческим жертвам. При этом проблема заключается не столько в самих атаках, сколько в изменениях в самих сетях АСУ ТП, которые перестают быть физически изолированными от внешнего мира. Нередки случаи организации удаленного доступа к АСУ ТП со стороны подрядных организаций или для передачи информации в центры диспетчерского управления. Модель информационной безопасности, разработанная Cisco, ориентированная на широкий спектр различных угроз, позволяет обеспечить мониторинг и контроль АСУ ТП, а также защитить их от несанкционированных вмешательств любого типа на всех направлениях, причем постоянно, в любой момент времени.

Чтобы надежно защититься от всевозможных атак на всех направлениях, необходимо знать и понимать современную сетевую среду АСУ ТП, используемые в нем устройства (например, контроллеры и исполнительные устройства), а также применяемые индустриальные протоколы. Особенно важно осознавать цели защиты АСУ ТП, отличающиеся от аналогичных задач в корпоративных сетях. Не менее важно при создании комплексной системы защиты АСУ ТП понимать и анализировать образа мышления нападающих.

Портфель интегрированных решений Cisco выполняет эти задачи, обеспечивая небывалую прозрачность и непрерывную защиту от самых изощренных атак. Он позволяет государственным и коммерческим заказчикам и операторам АСУ ТП действовать более быстро и интеллектуально до атаки, во время атаки и после ее отражения. И при этом в полном соответствии с требованиями российского законодательства.
Решения Cisco по информационной безопасности позволяют выполнить многие из требований приказа ФСТЭК №31.

Требования	ASA-X / ASA-SM	NGFW	IPS / NGIPS / wIPS	AMP / FireAMP	ISE / TrustSec	ESA	WSA	CTD	AC	VSG / ASAv
Идентификация и аутентификация	+	+	+		+	+	+		+	
Управление доступом	+	+	+	+	+	+	+	+	+	
Ограничение программной среды										
Защита машинных носителей					+					
Регистрация событий безопасности	+	+	+	+	+	+	+	+	+	+
Антивирусная защита				+						
Обнаружение вторжений		+	+	+			+	+		
Анализ защищенности		+			+			+		
Обеспечение целостности		+	+	+		+	+			
Обеспечение доступности	Обеспечивается любым решением компании Cisco, в т.ч. и не относящимся к решениям по информационной безопасности									
Защита среды виртуализации		+	+	+	+			+		+
Защита технических средств										
Защита АСУ ТП	+	+	+	+	+	+	+	+	+	
Безопасная разработка	Обеспечивается с помощью подхода Cisco к безопасной разработке (CSDL)									
Управление обновлениями					+					
Планирование мероприятий										
Обеспечение действий в нештатных ситуациях										
Обучение пользователей										
Анализ угроз и рисков				+						
Управление инцидентами		+	+	+	+			+		
Управление конфигурацией	Обеспечивается системами управления сетью и информационной безопасностью									

Примечание:

ASA-X – Cisco ASA 5500-X (5512, 5515, 5525, 5545, 5555, 5585), а также IOS Firewall
ASA-SM – Cisco ASA Service Module для Catalyst 6500 / Catalyst 6800 / Catalyst 7600
NGFW – Cisco ASA NGFW, Cisco AVC, Sourcefire NGFW
IPS – Cisco IPS 4200/4300/4500, Cisco IOS IPS, Cisco IPS-AIM, Cisco AIP-IPS
NGIPS – Sourcefire NGIPS
wIPS – Cisco Wireless Adaptive IPS
AMP – Sourcefire Advanced Malware Protection
ISE – Cisco Identity Service Engine, включая Virtual ISE
ESA – Cisco E-mail Security Appliance, включая Virtual ESA
WSA – WSA – Cisco Web Security Appliance, включая Virtual WSA, а также Cisco Cloud Web Security
CTD – Cisco Cyber Threat Defense
AC – Cisco AnyConnect
VSG – Virtual Security Gateway
ASAv – Virtual ASA

Для централизованного управления решениями, указанными в таблице, используются системы Cisco Security Manager и FireSIGHT.

Специально для работы в индустриальных сетях компания Cisco разработала целый ряд отдельных решений, часть из которых может выполнять и защитные функции. К ним можно отнести:

- Индустриальный маршрутизатор IE3000, выполняющий функции межсетевого экрана (сертифицирован в ФСТЭК России).
- Специализированные маршрутизаторы и коммутаторы для интеллектуальных сетей электроэнергетики Cisco Smart Grid Router (CGR) и Cisco Smart Grid Switch (CGS), также выполняющие функции межсетевого экрана (сертифицированы в ФСТЭК России).
- Регулярно обновляемая специализированная система обнаружения и предотвращения вторжений Cisco IPS for SCADA, умеющая идентифицировать и нейтрализовать атаки на различные компоненты АСУ ТП большого числа производителей.
- Система предотвращения вторжений Sourcefire NGIPS, которая обладает двумя встроенными препроцессорами для обработки индустриальных протоколов ModBus и DNP3 и позволяющая обнаруживать свыше 170 атак на АСУ ТП более чем двадцати производителей.

В настоящий момент подразделение IoTG компании Cisco разрабатывает еще ряд решений в области безопасности индустриальных сетей и АСУ ТП.

Оценка соответствия средств защиты информации

В соответствие с 31-м приказом ФСТЭК заказчики АСУ ТП могут использовать любую из определенных законодательством о техническом регулировании форм оценки соответствия (их 7). Есть среди них и испытания, и приемка и ввод в эксплуатацию, и государственный контроль (надзор). Есть среди этих форм оценки соответствия и обязательная сертификация по требованиям ФСТЭК и ФСБ. Даже в случае выбора именно этой формы оценки соответствия, заказчикам компании Cisco беспокоиться не надо – почти весь спектр решений Cisco по защите информации сертифицирован по требованиям информационной безопасности. Общее число полученных решениями Cisco сертификатов превышает 550, что существенно превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на отечественном рынке информационной безопасности.
На начало 2014-го года компанией Cisco были получены сертификаты ФСТЭК и ФСБ на 124 линейки своего оборудования, включая:

- Многофункциональные средства защиты информации Cisco ASA 5500 (все модели), Cisco ASA 5500-X (все модели), сервисный модуль Cisco ASA-SM – по требованиям к межсетевым экранам 3-го и 4-го класса защищенности по схеме “серия”
- Системы предотвращения вторжений Cisco IPS 4200 (все модели), Cisco AIP-SSM, Cisco IDSM-2 – по техническим условиям по схеме “серия”
- Маршрутизаторы Cisco 800, 1800, 1900, 2600, 2800, 2900, 3600, 3800, 3900, 7200, 7300, 7600 – по требованиям к межсетевым экранам 3-го и 4-го класса защищенности по схеме «серия»
- Маршрутизаторы Cisco ASR1000, GSR 12000 – по требованиям к межсетевым экранам 3-го и 4-го класса защищенности
- Коммутаторы Cisco Catalyst 2912, 2924, 2948, 2950, 2960, 2970, 35xx, 37xx, 4000, 4500, 4900, 6000, 6500 – по требованиям к межсетевым экранам 3-го и 4-го класса защищенности по схеме “серия”
- Коммутаторы Cisco Nexus 1010, 5500, 7000 – по требованиям к межсетевым экранам 3-го и 4-го класса защищенности
- Маршрутизаторы и коммутаторы в индустриальном исполнении – Cisco CGR2000, CGS2500, IE-3000 по требованиям к межсетевым экранам 3-го и 4-го класса защищенности по схеме «серия»
- Межсетевые экраны следующего поколения Sourcefire NGFW - по требованиям к межсетевым экранам 3-го класса защищенности.

В настоящий момент на сертификацию поданы и в 2014-м году должны быть завершены работы по сертификации следующих решений Cisco:

- Системы предотвращения вторжений Cisco IPS 4300, 4500, AIP-SSM, IPS-SSP, Sourcefire NGIPS – по требованиям к системам предотвращения вторжений
- Индустриальные системы предотвращения вторжений Cisco IPS for SCADA

- Средства защиты виртуализированных сред – Cisco Virtual Security Gateway, Cisco UCS Fabric Interconnect, Cisco ASAv.

Компания Cisco рассматривает возможность сертификации и других своих решений по требованиям безопасности.
Помимо обязательной сертификации в ФСТЭК и ФСБ, многие решения Cisco проходили оценку соответствия в системе добровольной сертификации «ГАЗПРОМСЕРТ».

Участие Cisco в разработке нормативных требований по защите АСУ ТП

Помимо предложения эффективных технических решений по защите автоматизированных систем управления технологическими процессами, компания Cisco активно участвует и в нормотворческой деятельности по данному вопросу. В частности, сотрудники российского офиса Cisco:

- Участвуют в экспертизе и выработке предложений по изменению законопроектов в области защиты обеспечения безопасности критических информационных инфраструктур.
- Участвуют в работе Технического комитета №362 по вопросам стандартизации защиты информации при ФСТЭК России.
- Участвуют в экспертизе отраслевых стандартов и требований федеральных органов исполнительной власти по защите информации в АСУ ТП и иных индустриальных системах.

Заключение

Защита критических информационных инфраструктур и АСУ ТП – одна из приоритетных задач на сегодняшний день для служб информационной безопасности, работающих на критически важных объектах России. Ее важность определяется не только наличием статей в Уголовном и Трудовом Кодексах, а также Кодексе об административных правонарушениях, предусматривающих наказание за нарушение законодательства по защите информации. Влияет на важность данной темы и рост числа атак, направленных на нарушение доступности, целостности или конфиденциальности критических инфраструктур. Поэтому, в условиях всё большей зависимости граждан России от внедряемых во все сферы нашей жизни информационных технологий, небезопасное внедрение или управление которыми может повлечь за собой тяжелые последствия, мы должны уделять больше внимания защите информации, обрабатываемой в АСУ ТП.

Огромный многолетний опыт компании Cisco на рынке построения сетей любой сложности, включая сети критически важных объектов, и построения систем информационной безопасности, наличие широкого портфеля решений и уникальных технологий нам дают возможность предоставить проработанные и законченные решения по построения и защите сетей АСУ ТП. При этом Cisco, принимающая активное участие в разработке и экспертизе нормативных требований по этому вопросу, готова предложить решения, полностью соответствующие требованиям российских регуляторов.

Дополнительная информация

Отраслевые решения Cisco для промышленности - http://www.cisco.com/web/strategy/manufacturing/index.html
Решения Cisco для индустриальных сетей - http://www.cisco.com/c/en/us/solutions/enterprise-networks/industrial-networking/index.html
Решения Cisco для информатизации отрасли добычи полезных ископаемых - http://www.cisco.com/web/strategy/materials-mining/index.html
Решения Cisco для топливно-энергетического комплекса - http://www.cisco.com/web/strategy/energy/index.html
Решения Cisco для автомобильной промышленности - http://www.cisco.com/web/strategy/automotive/index.html
Решения Cisco для транспорта - http://www.cisco.com/web/strategy/transportation/index.html
Совместные решения Cisco и Rockwell Automation - http://www.cisco.com/web/strategy/manufacturing/cisco-rockwell_automation.html
Дизайн сетевой инфраструктуры АСУ ТП - http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG.html

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465

Cisco и логотип Cisco являются товарными знаками или зарегистрированными товарными знаками корпорации Cisco и/или ее дочерних компаний в США и других странах. Чтобы просмотреть список товарных знаков Cisco, перейдите по ссылке: www.cisco.com/go/trademarks. Товарные знаки сторонних организаций, упомянутые в настоящем документе, являются собственностью соответствующих владельцев. Использование слова «партнер» не подразумевает наличия партнерских взаимоотношений между Cisco и любой другой компанией. (1110R)