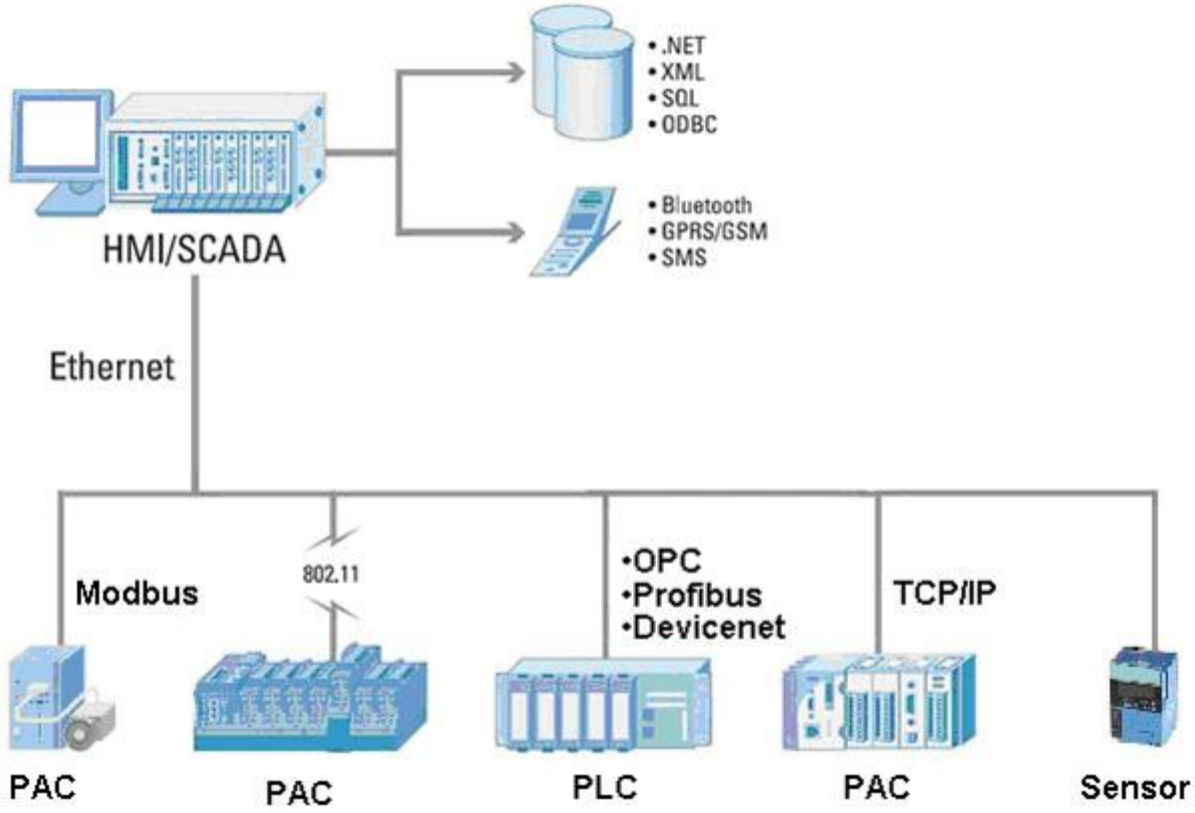
ЛЕКЦИЯ 10. УЯЗВИМОСТИ ТЕХНОЛОГИЙ АСУ ТП

10.1. Системы управления АСУТП

Автоматизированная система управления технологическим процессом (АСУ ТП) — комплекс программных и технических средств, предназначенный для автоматизации управления технологическим оборудованием на предприятиях. Большая часть этих систем была разработана в те годы, когда вопросы кибербезопасности имели низкий приоритет. Эти системы работали в изолированной среде, на базе индивидуального программного и аппаратного обеспечение, а так же устаревших коммуникационных технологий.

В отличие от старых систем, современные комплексы SCADA и АСУТП базируются на стандартных протоколах связи. Большинство контроллеров поддерживает адресные протоколы в IP среде. Стандартные операционные системы (Windows или UNIX) используется в операторских, которые в свою очередь имеют доступ к отдалённым системам контроля посредством частных каналов связи, предоставляемых телекоммуникационными компаниями.



В результате этого взаимодействия один из потенциальных доступов в систему обеспечивает сама коммуникационная сеть. Современные технологии кибератак ориентированы на обнаружение и использование различного рода узких мест в компонентах коммерческих системах. Способность операторов стратегических инфраструктур обнаружить возникающие угрозы и уязвимости в системе является необходимым условием для разработки эффективной стратегии безопасности и принятия контрмер.

10.2. Уязвимость в безопасности систем АСУ ТП

Системы SCADA и АСУТП обычно разрабатывались в соответствии с самыми жесткими международными требованиями в части безопасности. Тем не менее, уровень их безопасности уже не соответствует сегодняшним требованиям.

Подробный анализ потенциальных угроз и их возможных последствий вызывает ряд серьезных вопросов, касающихся безопасности и требующих решения следующих задач:

- связь с внешним миром;
- взаимозависимости;
- сложность;
- унаследованные системы;
- доступность системы;
- автономность;
- доступность информации.

Связь с внешним миром. Современные системы SCADA и АСУТП как правило связаны с корпоративными сетями, которые функционируют на базе стандартных операционных систем и имеют доступ в Интернет. Несмотря на то, что эти современные "удобства" повышают эффективность работы предприятия, они параллельно создают дополнительную уязвимость, так как не обеспечены требуемыми для промышленных систем контроля средствами безопасности.

Взаимозависимости. Из-за высокой степени взаимозависимости между секторами инфраструктуры, сбой в одном секторе может распространиться на другие секторы системы. Кибер - террористы могут воспользоваться этой взаимозависимостью для организации волны разрушений и таким образом увеличения общего экономического ущерба.

Сложность. Требования к контролю в режиме реального времени требует непрерывного доступа к системам большого количества пользователей, а также связи с корпоративными бизнес сетями. Различие в принципах построения систем ИТ и АСУТП, а также отсутствие понимания специалистами каждой из этих двух структур специфики второй технологии, приводят к проблемам в координации безопасности сетей между этими двумя ключевыми группами.

Унаследованные системы. Хотя старые системы АСУТП рассчитаны на работу в автономном режимы, они, как правило, не имеют структуры паролей и администрации безопасности. Более того, в этих системах не предусмотрены средства защиты протоколов, чем и обуславливается их уязвимость.

Доступность системы. Даже ограниченное подключение к Интернету подвергает АСУТП всем существующих угрозам взаимосвязанных компьютерных сетей, вирусов, червей, троянов, хакеров и кибер - террористов. Многочисленные каналы управления, использующие беспроводные или специально выделенные линии (VPN), проходящие по

коммерческим телекоммуникациям, также мало защищены от дублирования передаваемых данных. Эти вопросы особенно критичны в областях промышленности, расположенных на взаимосвязанных предприятиях и системах контроля имеющих удаленный доступ на территории или за её пределами.

Автономность. До сих пор не найдено приемлемой альтернативы вместо использования корпоративных сетей для вспомогательных модулей и подсистем (типа Архиваторов; серверов истории и Базы Данных). Зарубежные производители комплексов АСУТП не всегда считаются с государственными интересами тех стран, в которых используются их системы. Ещё одной проблемой являются договора технической поддержки дистрибьюторами и третьими лицами.

Доступность информации. Техническая Спецификация и Руководства по эксплуатации комплексов АСУТП являются общедоступными, в том числе и для хакеров, которые скачивают их из Интернета и используют для своей технической подготовки. Злоумышленники не обязаны быть экспертами в системах контроля, что бы нанести необратимый ущерб критическим инфраструктурам государства.

10.3. Статистика уязвимостей в элементах АСУ ТП

На сегодняшний момент существующие подходы к обеспечению информационной безопасности элементов АСУ ТП являются недостаточными в виду особенностей архитектуры и свойств программно-аппаратного обеспечения её элементов, что предоставляет злоумышленнику несколько векторов воздействия на технологические автоматизированные системы. С развитием информационных технологий и существенным усложнением архитектуры АСУ ТП появились множественные угрозы информационной безопасности, реализация которых со стороны злоумышленника может привести к катастрофическим последствиям.

В элементах АСУ ТП, составляющих её программно-аппаратную базу, были обнаружены множественные уязвимости, которые могут привести к нарушению корректной работы технологического процесса и реализации угроз несанкционированного доступа к информации, обрабатываемой в:

- системах диспетчерского управления и сбора данных (SCADA);
- отдельных интерфейсах управления объектами автоматизации;
- элементах телеметрической подсистемы и телемеханики;
- прикладных приложениях для анализа производственных и технологических данных;
- системах управления производством (MES-системы).

Использование традиционных информационных технологий в элементах АСУ ТП является одной из причин низкого уровня защищённости большинства из них. Данный фактор позволяет злоумышленнику апробировать существующие знания в отношении элементов АСУ ТП.

Таблица 10.1. Статистика обнаруженных уязвимостей в элементах АСУ ТП

Название продукта	Тип уязвимости	Описание уязвимости	Дополнения
DATAC RealWin 2.0 (система диспетчеризации)	Исполнение произвольного кода авторизированным пользователем	Переполнение стека при обработке специально сформированного FC_INFOTAG/SET_CONTROL пакета, направленного на приём в TCP-порт 910 удалённой	Дата обнаружения – 2008 год. Доступен полнофункциональный эксплуатирующий код.

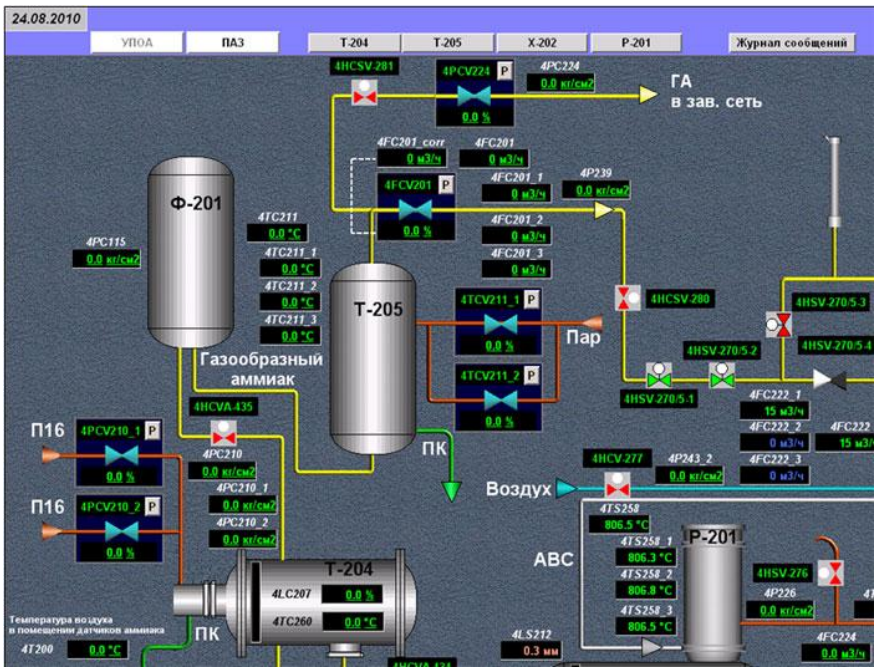
		системы	
GE Fanuc Proficy Information Portal 2.6 (WEB-приложения для анализа производственных данных)	Загрузка и исполнение произвольных файлов	Аутентифицированный пользователь может загрузить любой произвольный файл на сервер, используя сценарий «Add WebSource», в последствии исполнить его путём обращения к WEB-серверу. Данная уязвимость может привести к несанкционированному размещению на WEB-сервере программных «закладок» класса «WEB-shell»	Дата обнаружения – 2008 год. Уязвимость вызвана из-за небезопасного использования Java RMI вызова к указанному сценарию WEB-приложения, который позволяет задать имя файла и каталог, куда будет размещён файл.
ABB PCU400 4.4-4.6 (блок связи)	Неавторизированное исполнение произвольного кода	Удалённое переполнение буфера в модуле обработке протоколов IEC60870-5-101, IEC60870-5-104	Дата обнаружения – 2008 год. ABB PCU 400 является FEP-сервером системы диспетчеризации ABB SCADA, который отвечает за управление подсистемой телеметрических устройств.
GE Fanuc Cimplicity 6.1 (система диспетчеризации)	Неавторизированное исполнение произвольного кода	Удалённое переполнение кучи, которое может эксплуатироваться удалённым злоумышленником при доступности системы «из вне»	Дата обнаружения – 2008 год. На 2007-2008 год данный продукт был единственным, поддерживающим интеграцию с оборудованием ЧПУ семейства GE Fanuc.
AREVA e-terrahabitat (система диспетчеризации)	Множественные уязвимости, приводящие к отказу в обслуживании, повышению привилегий	Успешная эксплуатация уязвимости выводит из строя WEB-сервер WebFGServer, платформу NETIO. Повышение привилегий в среде WEB-сервера и приложения MLF	Дата обнаружения – 2009 год. Активно используется на малых объектах нефтегазового сектора.
OSISoft PI Server (OPC-сервер)	Раскрытие критичных данных для доступа к базе данных	Злоумышленник может раскрыть данные, передаваемые при аутентификации конечного клиента к базе	Дата обнаружения – 2009 год. Для устранения уязвимости рекомендуется

		данных	использовать IPSec между клиентами сети и PI Server
CitectSCADA (система диспетчеризации)	Неавторизированное исполнение произвольного кода	При наличии запущенного ODBC-сервера (TCP-порт 20222) удалённый злоумышленник может скомпрометировать целевую систему	Дата обнаружения – 2008 год. Для устранения уязвимости рекомендуется не использовать службу ODBC
Контроллеры Rockwell Automation (Allen Bradley) Micrologix 1100/1400 (удалённый терминал)	Отказ в обслуживании, несанкционированный доступ с возможностью повышения привилегий	Множественные уязвимости, приводящие к возможности несанкционированной модификации PLC, опознания сторонних устройств	Дата обнаружения – 2010 год. Контроллеры Micrologix являются одной из самой распространённых платформ для систем управления с программируемой логикой
WonderWare SiteLink version 2.0, WonderWare InTouch version 8.0 (система диспетчеризации)	Отказ в обслуживании	Эксплуатация уязвимости приводит к внештатному нарушению корректной работы системы и её отключению.	Дата обнаружения – 2008 год. На данный момент доступна 10 версия системы. Системы Intouch являются одними из самых распространённых систем SCADA в США.
Siemens WinCC	Ошибка конфигурации	При изменении пароля в приложениях WinCCAdmin/WinCCConnect дальнейшая работа с базой данных MSSQL становится недоступной, проект технологического процесса будет удалён и в последствии станет недоступен	Модераторы технического сообщества SIEMENS признали данный факт, разработанные ими рекомендации направлены на сохранение штатного пароля в неизменном виде.
TF3400	Ошибка конфигурации	Возможность удаления технологического проекта в обход привилегий супервайзера	Производитель уведомлён о наличии уязвимости.
Контроллеры TF3000	Ошибка конфигурации	Возможность неавторизированного съема информации о запущенных процессах в ОС контроллера	Производитель уведомлён о наличии уязвимости. Исправление уязвимости на

			данный момент отсутствует.
Netbiter® webSCADA	Множественные уязвимости безопасности	Возможность локального чтения файлов (класс «Local File Disclosure»), неавторизированное снятие данных об имеюшихся в системе пользователях, возможность загрузки злонамеренного кода («web-shell) для выполнения неавторизированного кода на сервере.	Производитель уведомлён о наличии уязвимости ([STANKOINFORMZASCHITA-10-01] Netbiter® webSCADA – множественные уязвимости - http://itdefence.ru/content/advisory/scada/10_01/). Исправление уязвимости на данный момент отсутствует.
ITS SCADA	SQL-инъекция в модуле авторизации пользователя для доступа в систему	Возможность неавторизированного чтения таблиц «RTUinfo», «Alarms», «BMWInfo», «dtproperties», «FlowData», «LSHistory», «Users» и др., раскрытие информации.	Производитель уведомлён о наличии уязвимости ([STANKOINFORMZASCHITA-10-02] ITS SCADA – Обход авторизации - http://itdefence.ru/content/advisory/scada/10_02/). Исправление уязвимости на данный момент отсутствует.
Broadwin SCADA	Blind SQL-инъекция в модуле авторизации пользователя для доступа в систему	Возможность неавторизированного чтения таблиц «bwdb_access», «bwdbbackup_excel», «bwdbexport_excel», «bwdnode_access», «bwpdata_access» и др. , раскрытие информации для последующей компрометации системы.	Производитель уведомлён о наличии уязвимости ([STANKOINFORMZASCHITA-10-03] Broadwin SCADA - Blind SQL-injection - http://itdefence.ru/content/advisory/scada/10_03/). Исправление уязвимости на данный момент отсутствует.
ICSCADA (Outlaw Automation)	Blind SQL-инъекция в модуле авторизации пользователя для	Возможность неавторизированного чтения данных, содержащих информацию	Используется в области газодобывающей промышленности.

	доступа в систему	об авторизации пользователей. Системой ведётся логирования действий пользователей, что может способствовать своевременному обнаружению злоумышленника.	Производитель уведомлён о наличии уязвимости ([STANKOINFORM ZASCHITA-10-04] ICSCADA (Outlaw Automation) – Blind SQL-injection - http://itdefence.ru/content/advisory/scada/10_04/). Исправление уязвимости на данный момент отсутствует.
InduSoft SCADA	Обход директорий в WEB-сервере CET системы SCADA (Indusoft Web Studio)	Возможность неавторизированного чтения файлов путём обхода ограничений на просмотр файлов директорий и их содержимого путём специально сформированного GET-запроса.	Производитель уведомлён о наличии уязвимости (подробности уязвимости пока не афишированы). Исправление уязвимости на данный момент отсутствует.

Реализация некоторых из перечисленных уязвимостей позволяет остановить технологический процесс, что может негативно отразиться на ходе его отдельных потоков и привести к аварийной ситуации:



Результат неавторизированного удаления проекта технологического процесса – обнуление показателей оборудования цеха химического завода по производству аммиака

Кроме специфических уязвимостей, которые напрямую относятся к элементной базе АСУ ТП, следует так же выделить возможность эксплуатации брешей в известных службах и сервисах, сетевых протоколах, платформах, которые используют данные элементы.

10.4. Доступность сведений для эксплуатации уязвимостей АСУ ТП

Одним из критериев, существенно влияющих на возможность эксплуатации уязвимостей, является доступность сведений о ней злоумышленнику. В настоящий момент 35% из числа всех приведённых уязвимостей имеют доступный функциональный код эксплуатации, включённый в состав свободно распространяемых программных пакетов для анализа защищённости и проведения тестов на проникновение.

Таблица 10.2. Эксплуатирующий код в составе свободно распространяющихся пакетов

Программный продукт	Тип уязвимости	Включение в состав	Ограничения
CitectSCADA	Неавторизированное исполнение кода	Metasploit Project	«Эксплоит» доступен под платформы Windows XP SP2/SP3, Windows 98 SE, Windows 2003 Server SP1
Wonderware Suitelink 2.0	Отказ в обслуживании	Metasploit Project	Требует наличие открытого TCP-порта 5413
RealWin SCADA Server 2.0	Неавторизированное исполнение кода	Metasploit Project	«Эксплоит» доступен под платформы Windows XP SP2 (EN/ES), Windows 2000 SP4 (EN/ES)
GE Fanuc Real Time Information Portal 2.6	Неавторизированное изменение данных	Metasploit Project	Отсутствуют, существует отдельный «эксплоит» на языке Python

Таблица 10.3. Примеры эксплуатирующего кода в составе коммерчески распространяемых пакетов

Программный продукт	Тип уязвимости	Включение в состав
Modicon PLC	Использование паролей по умолчанию	Nessus (Tenable), SCADA-Аудитор (НТЦ “Станкоинформзащита»)
Modicon PLC HTTP Server	Использование паролей по умолчанию	Nessus (Teenable), SCADA-Аудитор
Sisco OSI	Отказ в обслуживании	Nessus (Teenable), SCADA-Аудитор
Netbiter	Неавторизированное	Nessus (Teenable),

	исполнение кода	SCADA-Аудитор
Automated Solutions Modbus TCP Slave	Переполнение кучи в ActiveX-компоненте	Nessus (Teenable), SCADA-Аудитор
Livedata	Неавторизированное исполнение кода	Nessus (Teenable), SCADA-Аудитор
Takebishi Electric DeviceXPlorer OPC Server	Неавторизированное исполнение кода	Nessus (Teenable), SCADA-Аудитор
Iconics DlgWrapper	Переполнение буфера в ActiveX-компоненте	Nessus (Teenable), SCADA-Аудитор
TF3400	Обход авторизации	SCADA-Аудитор

Все из перечисленных уязвимостей на сегодняшний день имеют обновления безопасности, поэтому использование данных средств может использоваться исключительно для аудита безопасности автоматизированных систем, но никак не для реального проникновения.

10.5. Распространение специального злонамеренного кода в секторе АСУ ТП

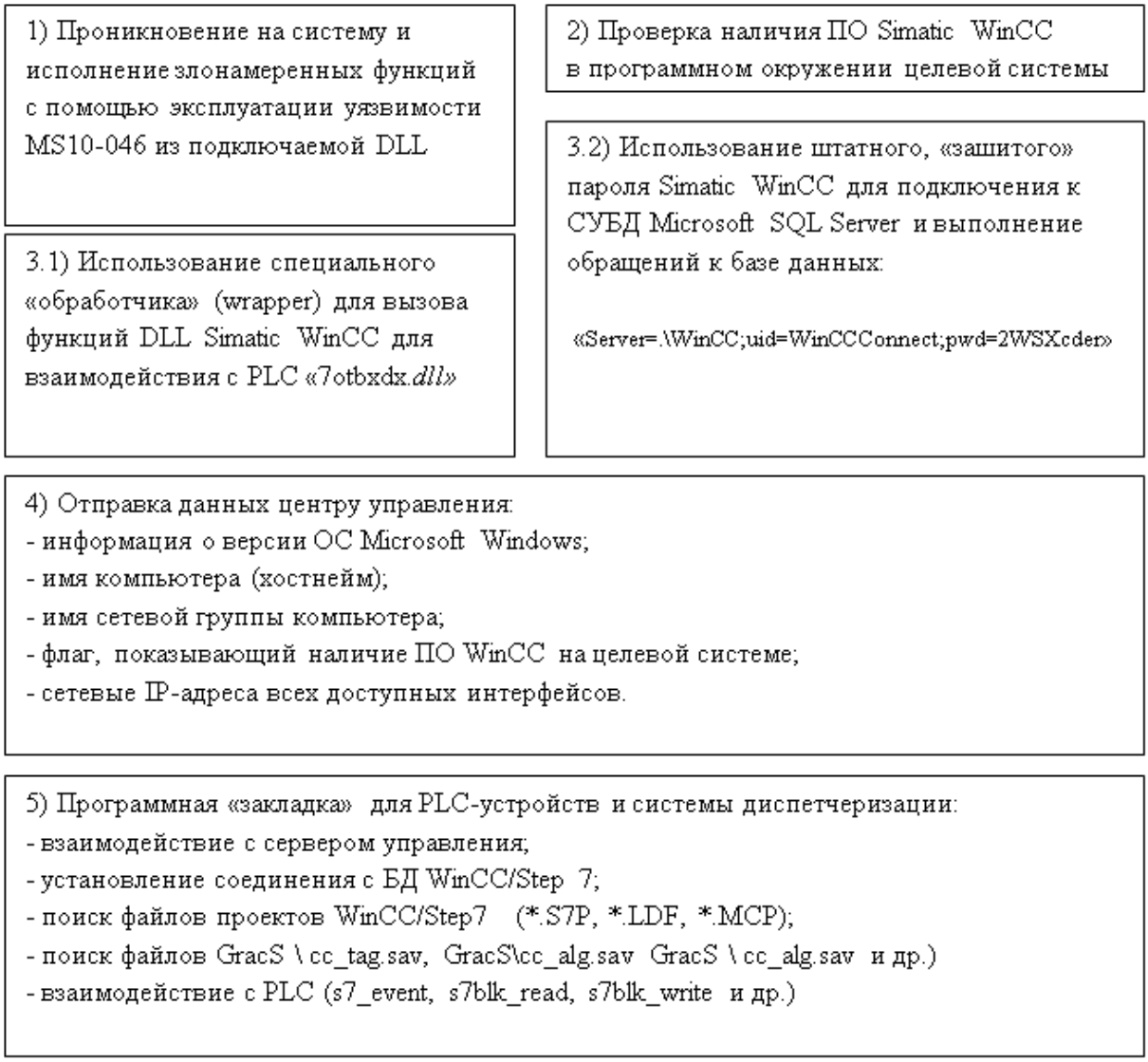
Отдельной угрозой, частично использующей штатные методы для исполнения, является распространение злонамеренного кода для кражи критически важных данных о проектах технологических процессов и нарушения их корректной работы, подтверждение чему является факт распространения вредоносного кода «Rootkit.TmpHider» и «Scope.Rookit.TmpHider.2».

Многие популярные системы диспетчеризации (SCADA) базируются на платформе ОС Microsoft Windows, поэтому данный факт указывает на необходимость обеспечения информационной безопасности операционной системы, на которую устанавливается прикладное программное обеспечение.

Названные образцы вредоносного кода использовали уязвимость MS10-046 (http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx) в Windows Shell, позволяющей неавторизированно исполнить произвольный код с помощью отображения специально сформированного ярлыка оболочки ОС Microsoft Windows.

Основным методом распространения являлось применение отделяемых носителей (USB-flash, Compact-Flash, сторонние съёмные носители информации), которые могут использовать Операторы для управления проектами технологических процессов, обмена информацией между собой.

В качестве полезной нагрузки зловреды использовали сценарий для СУБД MSSQL, с которой может быть сопряжена среда Simatic WinCC/STEP7 и модифицированную подключаемую библиотеку, в которой содержались основные функции для работы с PLC:



10.6. Статистика инцидентов информационной безопасности сектора АСУ ТП

Анализ повышения интереса независимых исследователей был существенно высок в период 2008 года. Практически из всех известных общественности уязвимостей были обнаружены в это время, наибольший рост появления сводок о безопасности компонентов АСУ ТП был зафиксирован в период с марта по сентябрь. Данный факт сопровождался появлением соответствующих инцидентов безопасности данной области.

Таблица 10.4. Инциденты информационной безопасности (2008-2010) сектора АСУ ТП

Объект	Инцидент	Дата
Блок 2 ядерной станции «Hatch» (штат Джорджиа, США)	Внештатное аварийное выключение на 48 часов после установки обновления программного обеспечения (похожий инцидент случился в 2006 году на ядерной станции «Browns Ferry» из-за	7 марта 2008 года

	нештатного сбоя программируемого логического контроллера при получении аномального выходного сетевого трафика из производственной сети)	
Корпорация Tennessee Valley Authority (TVA) (в ведомости данной энергетической корпорации находятся 11 угольных станций, 8 ТЭС, 3 ядерных станции, 29 ГЭС США)	Проверка регуляторов (GAO, HHS) выявила порядка 2000 уязвимостей разной степени критичности. Среди брешей в безопасности были выявлены сегменты производственной сети, подключённые к Интернет, множественные уязвимости прикладного ПО, отсутствие обновлений безопасности, ошибки в проектировании архитектуры сети и каналов обмена данными	май 2008 года
Центр полётного планирования Федерального управления гражданской авиации США	Диспетчерские трех десятков американских аэропортов выведены из строя в результате компьютерного сбоя в центре полётного планирования.	26 августа 2008 года
Газодобывающие компании США (Marathon Oil, ExxonMobil, ConocoPhillips)	Силовыми структурами США зафиксированы многочисленные проникновения в АС ведущих газодобывающих компаний.	май 2008 года
Сбой движения поездов немецких железных дорог (DB)	Компьютерный сбой привёл в приостановке системы бронирования и продажи билетов, диспетчеризация движения поездов осуществлялась «ручным» образом	14 января 2009
Электроэнергетическая сеть США	Силовыми структурами США зафиксировано проникновение в электроэнергетическую сеть и размещения в ней программных «закладок», направленных на внештатный останов её функциональных элементов	апрель 2009 года

	и нарушение корректной работы	
Энергетическая компания LCRA (Lower Colorado River Authority)	Специалистами LCRA зафиксировано свыше 4800 попыток получения доступа к их компьютерной системе. В настоящее время LCRA обслуживает более 1 миллиона людей в штате Техас.	5 апреля 2010 года