1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації

Сергей Гончар, Геннадий Леоненко, Алексей Юдин
ГосНИИ Спецсвязи

УДК 004.056.5

АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ ИНДУСТРИАЛЬНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Аннотация: **На основании рекомендаций NISTIR 800-82 (Guide to Industrial Control Systems (ICS) Security) рассматриваются особенности угроз и уязвимостей индустриальных автоматизированных систем управления.**
Summary: **Based on the recommendations of NISTIR 800-82 (Guide to the Industrial Control Systems (ICS) Security) are considered features of the threats and vulnerabilities for industrial control systems.**
Ключевые слова: **Угрозы, уязвимости, индустриальные автоматизированные системы управления.**

I Введение

В настоящее время индустриальные автоматизированные системы управления (ИАСУ), которые включают системы диспетчерского управления и сбора данных (SCADA), системы распределенного управления и другие конфигурации систем управления, используются в отраслях, жизненно важных для инфраструктуры государства. И если изначально ИАСУ были в виде отдельных компьютеров с собственными операционными системами и сетями, то на сегодняшний день происходит их интеграция с корпоративными системами и другими бизнес-приложениями через различные системы связи, включая Интернет.

Процесс интеграции позволяет обеспечивать управление производственной деятельностью в режиме реального времени, осуществлять дистанционный мониторинг систем управления технологическим процессом, повысить безопасность предприятия и персонала, снизить расходы на эксплуатацию. Однако ценой этих преимуществ является постоянно возрастающая уязвимость к угрозам. Для понимания актуальности проблемы приведем некоторые данные по уязвимостям ИАСУ (рис. 1 - 3) [1].

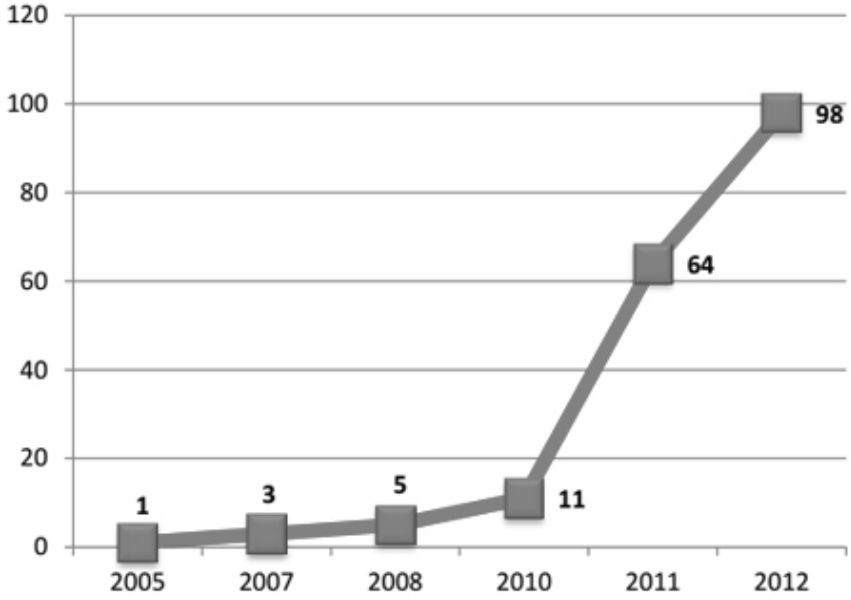

Рисунок 1 – Динамика количества уязвимостей в ИАСУ

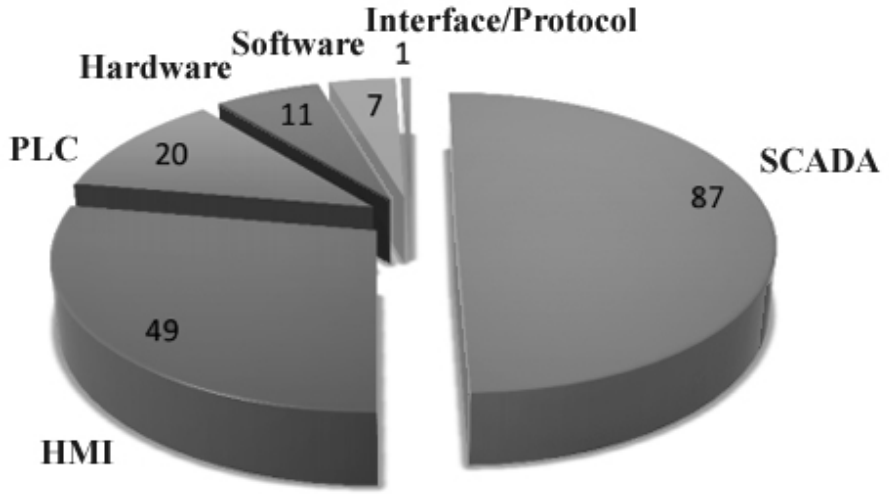

Рисунок 2 – Количество уязвимостей в различных типах компонентов ИАСУ

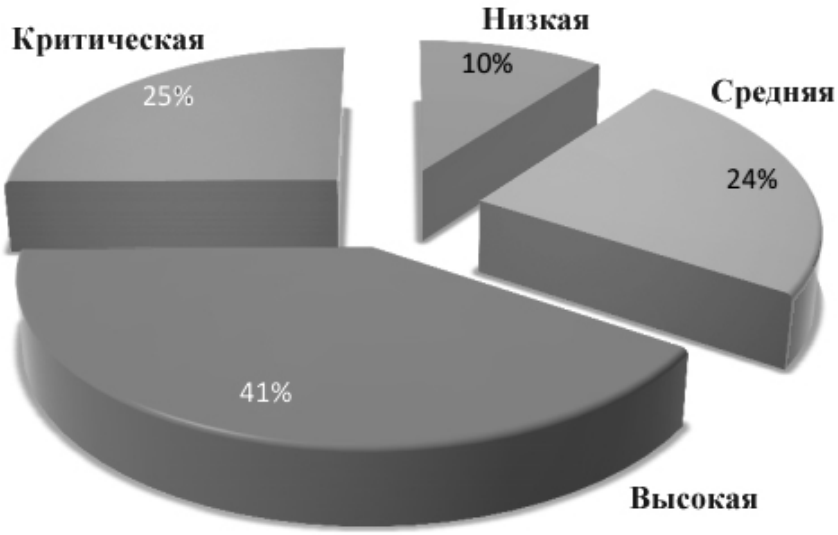

Рисунок 3 – Распределение уязвимостей ИАСУ по степени риска

Таким образом, непрерывный анализ угроз и уязвимостей ИАСУ становится важной необходимостью для своевременного совершенствования систем защиты.

II Угрозы ИАСУ

Угрозы для ИАСУ могут исходить из различных источников: умышленных (террористические группы, промышленные шпионы, недовольные сотрудники, злоумышленники), непреднамеренных (сложность системы, человеческие ошибки, аварии, отказы оборудования), природных (стихийные бедствия, климатические условия и т. п.) [2, 3]. Дадим более детальное описание групп, входящим в категорию умышленных угроз.

1. Злоумышленники. Зачастую хакеры взламывают сети для остроты ощущений в духе соревнований или для хвастовства среди коллег. Ранее удаленный взлом требовал изрядных компьютерных знаний и навыков, а теперь злоумышленники могут загрузить сценарии атаки и протоколы из Интернета. Таким образом, в то время как инструменты атаки стали более сложными, они также стали более доступными.

2. Операторы ботнета. Ботнет – компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами (автономным программным обеспечением). Чаще всего, бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера. Обычно ботнеты используются для

ISSN 2074-9481
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (26), 2013 р.

нелегальной или преступной деятельности: рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

3. Преступные группы. Преступные группы стремятся атаковать системы для получения денежной выгоды с помощью спама, фишинга, шпионских программ для совершения кражи и мошенничества в Интернете.

4. Иностранные спецслужбы. Иностранные спецслужбы используют киберсредства как часть их шпионской деятельности, направленной на сбор информации или для проведения операций в рамках информационных воздействий на противника.

5. Инсайдеры. Недовольные инсайдеры являются основным источником компьютерной преступности. Инсайдерам не нужно иметь много специальных знаний о кибератаках, потому что возможности, которыми они обладают находясь внутри системы, часто позволяют им получить неограниченный доступ к системе, а также осуществить ее повреждение или кражу данных. Еще инсайдерские угрозы представляют сторонние поставщики оборудования и программ, а также сотрудники, которые неумышленно внедряют вредоносные программы в системе. Инсайдерами могут быть работники, подрядчики, партнеры по бизнесу.

6. Фишеры. Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Данная угроза реализуется путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов. В письме содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с переадресацией. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль.

7. Сниффинг. Сниффинг – распространённый вид атаки, когда все пакеты, полученные сетевой картой, пересылаются на обработку специальному приложению, называемому снифферо̀м. В результате злоумышленник может получить большое количество служебной информации: кто, откуда и куда передавал пакеты, через какие адреса эти пакеты проходили. Самой большой опасностью такой атаки является получение самой информации, например логинов и паролей сотрудников, которые можно использовать для незаконного проникновения в систему под видом обычного сотрудника компании.

8. Спамеры. Спам – рассылка рекламы или иных видов сообщений лицам, не выражавшим желания их получать.

9. Авторы шпионских и вредоносных программ. Лица или организации, которые со злым умыслом проводят атаки на пользователей путем написания и распространения шпионского и вредоносного программного обеспечения.

10. Террористы. Террористы ставят перед собой цель уничтожить, вывести из эксплуатации критически важные объекты инфраструктуры, создать угрозу национальной безопасности, вызывать массовые жертвы, ослабить экономику страны, нанести ущерб общественной морали. Террористы могут атаковать одну цель, чтобы отвлечь внимание и ресурсы от других целей.

11. Промышленные шпионы. Целью шпионажа может стать компрометация информации или ее кража с последующим деструктивным использованием до полной остановки и банкротства промышленного объекта.

III Уязвимости ИАСУ

Уязвимостью является недостаток или слабое место информационной системы, системы безопасности, процедур внутреннего контроля, которые могут быть использованы для нарушения целостности или доступности системы и ее корректной работы. Анализ уязвимостей индустриальных автоматизированных систем управления дает возможность провести их структуризацию (рис. 4).

Рассмотрим более подробно уязвимости ИАСУ [2].

1. Уязвимости политик и процедур. К этой категории можно отнести:

- несоответствие или отсутствие политики безопасности;
- несоответствие или отсутствие процедур безопасности (должны быть разработаны конкретные процедуры безопасности и обучен соответствующий персонал);
- отсутствие повышения квалификации персонала в области безопасности;
- несоответствие архитектуры безопасности;
- несоответствие или отсутствие руководства по внедрению оборудования;
- отсутствие ответственности за документальное администрирование политик и процедур безопасности;
- отсутствие или недостаток аудитов в области безопасности;
- отсутствие конкретного плана аварийного восстановления системы в случае сбоя или аварии (план должен быть готов, апробирован и доступен в случае возникновения аппаратного или программного сбоя во избежание простоя и потери производства);

- отсутствие изменений конфигурации управления (должно осуществляться управление модификациями аппаратных средств, программируемого оборудования, программного обеспечения, чтобы гарантированно защитить систему от несоответствующих или неправомерных модификаций до, во время, и после внедрения системы).

Анализ показывает, что уязвимости политик и процедур в ИАСУ возникают из-за отсутствия или неполной, неадекватной документации в области безопасности, в том числе политик и руководства по внедрению (процедур), администрированию аудиту, восстановлению.

Рисунок 4 – Структура уязвимостей индустриальных автоматизированных систем управления

2. Уязвимости платформ. К данной категории можно отнести:

2.1. конфигурация:

- программное обеспечение не обновляется до выявления уязвимостей (из-за сложности программного обеспечения ИАСУ изменения должны пройти комплексное тестирование, что занимает определенное время и обеспечивает уязвимость для угроз);
- операционная система и приложения безопасности внедряются и обновляются без тщательных испытаний (должны быть разработаны документированные процедуры для тестирования новых приложений безопасности);

- параметры конфигурации используются по умолчанию (это часто приводит к небезопасному открытию портов других служб и выполнению нежелательных приложений);
- не сохраняются критические конфигурации системы (для поддержания доступности системы и предотвращения потери данных должны быть разработаны документированные процедуры для восстановления параметров конфигурации в случае случайного или злоумышленного изменения в конфигурации);
- хранение незащищенных конфиденциальных данных (например, пароли) на портативных устройствах (эти устройства могут быть утеряны или украдены и безопасность системы может быть нарушена);
- отсутствие адекватной политики паролей (когда пароли должны быть использованы, насколько стойкими они должны быть и как они должны храниться);
- отсутствие пароля (пароли должны быть реализованы для предотвращения несанкционированного доступа - для входа в систему (если в системе есть учетные записи пользователей), при включении питания (если в системе нет учетных записей пользователей), при выходе и режима заставки);
- раскрытие паролей (примерами могут быть совместное использование паролей для разных учетных записей пользователей, сообщение паролей посторонним, передача паролей в незашифрованном виде через незащищенные подключения);
- подбор пароля (плохо подобранный пароль может быть легко разгадан злоумышленником или компьютерной программой для получения несанкционированного доступа);
- неадекватность контроля доступа (неправильно настроенный контроль доступа может разрешить оператору действия администратора или запретить оператору корректирующие действия в аварийной ситуации);

2.2. оборудование:

- несоответствующее тестирование изменений системы безопасности;
- недостаточный уровень физической защиты критически важных систем;
- несанкционированный физический доступ посторонних лиц к оборудованию;
- незащищенный удаленный доступ к компонентам ИАСУ;
- двойные сетевые карты для соединения сетей (при подключении к разным сетям возможен несанкционированный доступ из одной сети в другую);
- отсутствие документирования активов (отсутствие точного списка активов в системе может оставить несанкционированные точки доступа);
- радиочастотный и электромагнитный импульс (последствия воздействия могут быть от временного нарушения управления до повреждения печатных плат);
- отсутствие резервного электропитания;
- потеря контроля окружающей среды системы (потеря контроля окружающей среды процессоров может привести к перегреву и повреждению или работе с ошибками);
- отсутствие резервирования критически важных компонентов;

2.3. программное обеспечение:

- переполнение буфера (может вызывать аварийное завершение или зависание программы, ведущее к отказу обслуживания; отдельные виды переполнений, например переполнение в стековом кадре, позволяют злоумышленнику загрузить и выполнить произвольный машинный код от имени программы и с правами учетной записи, от которой она выполняется);
- не включены или идентифицируются, как отключенные возможности безопасности, которые были установлены с программным продуктом;
- отказ в обслуживании;
- неправильная обработка неопределенных, плохо определенных, или "недопустимых" условий (некоторые реализации систем уязвимы для пакетов, которые искажены или содержат "недопустимые" значения полей);
- использование незащищенных отраслевых протоколов передачи данных;
- передача сообщений в незащищенном виде;
- запуск избыточных сервисов, т. е. тех служб, которые не используются для решения поставленных задач;
- использование проприетарного программного обеспечения, которое было предметом обсуждения на конференциях и в периодических печатных изданиях;
- недостаточная проверка подлинности и контроля доступа для конфигурирования и перепрограммирования;
- не установлено программное обеспечение обнаружения/предотвращения несанкционированного проникновения;

- не поддерживается протоколирование работы всех служб и сервисов;
- не регистрируются инциденты;

2.4. вредоносное программное обеспечение:

- не установлена защита от вредоносного программного обеспечения;
- защита от вредоносного программного обеспечения не актуальна, т. е. не обновляется или обновляется редко;
- защита от вредоносного программного обеспечения внедрена без проведения тщательных испытаний.

Как видим, уязвимости платформ в ИАСУ могут возникать из-за недостатков, ошибок, или некачественного обслуживания своих платформ, в том числе оборудования (аппаратных средств), операционных систем и приложений, отсутствие контроля физического доступа.

3. Уязвимости сети. К данной категории может быть отнесены:

3.1. конфигурация сети:

- несоответствие архитектуры сетевой безопасности;
- отсутствие контроля потока данных;
- некачественно настроенные параметры безопасности оборудования;
- отсутствие резервирования конфигурации сетевого устройства;
- передача паролей в незащищенном виде;
- недостаточно частая смена паролей доступа к сетевым устройствам;
- неадекватность контроля доступа к сетевым устройствам;

3.2. сетевое оборудование:

- недостаточный уровень физической защиты сетевого оборудования;
- несанкционированный доступ к портам сетевого оборудования;
- отсутствие избыточности для критически важных сегментов сети;

3.3. периметр сети:

- не определен периметр безопасности;
- отсутствует или неправильно настроен межсетевой экран;
- сети управления используются для трафика других типов;
- управление сетевыми сервисами сети ИАСУ реализуется в сети IT (сеть ИАСУ становится зависимой от сети IT, у которой нет необходимого приоритета надежности и доступности);

3.4. мониторинг сети:

- неадекватные журналы межсетевого экрана (количество контролируемых параметров не достаточно для проведения анализа инцидентов);
- отсутствие регулярного мониторинга безопасности в сети;

3.5. соединения:

- не идентифицируются критические пути контроля и управления;
- используются стандартные протоколы связи;
- отсутствует или недостаточна аутентификация пользователей, данных или устройств;
- отсутствует проверки целостности соединений;

3.6. беспроводные сети:

- несоответствие аутентификации между беспроводными клиентами и точками доступа;
- несоответствующая защита данных между беспроводными клиентами и точками доступа.

Анализ показывает, что уязвимости сети в ИАСУ могут возникать из-за недостатков, ошибок, или плохого администрирования сетей ИАСУ и их соединений с другими сетями. Эти уязвимости могут быть устранены или нивелированы с помощью правильного проектирования сети, шифрования сетевых соединений, обеспечения контроля физического доступа к сетевым компонентам.

IV Выводы

Проведенный анализ угроз и уязвимостей индустриальных автоматизированных систем управления дает представление о возможных рисках для данных систем, позволяет сформулировать требования и ограничения по применению возможных мер, методов и средств защиты информации при создании комплексных систем защиты информации.

Список использованной литературы: ***1.*** *Грицай Г., Тиморин А., Гольцев Ю., Ильин Р. Безопасность промышленных систем в цифрах – М.: Positive Technologies, 2012.* ***2****. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. – Recommendations of the National Institute of Standards and Technology.* ***3.*** *Industrial communication networks – Network and system security: IEC 62443. – Part 1-1: Terminology, concept*