УДК 621.039:004.9

А. А. Симонов, А. Л. Клевцов, С. А. Трубчанинов

Государственный научно-технический центр по ядерной и радиационной безопасности, г. Киев, Украина

Компьютерная безопасность информационных и управляющих систем АЭС: меры защиты от компьютерных угроз

Рассмотрены основные принципы и методы защиты от компьютерных угроз, методология, используемая для обеспечения компьютерной безопасности, политика, план и программа обеспечения компьютерной безопасности. Даны рекомендации по применению в Украине мер защиты от компьютерных угроз в зависимости от степени компьютерной безопасности. Проведен анализ различных подходов к обеспечению компьютерной безопасности в документах Международного агентства по атомной энергии, Комиссии ядерного регулирования США и Международной электротехнической комиссии.

Ключевые слова: компьютерная безопасность, информационная и управляющая система, компьютерная угроза, мера защиты, глубокоэшелонированная защита, политика в области обеспечения компьютерной безопасности, план обеспечения компьютерной безопасности, программа обеспечения компьютерной безопасности, степень компьютерной безопасности.

А. А. Симонов, О. Л. Клевцов, С. О. Трубчанінов

Комп'ютерна безпека інформаційних та керуючих систем АЕС: заходи захисту від комп'ютерних загроз

Розглянуто основні принципи та методи захисту від комп'ютерних загроз, методологія, яка використовується для забезпечення комп'ютерної безпеки, політика, план і програма забезпечення комп'ютерної безпеки. Дано рекомендації щодо застосування в Україні заходів захисту від комп'ютерних загроз залежно від ступеня комп'ютерної безпеки. Проведено аналіз різних підходів до забезпечення комп'ютерної безпеки в документах Міжнародного агентства з атомної енергії, Комісії ядерного регулювання США та Міжнародної електротехнічної комісії.

Ключові слова: комп'ютерна безпека, інформаційна та керуюча система, комп'ютерна загроза, захід захисту, глибокоешелонований захист, політика в сфері забезпечення комп'ютерної безпеки, план забезпечення комп'ютерної безпеки, програма забезпечення комп'ютерної безпеки, ступінь комп'ютерної безпеки.

Данная статья продолжает цикл публикаций [1, 2, 3] по компьютерной безопасности информационных и управляющих систем (ИУС) АЭС в журнале «Ядерна та радіаційна безпека». Анализ потенциальных кибернетических угроз на стадиях разработки и эксплуатации ИУС АЭС представлен в [1]. Обзор нормативных документов Международного агентства по атомной энергии (МАГАТЭ), Комиссии ядерного регулирования США (КЯР США) и Международной электротехнической комиссии (МЭК) по компьютерной безопасности ядерных установок (ЯУ) приведен в [2]. Требования, установленные в этих документах, зависят от принятой категоризации систем по компьютерной безопасности, которая детально рассмотрена в [3].

Цель данной статьи — проанализировать описанные в документах МАГАТЭ, КЯР США и МЭК меры защиты от компьютерных угроз и предложить соответствующие меры защиты от компьютерных угроз, которые целесообразно учитывать при разработке нормативного документа Украины по компьютерной безопасности ИУС АЭС.

Отметим, что устанавливать минимальные стандарты приемлемого риска или описывать в нормативных документах конкретный набор мер защиты от компьютерных угроз и смягчения последствий кибернетических атак не представляется возможным, так как любой набор конкретных стандартов быстро устаревает из-за развития информационных технологий, модернизации цифровых систем, появления новых угроз, разработки новых инструментальных средств защиты и изменения регулирующих требований. Поэтому целесообразно рассматривать только комплекс методологических рекомендаций общего характера по обеспечению защиты от компьютерных угроз.

Глубокоэшелонированная защита. В документе МАГАТЭ [4] указано, что основным принципом защиты от компьютерных угроз является использование глубокоэшелонированной защиты — концепции нескольких последовательных эшелонов и методов защиты. Отмечено, что глубокоэшелонированная защита обеспечивается сочетанием ряда последовательных независимых уровней защиты, только после отказа или выхода из строя которых компьютерная система может подвергнуться вредоносному воздействию. Если происходит отказ одного уровня защиты или преодоление одного барьера, имеются последующие уровни или барьеры. При надлежащей организации глубокоэшелонированной защиты единичный технический, человеческий или организационный отказ не может привести к вредоносному воздействию на компьютерную систему, а сочетания отказов, способные привести к компьютерному инциденту, маловероятны. Независимая эффективность разных уровней защиты — это необходимый элемент глубокоэшелонированной защиты.

В документах КЯР США [5] и МЭК [6] глубокоэшелонированная защита также указана в качестве основной концепции защиты от компьютерных угроз и имеет аналогичную схему реализации. Кроме того, в документе КЯР США [7] указано, что нужна защита не только на ЯУ, но и у разработчика ИУС АЭС, что тоже является частью глубокоэшелонированной защиты.

Методология, используемая для обеспечения компьютерной безопасности. Основная методология, используемая для обеспечения компьютерной безопасности, аналогична методологии по обеспечению физической ядерной безопасности и ядерной безопасности. Этим обусловлена необходимость внесения мероприятий по компьютерной безопасности в планы обеспечения физической безопасности ЯУ.

Приведем, в соответствии с [4], перечень мероприятий, которые должны использоваться при разработке, применении, поддержке и совершенствовании компьютерной безопасности на ЯУ:

обеспечение выполнения национальных законодательных и регулирующих требований;

изучение соответствующих международных руководящих материалов;

определение периметра компьютерной безопасности;

выявление взаимодействия между компьютерной безопасностью, с одной стороны, и эксплуатацией ЯУ, ядерной безопасностью и физической безопасностью площадки, с другой стороны;

разработка политики обеспечения компьютерной безопасности;

выполнение оценки компьютерных рисков;

выбор, разработка и применение защитных мер компьютерной безопасности;

интегрирование компьютерной безопасности в систему менеджмента ЯУ;

регулярное проведение аудита, рассмотрение и совершенствование системы менеджмента ЯУ.

Аналогичный перечень мер также определен в документах КЯР США и МЭК [5, 6].

Законодательные акты и регулирующие требования. Первоочередным заданием для защиты от компьютерных угроз является разработка и реализация национальных законодательных актов и регулирующих требований.

В силу специфики, для обеспечения компьютерной безопасности требуются законодательные акты, позволяющие учитывать уникальный характер преступлений и режимов работы, связанных с компьютерными системами. Поскольку компьютерные технологии стремительно развиваются, важно, чтобы государственное законодательство постоянно пересматривалось и обновлялось с учетом новых видов потенциальных угроз компьютерной безопасности.

При подготовке регулирующих требований по компьютерной безопасности следует учитывать регулирующие требования по физической, ядерной и радиационной безопасности. Согласно [4], регулирующие требования должны включать положения в части:

ответственности руководства по обеспечению компьютерной безопасности;

программы компьютерной безопасности;

распределения обязанностей эксплуатационного персонала и группы по компьютерной безопасности;

политики в сфере компьютерной безопасности;

реализации плана компьютерной безопасности;

аудита — внутреннего, внешнего или осуществляемого регулирующими органами;

текущей оценки угроз, результаты которой регулярно должны доводиться до сведения руководства и эксплуатационного персонала.

Политика, план и программа обеспечения компьютерной безопасности. Глубокоэшелонированная защита достигается путем использования не только нескольких уровней безопасности, но и введением и поддержкой политики, плана и программы компьютерной безопасности [5].

Политика обеспечения компьютерной безопасности устанавливает в организации цели компьютерной безопасности высшего уровня и должна отвечать определенным регулирующим требованиям.

План обеспечения компьютерной безопасности разрабатывается для осуществления политики в форме организационных ролей, обязанностей и процедур. В плане должны быть изложены основные действия в терминах чувствительности к уязвимости, защитным мерам, анализу последствий и мер по смягчению последствий с целью установления и сохранения на приемлемом уровне кибернетического риска на ЯУ и содействия возвращению в безопасный эксплуатационный режим.

Программа компьютерной безопасности определяет шаги и действия, которые необходимо предпринять для реализации последовательных организационных и технических мер и процедур, чтобы обеспечить достижение целей в области компьютерной безопасности, определенных в политике обеспечения компьютерной безопасности и изложенных в явном виде в плане обеспечения компьютерной безопасности.

Аналогичные требования относительно политики и плана обеспечения компьютерной безопасности содержатся и в [4, 6].

Организационные методы защиты. В документе [4] отдельно выделяются организационные методы защиты, к которым относятся полномочия и обязанности персонала и культура компьютерной безопасности.

Для успешной организации и поддержки мер защиты от компьютерных угроз нужно сформировать штат специалистов, четко определив их полномочия и обязанности (в [5] такой штат специалистов называется «команда компьютерной безопасности»). Для обеспечения компьютерной безопасности должны быть определены также обязанности руководящих работников разного уровня и всех сотрудников организации.

Высокая культура компьютерной безопасности — компонент любого эффективного плана обеспечения компьютерной безопасности. Важно, чтобы руководство гарантировало полную интеграцию информированности о компьютерной безопасности и общей культуры физической безопасности площадки ЯУ.

Кроме того, к организационным методам защиты можно отнести административные меры, в которых регламентированы порядок доступа к ИУС, порядок использования компьютерных сетей и носителей информации, реагирование на угрозы и атаки, порядок технического обслуживания ИУС и др.

Меры защиты от компьютерных угроз в зависимости от степени компьютерной безопасности. К компьютерной безопасности применяется дифференцированный подход, т. е. меры защиты должны быть пропорциональны потенциальным последствиям компьютерных атак [3]. В частности, для разных степеней компьютерной безопасности, которые рассмотрены в [3], применяются меры защиты различной жесткости: чем важнее система для безопасности, тем более строгая защита должна быть для нее обеспечена.

Поскольку при формировании предложений относительно категоризации по компьютерной безопасности в Украине за основу взята категоризация в соответствии со стандартом МЭК [6], целесообразно использовать требования этого документа к мерам защиты от компьютерных угроз. Основываясь на стандарте [6] и с учетом категоризации безопасности, предложенной в [3] для использования в Украине, предлагаются следующие требования к общим мерам защиты от компьютерных угроз и дифференцированным мерам защиты в зависимости от степени компьютерной безопасности.

Общие меры защиты. Для всех ИУС, независимо от их степени компьютерной безопасности, необходимо:

1. Определить проектные решения для обеспечения достаточной уверенности в том, что защита системы определенной степени компьютерной безопасности не деградирует в результате воздействия со стороны систем низшей степени компьютерной безопасности.

2. Сконфигурировать и настроить любую ИУС и любой ее компонент (в частности, покупной) так, чтобы минимизировать уязвимость системы.

3. Учесть в плане обеспечения компьютерной безопасности результаты анализа компьютерной безопасности. Если анализ показывает, что запланированные меры защиты недостаточны, определить требования к дополнительным контрмерам.

4. Адаптировать политику компьютерной безопасности к каждой ИУС или группе ИУС.

5. При проектировании, конфигурации и назначении параметров программируемого оборудования реализовать эффективные меры защиты в отношении:

управления выборочным доступом пользователей к функциям программного обеспечения (ПО) и к памяти;

линий передачи данных в системы с более низкой степенью компьютерной безопасности;

отслеживания состояния ПО и параметров его модификаций.

6. При верификации и валидации ИУС продемонстрировать эффективность функций компьютерной безопасности соответствующими испытаниями ИУС в ее окончательной конфигурации.

7. Обеспечить поддержку технических мер защиты по эффективности процедуры аутентификации при выдаче разрешения на доступ к любой ИУС.

8. Предоставлять доступ через интерфейс «человек—машина» только авторизированным сотрудникам и только для авторизированных операций.

9. Выполнить оценку компьютерной безопасности конфигурации ИУС и задать параметры ИУС на месте эксплуатации, чтобы убедиться в реализации соответствующих контрмер в отношении потенциальных угроз компьютерной безопасности.

10. Систематически планировать и проводить деятельность по модификации ПО, рассмотрев потенциальные угрозы компьютерной безопасности.

11. Периодически проверять журналы работы ПО с точки зрения компьютерной безопасности для ИУС, важных для ядерной и радиационной безопасности.

12. Периодически проверять журналы работы ПО для специализированных систем, выполняющих функции компьютерной безопасности; осуществлять централизованное управление этими журналами.

13. Минимизировать, насколько это возможно, количество точек доступа к компьютерным сетям, чтобы уменьшить их уязвимость.

14. Реализовать меры защиты по выявлению аномалий и анализу аварийных сигналов с последующим применением соответствующих мер реагирования, не нарушив при этом требования ядерной и радиационной безопасности.

15. Строго контролировать физический доступ к ИУС для предотвращения доступа неавторизованных лиц путем реализации мероприятий физической безопасности (установка замков на шкафах, контроль физического доступа в помещения или зону), а также внедрения соответствующих организационных и административных мер.

16. Ограничить продолжительность физического и программного доступа стороннего монтажного и ремонтного персонала к ИУС в соответствии с его задачами, а также конкретный перечень ИУС (или их компонентов), к которым разрешен доступ.

17. Идентифицировать и регистрировать все временные изменения (например, временный доступ или временные подключения дополнительных линий связи для испытательных устройств).

18. Запретить конфигурирование ПО и изменение технических средств, если они не запланированы, не утверждены и не задокументированы.

19. Определить порядок действий для своевременного восстановления приемлемого уровня работоспособности в случае, если кибернетическая атака привела к негативным последствиям; реализовать меры защиты по минимизации вероятности того, что указанный порядок восстановления будет уязвим для той же кибернетической угрозы.

Далее перечислены меры защиты от компьютерных угроз в зависимости от степеней компьютерной безопасности, которые определены в [3].

Меры защиты для ИУС степени компьютерной безопасности К1. В минимальном наборе мер защиты ИУС степени компьютерной безопасности К1 (в дополнение к общим мерам защиты) обязательны:

1. Ограничение связей ИУС степени компьютерной безопасности К1 другими ИУС степени компьютерной безопасности К1 и ИУС степени компьютерной безопасности К2, а также связанными с ними инструментальными средствами.

2. Ориентация связи в направлении от ИУС степени компьютерной безопасности К1 к ИУС степени компьютерной безопасности К2.

3. Ограничение передачи данных от ИУС степени компьютерной безопасности К2 в ИУС степени компьютерной безопасности К1 только обязательными данными, без которых невозможно выполнение функций в полном объеме; разрешение передачи только при условии детального обоснования и анализа рисков компьютерной безопасности. Надежная защита любых данных, передаваемых из ИУС степени компьютерной безопасности К2 в ИУС степени компьютерной безопасности К1, с помощью адаптированных статических ограничений (например, формат данных и контроль времени передачи).

4. Обновление ПО и изменения конфигурации ИУС степени компьютерной безопасности К1 — только с применением местных средств аппаратной блокировки (например, ключами) и только в одном канале системы за один раз. Двунаправленная передача данных между ИУС степени компьютерной безопасности К1 и специализированным оборудованием для технического обслуживания — с использованием отдельной выделенной линии передачи данных, которая отделена от других сетей. Защита этой линии передачи данных техническими, организационными и административными средствами. Контроль разрешенного доступа к ПО или изменению конфигурации с помощью сигнализации на блочном щите управления (БЩУ) или на местных щитах управления.

5. Реализация мер защиты, направленных против скрытых функций в ПО ИУС степени компьютерной безопасности К1.

6. Контроль физического доступа к ИУС степени компьютерной безопасности К1 с помощью сигнализации на БЩУ.

Меры защиты для ИУС степени компьютерной безопасности К2. В минимальном наборе мер защиты ИУС степени компьютерной безопасности К2 (в дополнение к общим мерам защиты) обязательны:

1. Ориентация связей в направлении от ИУС степени компьютерной безопасности К2 к ИУС степени компьютерной безопасности К3. При этом ИУС степени компьютерной безопасности К2 выступает как инициатор связи. Обеспечение ориентации и инициирования выполнением соответствующих технических требований по компьютерной безопасности (например, специальное оборудование для фильтрации).

2. Существенное ограничение и использование только в обоснованных случаях передачи данных от ИУС степени компьютерной безопасности К3 в ИУС степени компьютерной безопасности К2.

3. Исключение возможности обновления ПО и изменения конфигурации ИУС степени компьютерной безопасности К2 со стороны ИУС степени компьютерной безопасности К3.

4. Обновление ПО и изменение конфигурации ИУС степени компьютерной безопасности К2 — только в одном канале системы за один раз, только в течение заранее определенных временных промежутков, с защитой соответствующими блокировками. Двунаправленная передача данных между ИУС степени компьютерной безопасности К2 и специализированным оборудованием для технического обслуживания — с использованием отдельной выделенной линии передачи данных, которая отделена от других сетей. Защита этой линии передачи данных техническими, организационными и административными средствами.

5. Запрет на использование входных линий связи из-за пределов АЭС или компьютерных систем, которые не участвуют в управлении технологическими процессами, в ИУС степени компьютерной безопасности К2.

6. Ограничение доступа проектными решениями защиты к программируемым составным частям ИУС степени компьютерной безопасности К2 (например, путем аутентификации пользователей) и предотвращение любого несанкционированного создания новых путей доступа к этим составным частям.

Меры защиты для ИУС степени компьютерной безопасности К3. В минимальном наборе мер защиты ИУС степени компьютерной безопасности К3 (в дополнение к общим мерам защиты) обязательны:

1. Обоснование на индивидуальной основе доступа со стороны не участвующих в реализации технологического процесса компьютерных систем, которые могли бы повлиять на функции ИУС степени компьютерной безопасности К3, при условии, что доступ не ставит под угрозу соблюдение требований по ядерной и радиационной безопасности и физической безопасности, которые требуются от этой ИУС.

2. Инициирование со стороны ИУС степени компьютерной безопасности К3 связи между ИУС степени компьютерной безопасности К3 и компьютерной системой, не участвующей в реализации технологического процесса. Обоснование исключений должным образом, контроль связи.

Отметим, что приведенный перечень общих и дифференцированных мер защиты от компьютерных угроз является лишь минимально необходимым и должен быть расширен в зависимости от особенностей конкретной ЯУ и конкретной ИУС, к которой эти меры применяются. Конкретные меры безопасности для ИУС должны определяться по результатам анализа компьютерной безопасности этой ИУС, включая анализ соответствующих угроз и сценариев атак, а также определения уязвимостей системы.

Выводы

В статье рассмотрен комплекс методологических рекомендаций общего характера, описанных в документах МАГАТЭ, КЯР США и МЭК, по обеспечению защиты от компьютерных угроз. Отмечено, что устанавливать минимальные стандарты приемлемого риска или описывать в нормативных документах конкретный набор мер защиты от компьютерных угроз и смягчения последствий кибернетических атак не представляется возможным.

Анализ документов МАГАТЭ, КЯР США и МЭК продемонстрировал использование этими организациями одинаковых общих принципов и подходов к требованиям по обеспечению компьютерной безопасности и необходимых для этого мер защиты от компьютерных угроз. В частности отмечен аналогичный подход в документах МАГАТЭ, КЯР США и МЭК к принципу глубокоэшелонированной защиты, организационным методам защиты, политике, плану и программе обеспечения компьютерной безопасности. Также отмечена важность разработки и выполнения национальных законодательных актов и регулирующих требований.

В статье предложены меры защиты от компьютерных угроз в зависимости от степени компьютерной безопасности, которые целесообразно учитывать при разработке нормативного документа Украины по компьютерной безопасности ИУС АЭС.

Список использованной литературы

1. Клевцов А. Л., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: кибернетические угрозы. *Ядерна та радіаційна безпека.* 2015. № 1 (65). С. 54—58.

2. Клевцов А. Л., Ястребенецкий М. А., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: нормативная база. *Ядерна та радіаційна безпека*. 2015. № 4 (68). С. 51—57.

3. Клевцов А. Л., Симонов А. А., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: категоризация. *Ядерна та радіаційна безпека.* 2016. № 4 (72). С. 65—70.

4. Computer security at nuclear facilities : reference manual : technical guidance. Vienna : International Atomic Energy Agency, 2011. (IAEA nuclear security series, ISSN 1816-9317; No. 17). ISBN 978-92-0-120110-2.

5. RG 5.71. Cyber security programs for nuclear facilities. Washington : U.S. Nuclear Regulatory Commission, 2010. 105 p.

6. IEC 62645. Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based system. Geneva : International Electrotechnical Commission, 2014. (ISBN 978-2-8322-1810-5).

7. RG 1.152. Criteria for use of computers in safety systems of nuclear power plants. Washington : U.S. Nuclear Regulatory Commission, 2011. 13 p.

References

1. *Klevtsov, A.L., Trubchaninov, S.A.* (2015), "Computer Security of NPP Instrumentation and Control Systems: Cyber Threats" [Kompiuternaia bezopasnost informatsionnykh i upravliaiushchikh sistem AES: kiberneticheskiie ugrozy], Nuclear and Radiation safety, No. 1 (65), pp. 54—58. (Rus)

2. *Klevtsov, A.L., Yastrebenetsky, M.A., Trubchaninov, S.A.* (2015), "Computer Security of NPP Instrumentation and Control Systems: Regulatory Framework" [Kompiuternaia bezopasnost informatsionnykh i upravliaiushchikh sistem AES: normativnaia baza"], Nuclear and Radiation safety, No. 4 (68), pp. 51—57. (Rus)

3. *Klevtsov, A.L., Symonov, A.A., Trubchaninov, S.A.* (2016), "Computer Security of NPP Instrumentation and Control Systems: Categorization" [Kompiuternaia bezopasnost informatsionnykh i upravliaiushchikh sistem AES: kategorizatsiia], Nuclear and Radiation Safety, No. 4 (72), pp. 65—70. (Rus)

4. IAEA Nuclear Security Series, No. 17 (2011), Computer Security at Nuclear Facilities, Reference Manual, Technical Guidance, International Atomic Energy Agency, Vienna, 88 p.

5. *RG 5.71* (2010), Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, Washington, 105 p.

6. *IEC 62645* (2014), Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Security Programmes for Computer-Based System, International Electrotechnical Commission, Geneva, 93 p.

7. *RG 1.152* (2011), Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, 13 p.

Получено 03.03.2017.