УДК 621.039:004.9 Doi: https://doi.org/10.32918/nrs.2019.4(84).09

Компьютерная безопасность информационных и управляющих систем АЭС: документы, обосновывающие компьютерную безопасность

- **Симонов А. А.**
  Государственное предприятие «Государственный научно-технический центр по ядерной и радиационной безопасности», г. Харьков, Украина
  ORCID: https://orcid.org/0000-0001-6971-523X
- **Клевцов А. Л.**
  Государственное предприятие «Государственный научно-технический центр по ядерной и радиационной безопасности», г. Харьков, Украина
  ORCID: https://orcid.org/0000-0001-5665-5039
- **Трубчанинов С. А.**
  Государственное предприятие «Государственный научно-технический центр по ядерной и радиационной безопасности», г. Харьков, Украина
  ORCID: https://orcid.org/0000-0003-4256-5192
- **Лазуренко А. П.**
  Национальный технический университет «Харьковский политехнический институт», г. Харьков, Украина
  ORCID: http://orcid.org/0000-0002-4409-629X

В статье рассмотрены подходы к созданию и управлению документами, которые обосновывают компьютерную безопасность, такими как: политика, программа и план компьютерной безопасности, план реагирования на компьютерные инциденты, отчетные документы по компьютерной безопасности. Представлены требования к политике, программе и плану компьютерной безопасности, и проведен анализ различных подходов, принятых и отраженных в документах Международного агентства по атомной энергии (МАГАТЭ), Комиссии ядерного регулирования Соединенных Штатов Америки (КЯР США) и Международной электротехнической комиссии (МЭК). Отмечено, что подходы, применяемые указанными организациями, к созданию и управлению документами, обосновывающими компьютерную безопасность, являются весьма схожими.

Проведенный анализ различных международных подходов к разработке, внедрению и поддержанию политики, программы и плана компьютерной безопасности позволил, с учетом существующей ситуации на АЭС Украины, разработать требования к вышеуказанным документам, которые будут отражены в новом нормативном документе. Также в новый нормативный документ планируется включить отдельные требования к документации разработчика информационных и управляющих систем, относительно компьютерной безопасности, требования к плану реагирования на инциденты, связанные с компьютерной безопасностью и требования к отчетным документам по компьютерной безопасности. Даны рекомендации к содержанию, реализации и управлению указанными документами, которые обосновывают компьютерную безопасность.

Ключевые слова: компьютерная безопасность, информационная и управляющая система, политика компьютерной безопасности, программа компьютерной безопасности, план компьютерной безопасности.

Данная статья продолжает цикл публикаций [1] – [4] по компьютерной безопасности ИУС АЭС в журнале «Ядерна та радіаційна безпека». Анализ потенциальных кибернетических угроз на стадиях разработки и эксплуатации ИУС АЭС представлен в [1]. В [2] приведен обзор нормативных документов МАГАТЭ, КЯР США и МЭК по компьютерной безопасности ядерных установок (ЯУ). Требования, установленные в этих документах, зависят от принятой категоризации систем по компьютерной безопасности, которая детально рассмотрена в [3]. В [4] проанализированы основные принципы и методы защиты от компьютерных угроз и предложены соответствующие меры защиты от компьютерных угроз в зависимости от степени компьютерной безопасности.

Цель данной статьи — рассмотреть основные этапы создания документов, обосновывающих компьютерную безопасность, таких как: политика, программа и план компьютерной безопасности, план реагирования на компьютерные инциденты, отчетные документы по компьютерной безопасности, сравнить принятые подходы МАГАТЭ, КЯР США и МЭК, а также дать рекомендации по содержанию, внедрению и управлению документами, обосновывающими компьютерную безопасность, для ИУС АЭС Украины.

ИУС играют важную роль в обеспечении безопасной эксплуатации АЭС. Исторически сложилось так, что компьютерной безопасности на АЭС не уделялось должного внимания, поскольку предполагалось, что аппаратные или аналоговые системы неуязвимы для кибератак из-за их жесткой реализации, изоляции и сегрегации, а также из-за почти полного отсутствия коммуникаций с внешними сетями или системами. По мере своего развития цифровые технологии все чаще интегрируются в ИУС. Сейчас происходит повсеместный переход на цифровые ИУС при модернизации существующих и строительстве новых АЭС. Однако применение цифровых технологий в ИУС сделало их уязвимыми для кибератак. Влияние кибератак на ИУС может привести к широкому спектру последствий, таких как временная потеря контроля над технологическим процессом или радиологические последствия.

Основным принципом защиты от компьютерных угроз является использование глубокоэшелонированной защиты. Как было отмечено в [4], глубокоэшелонированная защита достигается путем использования не только нескольких уровней безопасности, но также введением и поддержкой политики, программы и плана компьютерной безопасности.

Политика компьютерной безопасности

Документы МАГАТЭ [5], [6], КЯР США [7], [8] и МЭК [9] регламентируют необходимость разработки и поддержания политики компьютерной безопасности. Согласно NSS 17 [5] политика компьютерной безопасности — это совокупность директив, регулирующих положений, правил и практики, предписывающая порядок того, как организация управляет компьютерами и компьютерными системами и обеспечивает их защиту.

Политика компьютерной безопасности устанавливает цели компьютерной безопасности и описывает требования к управлению компьютерной безопасностью в организации. Политика компьютерной безопасности должна отвечать действующим регулирующим требованиям и поддерживаться в течение всего срока службы ИУС АЭС путем регулярных пересмотров. Требования политики компьютерной безопасности для ИУС должны быть включены в документы более низкого уровня и должны быть достижимыми.

В NSS № 33-T [6] отмечено, что политика компьютерной безопасности должна включать в себя элементы для обеспечения безопасности ИУС и, следовательно, должна быть разработана и применяться в любой организации, участвующей в жизненном цикле ИУС. К этим организациям относятся разработчики, поставщики, подрядчики и эксплуатирующие организации, которые разрабатывают, производят, приобретают, внедряют и эксплуатируют ИУС, их компоненты и программное обеспечение.

Согласно IEC 62645 [9] политика компьютерной безопасности должна:

включать в себя постановку целей и определение общего направления и принципов действий в отношении компьютерной безопасности ИУС;

учитывать законодательные и нормативные требования, а также договорные обязательства по обеспечению компьютерной безопасности;

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

гарантировать применение требований компьютерной безопасности на всех этапах жизненного цикла;

согласовываться со стратегическим управлением рисками ЯУ, в контексте чего будет осуществляться создание и поддержание программы компьютерной безопасности ИУС;

устанавливать критерии, по которым будут оцениваться риски, включая рассмотрение результатов эксплуатации ИУС.

Программа компьютерной безопасности

Определяет последовательные организационные и технические меры и процедуры для обеспечения достижения целей в области компьютерной безопасности, которые определены в политике компьютерной безопасности. При разработке программы должны учитываться политика компьютерной безопасности и требования, установленные проектировщиком, органом регулирования ядерной и радиационной безопасности и эксплуатирующей организацией. Программа компьютерной безопасности разрабатывается с учетом оценки рисков.

На рис. 1 показаны подходы к процессу разработки, внедрения и поддержки программы компьютерной безопасности согласно [8] и [9].

Хотя на рис. 1 такие шаги как непрерывный мониторинг, пересмотр программы компьютерной безопасности, контроль изменений и хранение записей приведены последовательно, они могут выполняться и параллельно.

Как видно из рис. 1 в документах МЭК [9] и КЯР США [8] применяются схожие подходы к процессу разработки, внедрения и поддержки программы компьютерной безопасности, а также регламентируется обязательная разработка программы и плана компьютерной безопасности. В документе МАГАТЭ [5] рассматривается только план обеспечения компьютерной безопасности, который по своему содержанию аналогичен программам МЭК и КЯР США, поэтому будет рассмотрен в этом разделе. Также стоить отметить, что в более новом документе МАГАТЭ [6] используется понятие «программа компьютерной безопасности», вместо плана.

В своде федеральных нормативных актов США [7] регламентировано, что программа компьютерной безопасности должна быть направлена на:

реализацию мер обеспечения безопасности для защиты ИУС от кибернетических атак;

применение и поддержку стратегии глубокоэшелонированной защиты от кибернетических атак для обеспечения возможности обнаружения атак, реагирования на них и восстановления после атак;

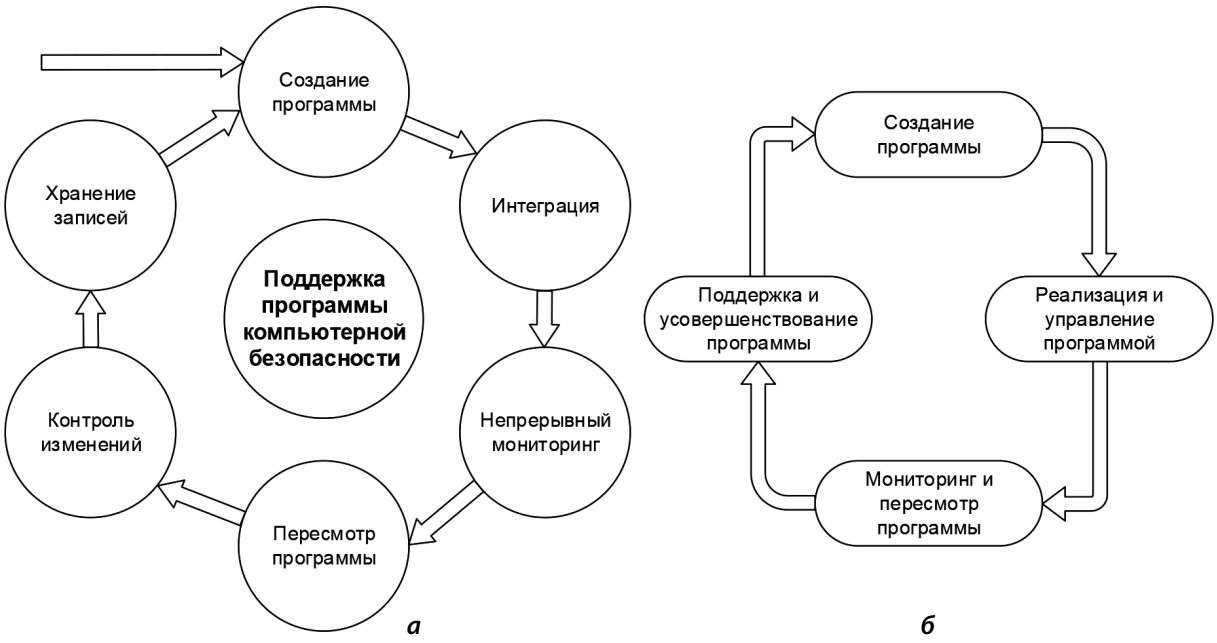

Рисунок 1 — Жизненный цикл программы компьютерной безопасности (*а*) согласно RG 5.71 [8] и (*б*) согласно IEC 62645 [9]

смягчение негативных последствий кибернетических атак;

обеспечение отсутствия негативного влияния кибернетических атак на функции ИУС.

Согласно [7] лицензиат в рамках программы компьютерной безопасности должен:

гарантировать, что персонал соответствующей ЯУ, а также подрядных организаций, ознакомлен с требованиями к компьютерной безопасности и прошел подготовку, необходимую для выполнения возложенных на него функций и обязанностей;

оценивать и управлять кибернетическими рисками;

гарантировать, что модификации критически важных ИУС и программного обеспечения (ПО) оцениваются до их внедрения;

сообщать о событиях компьютерной безопасности в соответствии с требованиями, установленными в [10].

В документах [5], [8] и [9] сформирован список задач, которые необходимо реализовать, для разработки, внедрения и усовершенствования программы компьютерной безопасности:

Анализ цифровых систем и сетей ЯУ, выявление и оценка критических для безопасности активов и ресурсов. Необходимо провести анализ цифровых компьютерных и коммуникационных систем и сетей на конкретной ЯУ для выявления критических для безопасности активов и ресурсов, компрометация которых может негативно повлиять на функции безопасности ЯУ. Такой анализ позволяет создать перечень оборудования и сетей, которые необходимо защищать в рамках программы компьютерной безопасности.

Внедрение безопасной архитектуры. При внедрении безопасной архитектуры системы группируются в соответствующие зоны компьютерной безопасности, которые разделяются защитными границами с использованием специальных защитных средств. Логическая модель распределения систем по зонам не всегда прямо корреспондируется с физическим размещением.

Анализ потенциальных рисков нарушений компьютерной безопасности. Подтверждение правильности выполнения требований компьютерной безопасности осуществляется с помощью оценки рисков. Такие анализы учитывают риски конкретных угроз и сценариев атак, а также риски уязвимости реализованных мер защиты.

Поддержка и усовершенствование программы компьютерной безопасности. После внедрения программы компьютерной безопасности необходимо проведение периодических пересмотров с нормированной периодичностью, а также внеплановых пересмотров при необходимости, например, в случае: модернизации или внедрения новых ИУС, их компонентов и ПО; инцидентов компьютерной безопасности; выявления новых кибернетических угроз; изменений в политике компьютерной безопасности.

Для эффективной поддержки и усовершенствования программы компьютерной безопасности должен быть регламентирован процесс:

внедрения улучшений программы, выявленных в процессе проведения периодических внутренних и внешних проверок, включая корректирующие и превентивные меры;

оповещения об изменениях в результате пересмотров всем заинтересованным сторонам;

проведения оценки и переоценки угроз компьютерной безопасности;

оценки достижения намеченных целей.

В нормативных документах МЭК [9], КЯР США [8] и МАГАТЭ [5] установлены требования к содержанию программы компьютерной безопасности. Также, согласно [5], [6], [8] и [9], в программе компьютерной безопасности должны быть регламентированы роли и обязанности должностных лиц, ответственных за компьютерную безопасность в эксплуатирующей организации, на АЭС, на предприятии-изготовителе ИУС и в проектной организации. Предусмотрено создание специального отдельного подразделения на АЭС, ответственного за компьютерную безопасность.

План компьютерной безопасности

IEC 62645 [9] требует создания плана компьютерной безопасности, в котором, в явном виде, необходимо указать шаги и действия для реализации предусмотренных в программе компьютерной безопасности процедурных и технических мер защиты от компьютерных атак. Требования в плане компьютерной безопасности должны дифференцироваться в зависимости от категории выполняемых функций ИУС (A, B или C согласно IEC 61226 [11]).

Как указано в [7], компьютерная безопасность является составной частью физической

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

безопасности. Лицензиат должен выполнять требования по компьютерной безопасности с учетом требований программы компьютерной безопасности, а также разработать, внедрить и поддерживать план компьютерной безопасности, который детализирует требования программы компьютерной безопасности и используется для реализации политики и программы компьютерной безопасности.

В [8] отмечено, что план должен определять и детализировать средства для достижения целей компьютерной безопасности и должен учитывать особенности ЯУ, влияющие на реализацию компьютерной безопасности. План должен содержать основные действия, которые необходимо принять для обнаружения и предотвращения вторжений, оценки последствий, а также защитные меры, необходимые для смягчения последствий, с целью установления и сохранения на приемлемом уровне компьютерной безопасности на ЯУ и содействия возвращению ЯУ в безопасный эксплуатационный режим.

В нормативных документах МЭК [9] и КЯР США [8] установлены требования к содержанию плана компьютерной безопасности.

Также в [6], [8] и [9] регламентировано создание отдельного документа — плана реагирования на инциденты и восстановления после кибернетических атак, содержащего описание, как достигается своевременное выявление и реагирование на кибернетические атаки, смягчение последствий кибернетических атак, исправление уязвимостей, восстановление пораженных систем, сетей и оборудования, пострадавших от кибернетических атак.

Предложения по разработке и внедрению документов, обосновывающих компьютерную безопасность ИУС АЭС в Украине

В связи с вступлением в силу в 2018 году Закона Украины «Про основні засади забезпечення кібербезпеки України» [12] в план нормативного регулирования Государственной инспекции ядерного регулирования Украины была включена разработка нормативного документа по компьютерной безопасности ИУС АЭС. В настоящее время Государственная инспекция ядерного регулирования Украины и Государственное предприятие «Государственный научно-технический центр по ядерной и радиационной безопасности» разрабатывают соответствующий нормативный документ «Вимоги з ядерної та радіаційної безпеки до кіберзахисту інформаційних та керуючих систем атомних станцій», один из разделов в котором посвящен требованиям к документам, обосновывающим компьютерную безопасность ИУС АЭС.

Проведенный анализ различных подходов к разработке, внедрению и поддержанию политики, программы и плана компьютерной безопасности позволил, с учетом существующей ситуации на АЭС Украины, разработать требования к политике, программе и плану компьютерной безопасности, которые будут отражены в новом нормативном документе. Также в новый нормативный документ планируется включить отдельные требования к документации разработчика ИУС, относительно компьютерной безопасности, требования к плану реагирования на инциденты, связанные с компьютерной безопасностью и требования к отчетным документам по компьютерной безопасности.

Исходя из вышеупомянутого, в новом нормативном документе Украины по компьютерной безопасности ИУС АЭС предлагается установить требования к документам, обосновывающим компьютерную безопасность ИУС АЭС, которые описаны ниже. В процессе разработки и согласования нормативного документа, указанные требования могут быть уточнены.

Требования к политике компьютерной безопасности. Организации и предприятия, участвующие в жизненном цикле ИУС, разрабатывают, реализуют и поддерживают политику компьютерной безопасности, которая устанавливает цели компьютерной безопасности, определяет основные задачи и процедуры обеспечения компьютерной безопасности, а также является частью общей политики физической защиты АЭС. Необходимо осуществлять регулярный пересмотр политики компьютерной безопасности для уверенности в том, что она продолжает должным образом учитывать риски для ИУС. При пересмотре учитываются новые угрозы компьютерной безопасности, развитие технологий, модификации ИУС, изменения организационной структуры АЭС и др.

Политика компьютерной безопасности должна рассматривать следующие аспекты, важные для ИУС: управление физическим и логическим доступом; управление конфигурацией; проверки системы и ее компонентов; процесс снабжения; управление рисками и угрозами; культура

компьютерной безопасности; реагирование на инциденты и восстановление; оценка соответствия требованиям к компьютерной безопасности.

Требования к программе компьютерной безопасности. Эксплуатирующей организацией должны быть разработаны и внедрены отдельные программы компьютерной безопасности для всех энергоблоков АЭС. В программе компьютерной безопасности рассматривается совокупность всех ИУС конкретного энергоблока АЭС.

Программа компьютерной безопасности должна разрабатываться, как часть программы физической защиты ЯУ.

В программе компьютерной безопасности должно быть отражено следующее:

роли и обязанности ответственных лиц для каждого этапа жизненного цикла каждой ИУС;

обеспечение выполнения целей, определенных в политике компьютерной безопасности и применение концепции глубокоэшелонированной защиты;

уровни компьютерной безопасности ИУС и зоны компьютерной безопасности (рассмотрено детальнее в [3]);

меры компьютерной безопасности для ИУС в соответствии с их уровнем компьютерной безопасности;

отсутствие влияния компьютерной безопасности на ядерную и радиационную безопасность и мер обеспечения компьютерной безопасности на выполняемые функции ИУС;

порядок доступа к ИУС, их компонентам, ПО, конфигурационным данным и инструментальным средствам на всех этапах жизненного цикла ИУС;

потенциальные уязвимости компьютерной безопасности на каждом этапе жизненного цикла и процедуры устранения уязвимостей;

процесс определения и обеспечения защиты чувствительной информации, в соответствии с уровнем компьютерной безопасности ИУС;

проведение и документирование оценки и периодической переоценки компьютерной безопасности ИУС;

дополнительные компенсирующие меры компьютерной безопасности для действующих систем;

требования к разработчикам и поставщикам оборудования и ПО;

меры своевременного выявления и реагирования на кибернетические атаки и процесс сообщения о событиях компьютерной безопасности (детализация этих требований отображается в плане реагирования на компьютерные инциденты);

требования к подготовке персонала;

требования к плану компьютерной безопасности для реализации программы компьютерной безопасности;

перечень отчетной документации, которую необходимо разработать в ходе реализации программы компьютерной безопасности.

Пересмотр программы компьютерной безопасности осуществляется на протяжении жизненного цикла энергоблока АЭС. Первый пересмотр не позднее одного года после первичного внедрения программы, периодические пересмотры не реже, чем один раз в два года, а внеочередные в случае:

модернизации существующих или внедрения новых ИУС, их компонентов и ПО;

инцидентов компьютерной безопасности на АЭС;

выявления новых кибернетических угроз;

изменений в политике компьютерной безопасности;

изменения ответственных лиц за компьютерную безопасность;

других изменений, которые влияют на программу компьютерной безопасности (при необходимости).

Во время пересмотра программы компьютерной безопасности должна быть проведена переоценка компьютерной безопасности ИУС энергоблока.

Требования к плану компьютерной безопасности. Эксплуатирующей организацией должен быть разработан и внедрен план компьютерной безопасности для всех ИУС и их компонентов, которые внедряются или модернизируются на энергоблоке АЭС, а также для действующих ИУС, в отношении которых реализуются меры компьютерной безопасности. Требования в плане компьютерной безопасности должны устанавливаться в зависимости от степени компьютерной безопасности ИУС (категоризация ИУС по компьютерной безопасности рассмотрена в [3]).

В плане компьютерной безопасности должно быть отражено следующее:

уровень компьютерной безопасности ИУС;

комплекс шагов и действий для выполнения регламентированных требований программы компьютерной безопасности с учетом

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

дополнительных условий, влияющих на реализацию этих требований;

процесс выполнения мероприятий и процедур, необходимых для реализации политики, культуры и программы компьютерной безопасности;

средства обеспечения защиты ИУС от кибернетических атак;

аспекты реализации и поддержки мероприятий, предусмотренных в программе компьютерной безопасности;

реализация стратегии глубокоэшелонированной защиты и ее использование для защиты, обнаружения, реагирования и восстановления ИУС после кибернетических атак;

процесс оценки компьютерной безопасности;

меры защиты, которые гарантируют отсутствие влияния средств обеспечения компьютерной безопасности на выполняемые функции ИУС, и оценка реализации этих мероприятий;

порядок использования покупных компонентов ИУС и ПО и их проверки;

управление всеми отчетами по компьютерной безопасности и вспомогательной технической документацией.

Требования к документации разработчика. Разработчик ИУС, их компонентов и ПО должен разработать отдельный документ, в котором должны быть регламентированы требования к обеспечению компьютерной безопасности на этапе разработки. В этом документе должны быть определены меры компьютерной безопасности, обеспечивающие безопасную среду разработки ИУС и ее компонентов, а также определен перечень отчетной документации по реализации обеспечения компьютерной безопасности на этапе разработки и перечень изменений, которые необходимо внести в программу компьютерной безопасности.

В указанном документе разработчик устанавливает уровни компьютерной безопасности разрабатываемых ИУС, их компонентов и ПО и регламентирует отсутствие влияния мер обеспечения компьютерной безопасности на выполняемые функции.

Требования к плану реагирования на компьютерные инциденты. Эксплуатирующая организация должна разработать план реагирования на компьютерные инциденты, который содержит процедуры идентификации и реагирования на возможное аномальное функционирование ИУС. Такой план определяет порядок действий персонала, направленных на предотвращение развития аномальных ситуаций и восстановление после инцидентов компьютерной безопасности.

План реагирования на компьютерные инциденты определяет состав и распределение обязанностей персонала, входящего в состав команды реагирования на компьютерные инциденты. В состав команды должен входить не только персонал по компьютерной безопасности, но и персонал, ознакомленный со спецификой построения и функционирования ИУС. План должен периодически пересматриваться и, при необходимости, дополняться.

Требования к отчетным документам по компьютерной безопасности. По результатам реализации программы и плана компьютерной безопасности эксплуатирующая организация разрабатывает соответствующие отчеты, в которых должно быть подтверждено выполнение требований, регламентированных в программе и плане компьютерной безопасности.

Выводы

В статье рассмотрены требования к документам, обосновывающим компьютерную безопасность. Проанализированы и отражены требования МЭК, КЯР США и МАГАТЭ к содержанию, процессу разработки, внедрению, поддержанию и улучшению политики, программы и плана компьютерной безопасности.

На основе проведенного анализа международных документов и с учетом специфики и существующей ситуации на АЭС Украины даны конкретные требования к документам, обосновывающим компьютерную безопасность, которые планируется отразить в новом нормативном документе Украины «Вимоги з ядерної та радіаційної безпеки до кіберзахисту інформаційних та керуючих систем атомних станцій», а именно:

политике компьютерной безопасности, которая должна быть разработана и применяться в любой организации, участвующей в жизненном цикле ИУС, и должна устанавливать цели компьютерной безопасности и требования к управлению компьютерной безопасностью в организации;

программе компьютерной безопасности, которая должна определять последовательные организационные мероприятия и технические меры и процедуры для обеспечения достижения целей в области компьютерной безопасности.

В программе должна рассматриваться совокупность всех ИУС энергоблока АЭС;

плану компьютерной безопасности, который детализирует требования программы компьютерной безопасности и используется для реализации политики и программы компьютерной безопасности для отдельной ИУС;

документации разработчика по компьютерной безопасности, регламентирующей требования, которые должны быть реализованы в ИУС, их компонентах и ПО, на этапе разработки;

плану реагирования на компьютерные инциденты, который содержит процедуры идентификации и реагирования на возможное аномальное функционирование ИУС вследствие кибератак;

отчетным документам по компьютерной безопасности, в которых должно быть подвержено выполнение требований по компьютерной безопасности.

Необходимо отметить, что в процессе разработки и согласования нормативного документа «Вимоги з ядерної та радіаційної безпеки до кіберзахисту інформаційних та керуючих систем атомних станцій», требования к указанным документам, обосновывающим компьютерную безопасность, могут быть уточнены.

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. Симонов А. А., Клевцов А. Л., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: меры защиты от компьютерных угроз. *Ядерна та радіаційна безпека*. 2017. № 2 (74). С. 46–50.

5. 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.

6. Computer security of instrumentation and control systems at nuclear facilities: technical guidance. Vienna : International Atomic Energy Agency, 2018. (IAEA Nuclear Security Series, ISSN 1816-9317; No. 33-T). ISBN 978-92-0-103117-4.

7. U.S. Nuclear Regulatory Commission Regulations: Title 10, Code of Federal Regulations, Part 73 — Physical protection of plants and materials, § 73.54 Protection of digital computer and communication systems and networks. Washington — DC, December 02, 2015.

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

9. 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.

10. RG 5.83. Cyber security event notifications. Washington : U.S. Nuclear Regulatory Commission, 2015. 21 p.

11. IEC 61226. Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions. — Geneva : International Electrotechnical Commission, 2009. (ISBN 978-2–88910-448-2).

12. Закон Украины «Про основні засади забезпечення кібербезпеки України» № 2163-VIII от 05.10.2017 // Ведомости Верховной Рады Украины. — 2017. — № 45. — Ст. 403. Источник https://zakon.rada.gov.ua/laws/show/2163–19.

References

1. Klevtsov, A. L., Trubchaninov, S. A. (2015). *Computer security of NPP instrumentation and control systems: cyber threats*. Nuclear and Radiation Safety, 1(65), pp. 54–58.

2. Klevtsov, A. L., Yastrebenetsky, M. A., Trubchaninov, S. A. (2015). *Computer security of NPP instrumentation and control systems: regulatory framework*. Nuclear and Radiation Safety, 4(68), pp. 51–57.

3. Klevtsov, A. L., Symonov, A. A., Trubchaninov, S. A. (2016). *Computer security of NPP instrumentation and control systems: categorization*. Nuclear and Radiation Safety, 4(72), pp. 65–70.

4. Symonov, A. A., Klevtsov, A. L., Trubchaninov, S. A. (2017). *Computer security of NPP instrumentation and control systems: protective measures against computer threats*. Nuclear and Radiation safety, 2(74), pp. 46–50.

5. IAEA Nuclear Security Series, No. 17 (2011). *Computer security at nuclear facilities. Reference manual. Technical guidance*. International Atomic Energy Agency, Vienna, 88 p.

6. Computer security of instrumentation and control systems at nuclear facilities: technical guidance. International Atomic Energy Agency, Vienna, 2018. (IAEA nuclear security series, ISSN 1816-9317; No. 33-T). ISBN 978-92-0-103117-4.

7. U.S. Nuclear Regulatory Commission Regulations. *Title 10, Code of Federal Regulations, Part 73 — Physical protection of plants and materials, § 73.54 Protection of digital computer and communication systems and networks*. Washington, DC, 02 December 2015.

8. RG 5.71 (2010). *Cyber security programs for nuclear facilities*. U.S. Nuclear Regulatory Commission, Washington, 105 p.

9. IEC 62645 (2014). *Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based system*. International Electrotechnical Commission, Geneva, 93 p.

10. RG 5.83 (2015). *Cyber security event notifications*. U.S. Nuclear Regulatory Commission, Washington, 21 p.

11. IEC 61226 (2009). *Nuclear Power Plants — Instrumentation and Control Important to Safety, Classification of Instrumentation and Control Functions.* International Electrotechnical Commission, Geneva, 64 p.

SSTC NRS | ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

12. *Law of Ukraine «On Basic Principles of Cyber Security in Ukraine» 2163-VIII of 05 October 2017.* Bulletin of the Verkhovna Rada of Ukraine, 45, Art. 403. Retrieved from https://zakon.rada.gov.ua/laws/show/2163–19.

Computer Security of NPP Instrumentation and Control Systems: Computer Security Justification Documents

Symonov A.[1], Klevtsov O.[1], Trubchaninov S.[1], Lazurenko O.[2]

[1] State Scientific and Technical Center for Nuclear and Radiation Safety, Kharkiv, Ukraine
[2] National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine

The approaches to the development and management of computer security justification documents such us computer security policy, program and plan, computer incident response plan, reports related to computer security are considered in the paper. Requirements for computer security policy, program and plan are presented, and the analysis of different approaches adopted and reflected in the documents of the International Atomic Energy Agency, U.S. Nuclear Regulatory Commission and International Electrotechnical Commission is carried out. It is noted that the approaches used by these organizations to the development and management of computer security justification documents are quite similar.

The paper provides suggestions for the development of requirements for computer security justification documents on the instrumentation and control systems at Ukrainian NPPs.

The analysis of different international approaches to the development, implementation, and management of the computer security policy, program and plan has allowed developing requirements for the above-mentioned documents, which will be reflected in the new regulation taking into account the current situation at Ukrainian NPPs. Besides, it is planned to include separate requirements for computer security documentation of the developers of instrumentation and control systems regarding computer security, requirements for computer security incident response plan and requirements for reporting documents of computer security in this regulation.

K e y w o r d s: computer security, instrumentation and control system, computer security policy, computer security program, computer security plan.

Комп'ютерна безпека інформаційних та керуючих систем АЕС: документи, що обґрунтовують комп'ютерну безпеку

Симонов А. А.[1], Клевцов О. Л.[1], Трубчанінов С. О.[1], Лазуренко О. П.[2]

[1] Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Харків, Україна
[2] Національний технічний університет «Харківський політехнічний інститут», м. Харків, Україна

У статті розглянуті підходи до створення та керування документами, що обґрунтовують комп'ютерну безпеку, такими як: політика, програма та план комп'ютерної безпеки, план реагування на комп'ютерні інциденти, звітні документи з комп'ютерної безпеки. Представлені вимоги до політики, програми та плану комп'ютерної безпеки, й проведено аналіз різноманітних підходів, прийнятих і відображених в документах Міжнародного агентства з атомної енергії, Комісії ядерного регулювання США та Міжнародної електротехнічної комісії. Відзначено, що підходи, які застосовуються зазначеними організаціями, до створення та керування документами, що обґрунтовують комп'ютерну безпеку, є досить схожими.

В нормативний документ з комп'ютерної безпеки інформаційних і керуючих систем АЕС України, що розробляється, запропоновано включити розділ, який буде присвячений вимогам до документів, що обґрунтовують комп'ютерну безпеку.

Проведений аналіз різних міжнародних підходів до розробки, впровадження й підтримки політики, програми та плану комп'ютерної безпеки дозволив, з урахуванням існуючої ситуації на АЕС України, розробити вимоги до вищезазначених документів, які будуть відображені в новому нормативному документі. Також в новий нормативний документ планується включити окремі вимоги до документації розробника інформаційних і керуючих систем, щодо комп'ютерної безпеки, вимоги до плану реагування на інциденти, пов'язані з комп'ютерною безпекою та вимоги до звітних документів з комп'ютерної безпеки. Надано рекомендації до змісту, реалізації та керування зазначеними документами, що обґрунтовують комп'ютерну безпеку.

К л ю ч о в і с л о в а: комп'ютерна безпека, інформаційна та керуюча система, політика комп'ютерної безпеки, програма комп'ютерної безпеки, план комп'ютерної безпеки.

Отримано 24.06.2019