УДК 620.9:004 (056.5+822)

Ворожцова Т.Н.

РАЗРАБОТКА ОНТОЛОГИИ КИБЕРБЕЗОПАСНОСТИ В ЭНЕРГЕТИКЕ

Анотація:

У статті розглядаються основні поняття, які стосуються кіберебезпеки в системах енергетики. Пропонується онтологія, яка описує ці поняття та їх взаємозв'язки. Кібербезпека розглядається як деяке поєднання умов, що характеризують положення та взаємодію об'єкта енергетики з оточуючим середовищем. Онтологія дозволяє врахувати всі необхідні взаємозв'язки з об'єктами і суб'єктами зовнішнього середовища при оцінці кібербезпеки.

Аннотация:

В статье рассматриваются основные понятия, касающиеся проблемы кибербезопасности в системах энергетики. Предлагается онтология, описывающая эти понятия и их взаимосвязи. Кибербезопасность рассматривается как некоторое сочетание условий, характеризующее положение и взаимодействие объекта энергетики с окружающей средой. Онтология позволяет учесть все необходимые взаимосвязи с объектами и субъектами внешней среды при оценке кибербезопасности.

Abstract:

In article the main concepts concerning a problem of cybersecurity in energy systems are considered. The ontology describing these concepts and their interrelations is offered, Cybersecurity is considered as some combination of conditions characterizing situation and interaction of object energy with environment. The ontology allows to consider all necessary interrelations with objects and subjects of environment at a cybersecurity assessment.

Вступление

Разные аспекты проблемы кибербезопасности в современных условиях в настоящее время исследуются на разных уровнях – от межгосударственного (кибербезопасность Евросоюза) до конкретного пользователя, подключенного к сети Интернет. В связи с неограниченным ростом количества компьютеров, развитием современных информационных технологий типа облачных систем хранения данных и вычислений, а также использованием разнообразных компьютерных устройств в управлении сложными техническими системами все острее проявляется проблема не только защиты данных и информации, но и обеспечения безопасности людей и объектов критической инфраструктуры, к которым относятся системы и объекты энергетики, энергетические магистральные сети и т.п. Появились такие понятия как кибератака, кибертерроризм, кибервойна.

В Институте систем энергетики им. Л.А. Мелентьева Сибирского отделения РАН (ИСЭМ СО РАН) проблемы «энергетической безопасности» исследуются с 70-х годов прошлого века. Но в отличие от экономических и технических аспектов этой проблемы в настоящее время вопросам безопасности уделяется еще больше внимания в связи с разработкой новой технологической платформы ЕЭС России – интеллектуальной энергосисте-

мы с активно-адаптивной сетью (ИЭС ААС). При этом проблема обеспечения безопасности энергосистем смещается в область обеспечения кибербезопасности [1, 2].

Терминология

Кибербезопасность (компьютерная безопасность) – это информационная безопасность в применении к компьютерам и сетям. Данное понятие включает совокупность технологий, процессов, методов, предназначенных для защиты компьютерного оборудования, информации, программ, услуг, сетей от непреднамеренного или несанкционированного доступа, изменения и разрушения, а также от незапланированных событий и стихийных бедствий.

Для формирования онтологии данной предметной области используем некоторые методологические аспекты исследования проблемы безопасности, рассмотренные в работах [3].

По отношению к сложным техническим системам, в том числе и системам энергетики, понятия "киберопасность"/"кибербезопасность" предлагается рассматривать как некоторое сочетание условий, определенную "ситуацию", характеризующую положение и взаимодействие объекта (системы энергетики) с окружающей средой, которое субъект считает соответственно опасной или безопасной. На рис. 1 показана схема воздействий и взаимосвязей субъекта, объекта кибербезопасности и внешней среды. Выводы о наличии опасности для объекта необходимо делать с учетом множества этих взаимосвязей.

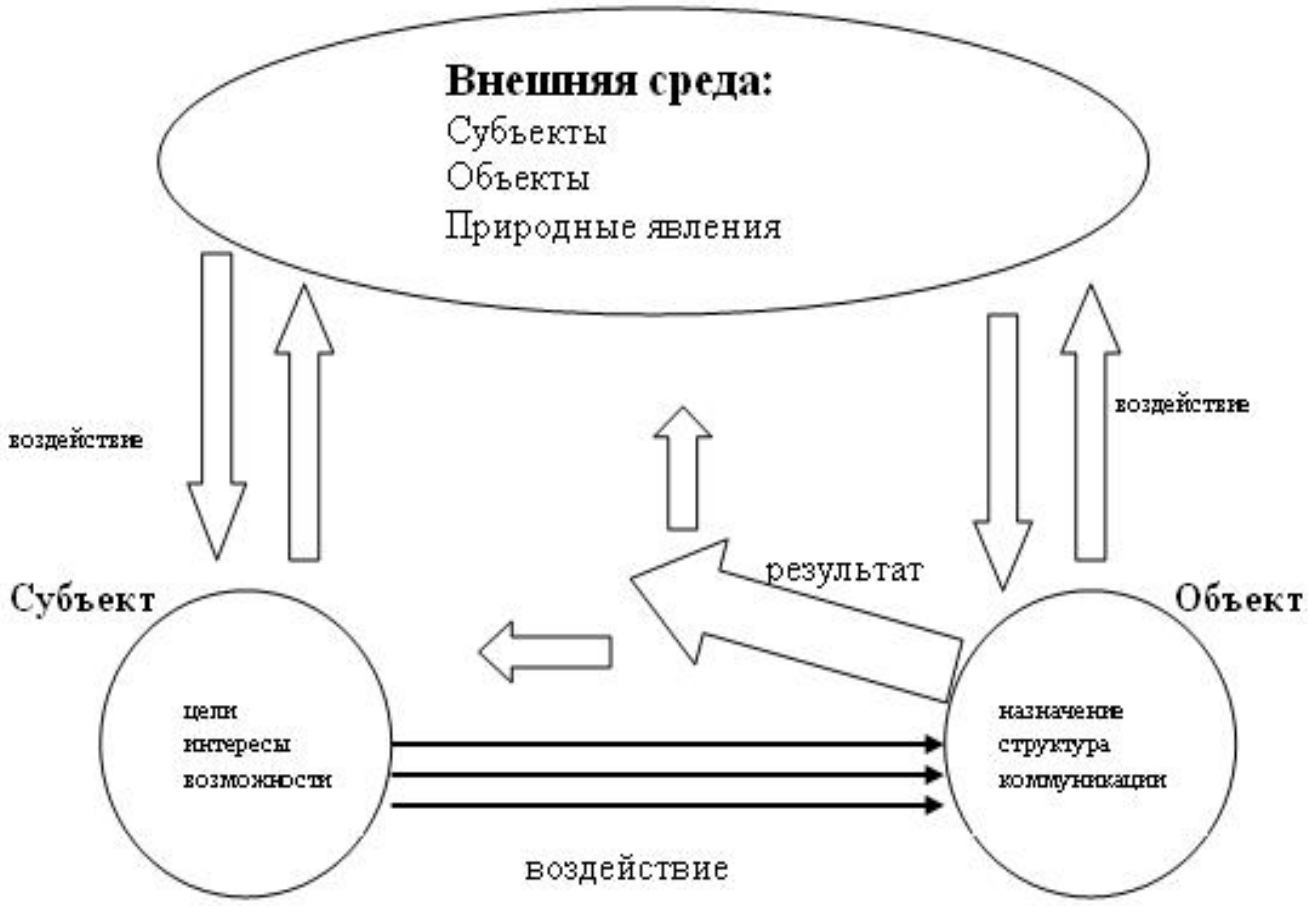

Рис. 1 Структурная схема взаимосвязей субъектов и объектов кибербезопасности

Субъектом в данном случае является управляющая данным техническим объектом структура того или иного уровня, от персонального до государственного. При этом возможны разные варианты оценки и анализа ситуации:

- Субъект сам оценивает факты и показатели, характеризующие ситуацию, и делает вывод о киберопасности/кибербезопасности. В данном случае субъект тождественен объекту. Такая оценка возможна при наличии автоматических систем управления техническим объектом достаточного высокого уровня. Но воздействия компьютерных вирусов, кибератак и др. негативных воздействий наиболее опасны именно для таких систем.
- Субъект противостоит объекту безопасности и оценивает положение этого объекта, при этом он проецирует свою субъективную оценку на ситуацию. Это возможно при наличии автоматизированной системы управления техническим объектом достаточно высокого уровня, в частности с использованием экспертных и других систем с элементами искусственного интеллекта. Если при этом уровень компетентности субъекта достаточно высок и одновременно используются широкие технические возможности для идентификации необходимых параметров, то такая оценка может быть наиболее приближенной к реальной.
- Субъект также противостоит объекту безопасности, но ему навязывается оценка, сформированная другим субъектом, которая может не соответствовать реальной действительности. Такая ситуация возможна при наличии слишком строгих регламентирующих инструкций или распоряжений другого уровня управления. В условиях современных информационных и кибервойн появляется вероятность получения недостоверной или искаженной информации, ведущей к неправильной оценке ситуации.

Субъект оценивает ситуацию с точки зрения причинения вреда объекту кибербезопасности. Вред – это результат воздействия на объект, приводящий к неблагоприятным последствиям. Понятие "вреда", применительно к объектам и системам энергетики, включает много составляющих от негативного воздействия на информационные системы, приводящие к нарушению конфиденциальности, целостности и доступности информации до непосредственного воздействия на человека или социальную систему (вывод из строя производственных мощностей, отключение объектов стратегического назначения, разрушение магистральных сетей, нефте- и газопроводов и др.).

Понятие кибербезопасности нельзя рассматривать в отрыве от понятия "киберопасность", как описания ситуации вероятности или возможности происхождения нежелательных событий, связанных с использованием компьютерных технологий. К киберопасностям специалисты относят такие понятия, как кибератака, киберпреступление (воровство, шпионаж, несанкционированный доступ, разрушение информации и другая криминальная деятельность в интернете). Особую опасность представляют действия, направленные на несанкционированный доступ к сложным техническим системам, например, к системам, контролирующим сети электропередач или другим аналогичным системам жизнеобеспечения. По мнению ведущих специалистов по борьбе с компьютерными вирусами [4] человечеству уже угрожают киберэпидемии с апокалиптическими последствиями.

Любая опасность, в том числе и киберопасность имеет совокупность характеристик или свойств, таких как вероятность появления, время существования, степень и размер зоны воздействия. В свою очередь свойства могут иметь количественные и качественные показатели, которые необходимо рассматривать и учитывать при разработке средств за-

щиты, так как они отражают меру опасности. Для оценки меры опасностей применяются численные, балльные и другие показатели, такие как число пострадавших, ущерб для окружающей среды, затраты на ликвидацию последствий и т.п.

Вероятно имеет смысл отличать понятия "киберопасность", как уже начавшееся неблагоприятное воздействие на компьютерную систему от понятия "киберугроза", которое используется в настоящее время более часто, но представляет собой потенциальную опасность, в большей степени характеризующуюся некоторой вероятностью возникновения.

Одним из распространенных понятий, связанных с кибербезопасностью, является "риск", как наиболее распространенная оценка степени опасности, вероятности причинения вреда или потерь того или иного вида. С другой стороны, понятие риска обусловлено наличием неопределенности результата деятельности как субъекта, так и объекта кибербезопасности. В таком случае и угрозы, и риски можно идентифицировать как опасность, если размер возможного вреда превысит некоторый установленный субъектом порог.

На рис. 2 представлена попытка отобразить некоторые основные взаимосвязи понятий, связанных с кибербезопасностью объекта энергетики. Понятие «кибербезопасность» в отличие от большинства представленных на рисунке является абстрактным, отражающим некоторую совокупность условий, необходимых для реального обеспечения безопасности объекта.

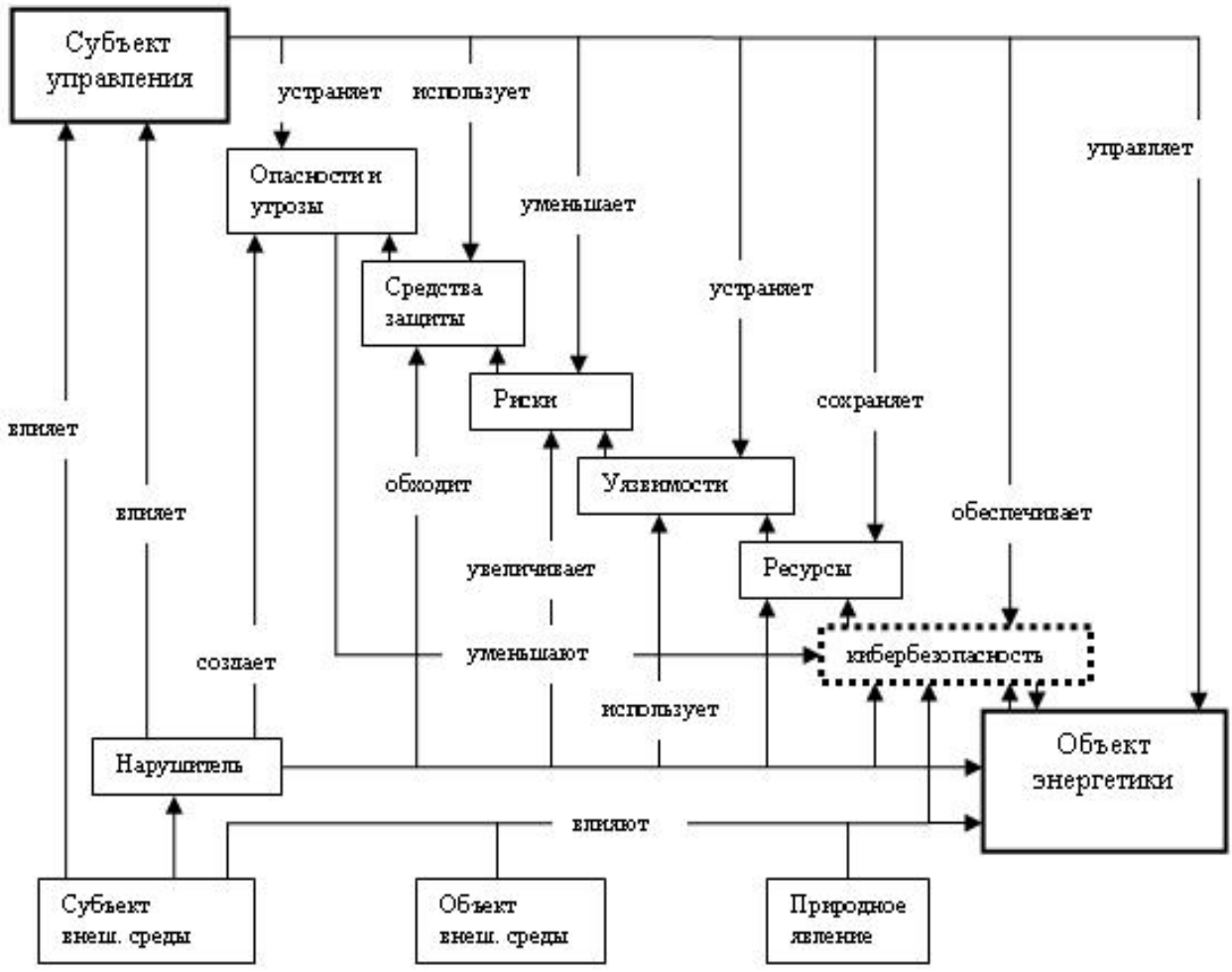

Рис. 2 Онтология кибербезопасности

К другим терминам предметной области кибербезопасности систем энергетики, связанным с понятием "вред" относятся интересы социального объекта (субъекта), неблагоприятное воздействие или последствие (деструкция, дисфункция, дестабилизация), уязвимость, источник угроз.

Кибербезопасность, тесно связана с информационной безопасностью, и, соответственно, с такими понятиями как целостность, конфиденциальность и доступность информации.

Источники, виды киберугроз и киберопасностей

В качестве основных источников киберугроз или киберопасностей в системах энергетики необходимо рассматривать субъекты управления либо внешнюю среду, которая, в свою очередь, состоит из субъектов, объектов и природных явлений. Как уже было отмечено ранее, субъект и объект кибербезопасности могут быть тождественны. С одной стороны, система энергетики, как сложный технический объект с автоматическим или автоматизированным управлением, может рассматриваться как объект кибератаки и при этом возможна автоматическая оценка необходимых параметров ее состояния с точки зрения безопасности. С другой стороны, человек, группа людей, государство или другая социальная структура, как субъект управления и кибербезопасности, в то же время является и объектом этой безопасности, так как нарушение работы таких стратегически важных систем, как энергетические, влияет на человека непосредственно.

Разные виды киберугроз формировались по мере развития интернета, начиная с распространения вирусов и троянских программ (программно-технические угрозы). Следующей группой являются экономические киберугрозы, связанные с развитием систем интернет-платежей, электронной торговлей. В настоящее время большое распространение получают контентные киберугрозы, имеющие отношение к несанкционированному доступу к персональной информации и распространению материалов, нарушающих законодательство.

При разработке систем защиты кроме описанных выше преднамеренных киберугроз необходимо учитывать также и непреднамеренные или случайные угрозы, связанные, например, с человеческими ошибками.

Помимо перечисленных киберугроз, применительно к проблеме кибербезопасности систем энергетики, связанной с разработкой ИЭС ААС, наиболее актуальными становятся угрозы, связанные с нарушениями работы систем управления технологическими процессами, последствием которых могут стать разрушение жизнеобеспечивающих систем тепло-, электро-, водоснабжения и др. По прогнозам на 2013 год, опубликованным корпорацией Symantec, конфликты между людьми, организациями и государствами перейдут в киберпространство. Кибератаки будут направлены не только на финансовые ресурсы противника с целью заработка, но и на стратегические объекты для демонстрации силы и решения политических вопросов.

Одной из наиболее опасных киберугроз в XXI веке становится кибертерроризм, под которым понимается преднамеренная атака на информацию, обрабатываемую компьютером, компьютерную систему или сети и создающая опасность для жизни и здоровья людей или наступление других тяжких последствий. Эта форма терроризма, используемая террористическими организациями, особенно опасна в связи с высокой уязвимостью компьютерных систем управления критической инфраструктурой (транспорт, атомные элек-

тростанции, водоснабжение и энергетика), подключенных к Интернету. Например, реализация кибератаки на компьютеры, контролирующие сети электропередач, может привести к катастрофическим последствиям для города, региона или даже страны [5].

Киберуязвимости систем энергетики

Термин уязвимость имеет очень тесную связь с понятием кибербезопасности, так как именно уязвимости в компьютерных системах и позволяют осуществлять кибератаки и киберпреступления. Уязвимости, как правило, это результат недостатков в проектировании информационных и операционных систем, ошибок программирования, ненадежных паролей, а также, результат воздействия вирусов и других вредоносных программ. Наличие уязвимостей позволяет внедряться в коды приложений и выполнять непредусмотренные или несанкционированные действия, нарушая их работу, целостность систем или данных.

Проблемы выявления уязвимостей в информационных системах, используемых в энергетике, существовали с момента их разработок. Например, применительно к электроэнергетике, еще в 2007 году были выявлены следующие уязвимости систем [6]:

- Уязвимость центра управления через каналы передачи данных и удаленное обслуживание.
- Использование коммерческого программного обеспечения и привлечение внешних исполнителей для текущего обслуживания EMS, а также для поддержки приложений.
- Уязвимость при удаленном обслуживании и администрировании.
- Восприимчивость к атаке интеллектуальных электронных устройств на подстанциях.
- Уязвимость цифровых программируемых устройств защиты, перенастройка которых может привести к физическому уничтожению оборудования.
- Уязвимость удаленных систем сбора данных для центра управления.
- Уязвимость телекоммуникаций, волоконно-оптических сетей общего пользования для связи между элементами систем управления.
- Уязвимость собственной инфраструктуры коммуникаций путем использования устройств для создания помех.
- Уязвимость инфраструктуры сетей общего пользования.

Список уязвимостей не остается неизменным. По мере усложнения программного обеспечения разрабатываются и инструментальные средства для обнаружения уязвимостей. Постоянный мониторинг систем на предмет выявления уязвимостей – это один из наиболее действенных методов защиты любой компьютерной системы, в том числе и в энергетике.

Обеспечение кибербезопасности требует скоординированных усилий во всех областях компьютерных систем – прикладной, информационной, сетевой, технической, образовательной и научной. Невозможно обеспечить абсолютную кибербезопасность, но необходимо стремиться к достижению киберустойчивости системы.

Заключение

Проблемам кибербезопасности уделяется все больше внимания во всех странах. В российской армии создается род войск, который будет отвечать за информационную безопасность страны, в частности, осуществлять мониторинг и обработку информации, посту-

пающей извне и борьбу с киберугрозами. Но, несмотря на все усилия абсолютную кибербезопасность обеспечить невозможно. По сведениям специалистов по проверке устойчивости компьютерных систем в 99% случаев такие системы взламываются, а для оставшегося 1% определяющим является только вопрос времени и средств. В таком случае можно говорить только о непрерывном совершенствовании систем киберзащиты, мониторинге ситуации с точки зрения отражения кибератак, поиска и устранения уязвимостей и обеспечении киберустойчивости в сложных технических системах, к которым относятся и системы, и объекты энергетики. Все острее проявляется необходимость разработки интеллектуальных экспертных систем с использованием постоянно пополняющихся баз знаний, а также, программных агентов, как средства мониторинга ситуации.

Литература:

1. Воропай Н.И. Интеллектуальные электроэнергетические системы: концепция, состояние, перспективы / Н.И. Воропай.// Автоматизация и IT в энергетике. – 2011. – №3. – С. 11–16.

2. Массель Л.В. Интеллектуализация поддержки принятия решений при моделировании и управлении режимами в Smart Grid / Массель Л.В. // Интеллектуализация обработки информации: труды 9-й Международной конференции. – Черногория, Будва, 2012. – С. 692–695.

3. Атаманов Г.А. Методология безопасности / Г.А. Атаманов // Материалы и публикации о безопасности [Электронный ресурс] – Режим доступа : http://www.naukaxxi.ru/materials.

4. Касперский Е. России грозит киберопасность [Электронный ресурс] / Е. Касперский – Режим доступа: http://obozrevatel.com/technology/04839-rossii-grozit-kiberopasnost-kasperskij.htm.

5. Шмидт Ф. Киберопасность подстерегает на каждом шагу [Электронный ресурс] / Ф. Шмидт, М. Бушуев. – Режим доступа : http://www.dw.de.

6. Крюкова Э.П. Информационная безопасность в индустрии электроэнергии. Современный мировой опыт / Э.П. Крюкова, О.В. Чурко // Энергетика и ТЭК. – 2007 – №12. – С.42–45.

7. Бенитес Х. Воздушные замки кибербезопасности [Электронный ресурс] / Хорхе Бенитес, Джейсон Хили – Режим доступа :

http://www.inoforum.ru/inostrannaya_pressa/vozdushnye_zamki_kiberbezopasnosti.