Проблемы обеспечения кибербезопасности в условиях цифровой трансформации

Р.И. Исаев к.т.н., профессор, Н.Э. Уткурхужаева, магистрант (ТУИТ)

Ушбу мақолада рақамли ривожланишда киберхавфсизликни таъминлаш муаммолари, киберхавфсизликни таъминлаш мезонлари ва ҳимоялаш технологияларнинг таснифлари келтирилган.

В данной статье рассмотрены проблемы обеспечения кибербезопасности в условиях цифровой трансформации, приведены критерии обеспечения кибербезопасности и классификация технологий защиты.

This article discusses the problems of ensuring cybersecurity and its components, examines the criteria for ensuring cybersecurity on the basis of which protection technologies are classified.

Международным Союзом Электросвязи (International Telecommunication Union, ITU) принята Глобальная программа кибербезопасности и все страны – члены ITU приняли обязательство по обеспечению кибербезопасности в соответствии с пятью основными составляющими, которые включены в Глобальный индекс кибербезопасности (ГИК): правовые нормы, технические меры; организационные меры, развитие потенциала, сотрудничество.

Правовые нормы – законодательства государства в области кибербезопасности.

Технические меры – наличие в государствах групп реагирования на компьютерные инциденты (CIRT, CSIRT или CERT).

Организационные меры – наличие в государстве национальной стратегии (политики) кибербезопасности.

Создание потенциала – осуществление разработок и проведение компаний (мероприятий) по повышению осведомленности населения в области кибербезопасности.

Сотрудничество – осуществление двусторонних соглашений между государствами, направленные на сотрудничество в области кибербезопасности.

Предложенные ITU пять основных составляющих, включенных в ГИК, оказывает помощь решению проблем обеспечения кибербезопасности в условиях быстро развивающееся цифровой трансформации.

Изменения современного мира, вызванные бурным ростом телекоммуникационных и информационно-коммуникационных технологий и всеобщей цифровизацией, не могли не затронутцифровое общество в целом. Создание и повсеместное использование программируемых контроллеров, роботов, цифровых систем управления цифровыми объектами, интегрированных с корпоративными, национальными и международными сетями, привело к серьезным проблемам по обеспечению кибербезопасности.

Появились новые классы угроз, названных, в соответствии с требованиями времени, «киберугрозами» и ставится в соответствие новый класс систем обеспечения безопасности: систем кибербезопасности цифрового объекта – «четвертая промышленная революция», охватывающая мировое сообщество, приводит к появлению и переходу к цифровой экономике, вызванной бурными темпами технического развития, широтой применения телекоммуникационно-информационных технологий и системностью использования цифровых устройств и объектов. Термин «Индустрия 4.0», прозвучал впервые в 2011 году на Ганноверской ярмарке при обозначении процесса коренного преобразования глобальных цепочек создания стоимости. Основой этого процесса стали технологии «умного» производства, «умных» домов, «умных» городов, оборудования, бытовых устройств – цифровых объектов, подключенных к сети связи. В настоящее время гибкое взаимодействие различных физических систем посредством цифровых технологий меняет вид не только отдельных секторов экономики, но и экономики государства в целом [1].

Современный период называется «вторым машинным веком», подчеркивая разницу между традиционными подходами использования аппаратного и программного обеспечения. Несмотря на то что в отраслях экономики, его применение в последнее годы имеют следующие существенные отличия:

- существенно возрастает масштаб проникновения цифровых технологий, как в различные отрасли и сферы секторов экономики, так и в отдельные новые направления экономики;
- происходит синтез технологий, от расшифровки генома до нано технологий и систем возобновляемых энергоресурсов;
- стремительно возрастает скорость изменений – в отличие от предыдущих индустриальных революций «Индустрия 4.0» развивается не линейно, а по экспоненте.

Необходимо особо обратить внимание на то, что ценность общества «Индустрия 4.0» представляет собой не продукция, а информация и потенциал информационного воздействия, за счет повсеместного использования автоматизации и обмена данных, компьютеризированных рабочих

мест, объектов, производственных систем, Интернета вещей и облачных сервисов [2].

Объект защиты, понимаемый ранее как совокупность классифицированных данных, приобретает более сложное представление – как киберпространство, включающее не только данные, но и системы их передачи, обработки и хранения, системы управления, средства защиты, а также их динамически изменяющиеся взаимосвязи, составляющие определенную ценность. Сегментами киберпространства являются суперкомпьютеры, корпоративные и домашние сети, мобильные системы, облачные сервисы, предоставляемыев глобальной сфере информационного пространства, представляющую собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры [3].

Сегодня происходит активное развитие киберфизических систем и переход к этапу интеграции с бизнес процессами – цифровой экономикой. Киберфизический объект – это концептуальная парадигма представления производственных, технологических схем в виде конгломерата средств преобразования различных видов материи и энергии и информационно-телекоммуникационной среды, обеспечивающей как обмен информацией между компонентами, так и устойчивое функционирование всей системы в условиях внешних воздействий с помощью автоматизированного
управления [4].

Кибербезопасность в условиях цифровой трансформации – это набор принципов и средств обеспечения безопасности информационных процессов, подходов к управлению безопасностью и прочих технологий, которые используются для активного противодействия реализации киберугроз.

Проблемы обеспечения кибербезопасности могут быть систематизированы как анализ механизмов нарушения защиты киберпространства, моделирование разрушающих воздействий, управление кибербезопасностью, определение зоны устойчивости объекта защиты, анализ киберрисков, разработка стандартов и нормативов безопасности киберпространства, синтез средств защиты киберпространства и контроль текущего состояния и функционирования компонентов киберпространства. В соответствии с этим современная парадигма обеспечения кибербезопасности включает [4]:

1. Пересмотр моделей управления доступом, учитывающих открытость, гибкость и распределенность.
2. Принятие технологии виртуализации как мощнейшего средства защиты, которое позволяет перейти от понятия «защищенной системы» (от фиксированного множества угроз) к понятию «система с прогнозируемым поведением».

3. Реализация принципа разделения среды обработки информации и средств защиты.

4. Построение теоретических основ управления динамической защитой (адаптирующейся к текущим угрозам) как объекта автоматического регулирования с понятием зоны устойчивости, последействием (инерционностью) динамическими характеристиками.

5. Принятие открытости систем (связи по Интернет) как неотъемлемого свойства и построение защиты с учетом этого.

6. Разработка основ оценки эластичности (настраиваемой системы) и масштабируемости.

7. Учет возможности использования суперкомпьютеров для создания новых сценариев атак, систем сканирования, вмешательства в управление цифровым объектом, криптоанализа. Учитывая, что вошли в эпоху кибервойн, суперкомпьютер – возможность создания нового оружия.

8. Анализ существующих тенденций развития средств обеспечения безопасности позволяет сделать вывод о смене парадигм защиты, базирующихся на технологиях защиты, которые условно могут быть определены как статическая, активная, адаптивная и динамическая. Идея такой классификации технологий защиты заимствована из теории управления. Несмотря на различие целей, преследуемых в теории управления и методов защиты информации, можно увидеть сходство подходов, используемых для достижения этих целей и направленных на удержание системы в границах некоторого набора состояний. Множество критериев, на основе которых строиться классификации методов управления, включают следующие параметры:

1. Наличие обратной связи – в общем случае регуляторы с обратными связями могут использовать множество измеряемых величин и формировать управляющих воздействий на регулируемый объект.

2. Наличие контура адаптивного управления – подстраивается над контуром регулирования, назначение которого – подстраивать внутренние параметры регулятора так, чтобы достигался оптимум, характеризуемый определенным набором критериев – показателем качества.

3. Наличие в контуре обратной связи функций прогнозирования состояния системы – на основании показателей, характеризующих систему и её окружающую среду, строится множество условных сценариев, прогнозирующих развитие системы результат. Прогноза подается на вход регуляторов и влияет на формирование текущего управляющего воздействия.

На основе перечисленных критериев можно безошибочно классифицировать существующие технологии защиты – для каждого из классов характерно наличие определенной совокупности перечисленных контуров.

В статической технологии защиты, функция управления не изменяется во времени и режим работы описывается функциями зависимости выходного состояния объекта защиты от постоянных управляющих воздействий и других дестабилизирующих факторов, обратная связь, адаптивное управление и прогнозирование состояния системы отсутствуют.

В активной технологии защиты, функция управления дополняется введением обратной связи – результаты экспериментального тестирования объекта защиты используются для изменения настраиваемых параметров системы безопасности. Активная технология защиты, соответственно, требует наличия контура адаптивного управления – параметры систем безопасности периодически изменяются таким образом, чтобы показатели эффективности защиты (вычисляемые на основе характеристик объекта защиты в ходе мониторинга) стремились к максимуму.

Динамическая технология защиты – динамическая компенсация нежелательных изменений состояния системы в реальном масштабе времени, путем взаимодействия как с объектом защиты, так и с его инфраструктурой. Фундаментальным отличительным признаком динамической защиты является то, что защищаемая система трактуется как нелинейный динамический объект с непрерывным временем, а сама система защиты становится дискретно – непрерывной.

Поэтому полное множество методов динамической защиты, лежащей на основе парадигмы кибербезопасности, включает методы изучения и влияния на окружающую среду изучаемого объекта, направленные на прогнозирование состояния системы в зависимости от динамики изменения внутренних и внешних (по отношению к защищаемой системе) факторов.

Таким образом, появляется понятие «система с прогнозируемым поведением» - для обеспечения кибербезопасности недостаточно описания только состояния безопасности системы, необходимо также предусмотреть систему мониторинга, сбора, анализа угроз, инцидентов, разработка модели и алгоритма прогнозирования поведения системы. Необходимо иметь возможность предсказать поведение системы в заданной (по неконтролируемой и не доверенной) окружающей среде, а в будущем – предсказать и динамику изменения внешних воздействий на защищаемую систему.

Вышерассмотренное означает, что динамическая защита должна быть направлена на исследование не только защищаемой системы и механизмов реализации угроз, но и окружающей среды защищаемого объекта и перспективных средств нарушения безопасности.

Наиболее перспективным является интегральный подход решения проблем обеспечения кибербезопасности, основной задачей которого является сохранение

работоспособности системы цифрового объекта в условиях различных целенаправленных воздействий. Эта концепция соответствует основному направлению развития системы защиты сегодня - предчувствие угрозы и адаптация системы обеспечения кибербезопасности цифрового объекта к будущему воздействию, т.е. реализация опережающей стратегии защиты.

Выводы:

В условиях цифровой трансформации для обеспечения кибербезопасности необходимо:

1. Выполнение обязательств по обеспечению кибербезопасности, принятой Глобальной программой кибербезопасности ITU.

2. Четвертая промышленная революция привела к развитию цифровой трансформации и в результате само пространство и его цифровые объекты стали управляемыми и соответственно это привело к возможности управления информационной безопасностью - кибербезопасности.

3. Проблемы обеспечения кибербезопасности требуют систематизации:

- механизмов нарушения защиты киберпространства;
- моделирование разрушающих воздействий;
- управление кибербезопасностью;
- определение зоны устойчивости объекта защиты;
- анализ киберрисков;
- разработка стандартов и нормативов безопасности киберпространства;
- синтез средств защиты киберпространства;
- контроль текущего состояния и функционирования компонентов киберпространства.

Наиболее перспективным является интегральный подход решения проблем обеспечения кибербезопасности, основной задачей которого является сохранение работоспособности системы цифрового объекта в условиях различных целенаправленных воздействий. Эта концепция соответствует основному направлению развития системы защиты – предчувствие угрозы и адаптация системы обеспечения кибербезопасности цифрового объекта к будущему воздействию.

Список использованной литературы:

1. Шваб К. Четвертая промышленная революция / К.Шваб – «Эксмо», 2016 – (TopBusinessAwards).

2. Industry 4.0 How to navigate digitization of the manufacturing sector // McKinsey Digital 2015 http://www.doud-finder.ch/fileadmin/Dateien/PDF/Themen-kategorien/indastrie 4.0/McKinsey_Report_industry_4.0_3_pdt.

3. Зегжда П.Д. Систематизация киберфизических систем и оценка их безопасности // П.Д. Зегжда, М.А. Полтавцева, Д.С. Лаврова. Проблемы информационной безопасности. Компьютерные системы. 2017 №2 С.127-138.

D.P.Zegzhda, E.Yu.PavlenkoCyber_PhysicalSystemHomeostaticSecurity Management // Automatic Control and Computer Sciences ISSN 0146-4116. Vol.51, №8, 2017.