IV. Кибербезопасность. Особенности обеспечения безопасности в социальных сетях

DOI: 10.25728/iccss.2022.57.97.032

Промыслов В.Г., Семенков К.В.

Проблема обеспечения кибербезопасности критических объектов в недоверенной среде

Аннотация: В работе рассматривается проблема синхронизации жизненного цикла кибербезопасности с жизненным циклом объекта в промышленных системах. Отмечается, что несоответствие в жизненных циклах может привести к невозможности обеспечить основные свойства монитора безопасности в системе. Для противодействия данной угрозе, предлагается использовать глубокоэшелонированную защиту основных компонентов системы от информационных угроз.

Ключевые слова: кибербезопасность, глубокоэшелонированная защита, жизненный цикл, доверенная среда

Введение

Концепция обеспечения информационной безопасности по умолчанию всегда строилась на концепции доверия [1]. В рамках этой концепции основным являлось понятие доверенной среды и наличия монитора обращений, в рамках которого реализовывалась политика безопасности. Причем предполагалось, что монитор обладает свойствами, препятствующими попыткам его обмануть или скомпрометировать, постоянной готовностью и простотой.

Концепция доверия, несмотря на некоторые сложности в ее реализации, в целом выполнялась и выполняется для большинства цифровых систем общего назначения, ориентированных в основном на конфиденциальность. Однако реализация данной концепции столкнулась с трудностями, когда встала проблема обеспечения информационной безопасности, для промышленных объектов с

цифровыми системами управления ориентированной на сохранение доступности и целостности. Информационную безопасность в контексте промышленных объектов, часто определяют как кибербезопасность, чтобы подчеркнуть различие в приоритетах целей безопасности. Проблема обеспечения кибербезопасности промышленных систем является комплексной, связанной с обеспечением общепромышленной безопасности. Для критических объектов безопасность может быть также связана с энергетической, транспортной, ядерной и иными аспектами безопасности [2].

Трудности в реализации механизма монитора обращений и всей доверенной среды для промышленных систем управления состоят в том, что жизненный цикл системы кибербезопасности не соответствует жизненному циклу объекта, что приводит к невозможности обеспечить основные свойства безопасности монитора обращений.

В работе рассмотрены проблема соотнесения жизненного цикла кибербезопасности с жизненным циклом защищаемой системы и предложены решения, смягчающие несоответствия в жизненных циклах.

Жизненный цикл обеспечения кибербезопасности

Возможный жизненный цикл работ по обеспечению кибербезопасности программируемой цифровой АСУ ТП для атомной электростанции (АЭС) и его соотнесение с жизненным циклом самой АСУ ТП приведен на рисунке 1.

Можно видеть, что по составу этапов жизненные циклы защищаемой системы (левая часть рисунка) и системы кибербезопасности (правая часть) принципиально не отличаются. Проблема возникает в случае наличия переходов между этапами вверх на каждом из жизненных циклов. Такие переходы могут возникать при устранении несоответствий в выполненных ранее работах на объекте, повышения эффективности его функционирования, а для системы кибербезопасности, например, при выявлении новых угроз для системы или уязвимостей в компонентах.

Временные рамки таких переходов и их частота, как показала практика, не сопоставима для обоих жизненных циклов. Для примера приведем характерные значения для АСУ ТП АЭС (таблица 1).

Рисунок 1 – Жизненный цикл работ по обеспечению кибербезопасности АСУ ТП АЭС

Таблица 1 – Параметры жизненного цикла. Данные параметры являются субъективными оценками авторами, основанными на опыте работы для проектов АСУ ТП АЭС с реакторами типа ВВР-1000

Параметр	Система кибербезопасности АСУ ТП АЭС	АСУ ТП АЭС
Частота необходимостей изменений в год	Еженедельно	Менее 5 раз в год
Частота уязвимостей/несоответствий	Около 200 в месяц	Менее 5 в год
Фактическая длительность внесения изменения на объекте	Менее 1 дня	От одного дня до нескольких недель
Время на подготовку изменения	Около 1 месяца	Не менее 1 месяца

Как мы видим, число выявленных несоответствий и интервал их устранения значительно отличаются для ситемы кибербезопасности и собственно объекта защиты. Оценка частоты выявления уязвимостей сделана по базе данных уязвимостей CVE [3]. За 2021 год выявлено чуть более 20000 новых уязвимостей, с учётом того, что значения охватывают все наиболее известные ОС и прикладные пакеты, то для конкретной АСУ ТП доля уязвимостей, относящихся к ней, по нашим оценкам будет составлять около 10 процентов. Следовательно, за год в системе будет открыто приблизительно 2000 уязвимостей, часть которых будет носить критический характер.

Остальные значения, оценивающие трудоемкость внесения изменений сравнимы. Необходимо также учесть, что некоторые обновления программных пакетов, требуемые для кибербезопасности, конфликтуют с прикладным ПО (программным обеспечением АСУ ТП), и для их установки требуется переработка прикладного ПО. Таким образом, если жизненный цикл объекта превалирует над жизненным циклом его системы кибербезопасности, то это приводит к тому, что основную часть времени система находится в недоверенном с точки зрения кибербезопасности состоянии.

Очевидным способом обеспечения кибербезопасности в этом случае является внедрение административных и организационных мер защиты или применения, если это возможно, стратегии по переносе риска кибербезопасности от объекта на третью сторону. Однако перенос риска, являясь предпочтительным, невозможен для многих объектов критической инфраструктуры т.к. риск для них может быть неприемлемым ни в какой форме, а административные и организационные меры сами по себе не могут обеспечить кибербезопасность системы. Одним из способов обеспечения кибербезопасности в частично недоверенной среде является реализация на уровне архитектуры системы концепции глубоко эшелонированной защиты кибербезопасности ГЭЗК [4].

Архитектура кибербезопасности для работы в недоверенной среде

Глубокоэшелонированная защита от компрометации активов по кибербезопасности включает в себя обеспечение нескольких последовательных мер защиты, которые необходимо обойти для

того, чтобы кибератака прогрессировала и повлияла на компонент АСУ ТП и на выполняемые системой критические функции.

Последовательность преодоления мер защиты, на пути атаки обеспечивается делением системы на уровни и зоны кибербезопасности (рисунок 2).

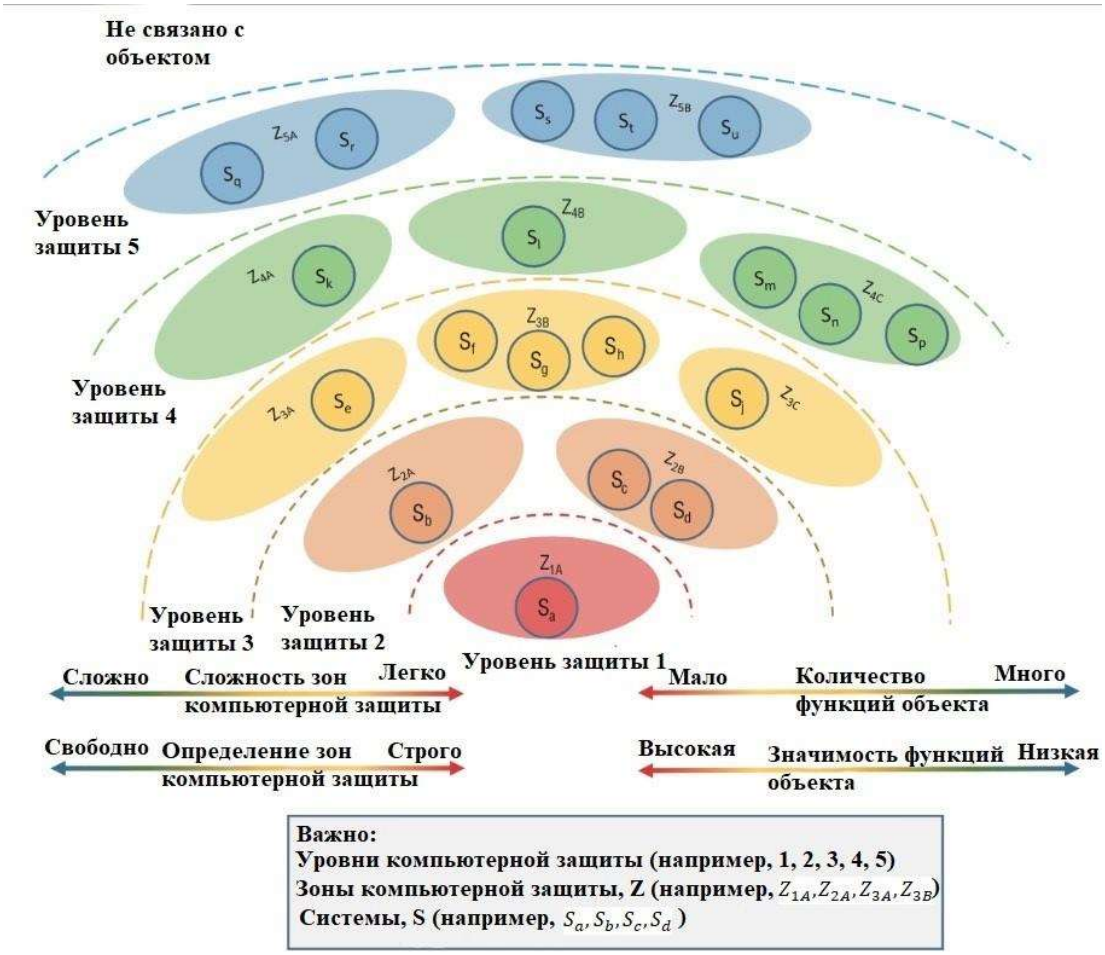

Рисунок 2 – Концептуальная модель уровней и зон кибербезопасности в рамках ГЭЗК [2]

Для кибербезопасности важно не только наличие последовательных мер защиты, но и их разнообразие. Разнообразие в реализации мер защиты потенциально увеличивает возможную размерность вектора атаки. Это происходит из-за большего набора механизмов защиты, которые может атаковать злоумышленник, но это же и обеспечивает независимость мер защиты в последовательной цепочке барьеров, преодолеваемых злоумышленником.

Общий подход в обеспечении ГЭЗК включает в себя пункты, необходимые для обеспечения кибербезопасности с использованием комбинации независимых и разнообразных мер. Данные меры должны быть преодолены нарушителем для достижения целей атаки путем компрометации актива [5]. Разработчики подсистем при выборе компенсирующих мер защиты должны учитывать воздействие конкретной меры защиты на определенную угрозу.

Заключение

В современном мире обеспечение кибербезопасности промышленных объектов, например АЭС, транспортной и энергетической инфраструктуры является актуальной задачей. Однако, ее трудно решить, оставаясь в рамках классической парадигмы, когда уязвимости, по крайней мере связанные с критическими компонентами системы, устраняются фактически сразу после их появления. Практика показывает, что из-за несоответствия временных рамок жизненного цикла объекта защиты и системы обеспечения кибербезопасности основную часть времени в системе нельзя выделить доверенную часть. Это верно не только для этапа эксплуатации, но и для более ранних этапов жизненного цикла: проектирования и разработки.

Задачу обеспечения кибербезопасности в этом случае необходимо трактовать как комплексную задачу, с приоритетом административных, организационных и физических мер защиты.

Как одна из возможных мер, обеспечивающих выполнение системой кибербезопасности своих функций, предлагается использовать концепцию глубокоэшелонированной защиты, реализуемую на уровне архитектуры защищаемого объекта.

Литература:

1. Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD Supersedes CSC-STD-00l-83, dtd l5 Aug 83. Library №. S225,7ll. – URL: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf (дата обращения 12.10.2022).

2. IAEA 17-T INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear

Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021). – URL: https://www.iaea.org/publications/14729/computer-security-techniques-for-nuclear-facilities (дата обращения 12.10.2022).

3. CVE [Электронный ресурс]. – URL: https://cve.mitre.org (дата обращения 12.10.2022).

4. *Промыслов В.Г., Семенков К.В., Шумов А.С.* Синтез архитектуры кибербезопасности для систем управления атомных электростанций // Проблемы управления. – 2019. – № 3. – С. 61-71.

5. *Chris Moschovitis.* "Controls," in Privacy, Regulations, and Cybersecurity: The Essential Business Guide. – John Wiley & Sons, 2021. – P. 301-320. DOI: 10.1002/9781119660156.ch18

DOI: 10.25728/iccss.2022.60.22.033

Степанцов М.Е.

Моделирование сценария информационного противоборства с асимметричным влиянием на малые группы

Аннотация: В работе рассматривается сценарий бинарного информационного противоборства, в котором одна из сторон имеет большую степень влияния на общество в целом, а вторая – на малые группы. Для математического моделирования используется ранее предложенная автором клеточно-автоматная модификация модели информационного противоборства, основанной на нейрологической схеме Рашевского. Вычислительные эксперименты, проведенные при помощи имитационной системы, построенной на основе данной модели, показывают, что в достаточно широком диапазоне параметров описанная ситуация приводит к «атомизации» общества.

Ключевые слова: математическое моделирование, имитационное моделирование, клеточные автоматы, информационное противоборство, малые группы

В рамках исследования различных сценариев информационного противоборства представляется уместным рассмотреть ситуацию, в которой информационное воздействие с двух сторон происходит