Эталонная модель безопасности критических информационных инфраструктур

А. Н. Петухов
Кафедра информационной безопасности
Национальный исследовательский университет
«Московский институт электронной техники» (МИЭТ)
anpetukhov@yandex.ru

С. Ю. Гуснин
Кафедра системы интеллектуального мониторинга
Московский авиационный институт (национальный исследовательский университет)
gusnin@testing.ru

Аннотация. **В работе обсуждается модель безопасности критических информационных инфраструктур, в условиях невозможности исчисления ущерба, нанесенного инцидентом, отсутствия допустимого остаточного риска и миграции критериев безопасности за пределы информационно-технологической сферы. Показывается принципиальная неполнота моделирования угроз и оценки защищенности на базе анализа событий безопасности. Предлагаемая модель наряду с адаптацией традиционных аспектов безопасности (проактивного, пассивного и реактивного) включает многоуровневую статическую модель, используемую для описания функциональных и информационных процессов объекта критической информационной инфраструктуры. Модель безопасности включает динамические модели анализа причинно-следственных цепочек для описания процессов возникновения и распространения инцидентов безопасности. Для адекватного и бесконфликтного размещения активностей предлагается стратегия применение большого числа контрмер в ступенчатом виде, распределенных на всю глубину информационного пространства.**

Ключевые слова: критические информационные инфраструктуры; информационная безопасность; эталонная модель

В разных сферах деятельности к критическим могут быть отнесены различные объекты, однако можно отметить ряд общих признаков таких объектов, выявляя специфику безопасности критических информационных инфраструктур (КИИ).

КИИ определяются не через свои свойства, а через ситуацию (инцидент), когда с ними что-то произошло. Определение КИИ включает состояние среды (государство, люди, природа и т.д.), которые могут непосредственно не участвовать в функционировании КИИ, в том числе не влиять на их безопасность.

Под безопасностью КИИ понимается состояние защищенности КИИ, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак [1]. Такое определение выводит безопасность КИИ за пределы собственно информационной безопасности, «захватывая» пространства функциональной безопасности. Поэтому при защите КИИ нельзя говорить исключительно об информационной безопасности, должно быть привлечено понятие функциональной безопасности – части безопасности критического объекта, которая зависит от корректного функционирования связанных с безопасностью электрических систем управления, систем безопасности, основанных на других технологиях.

Следствием этого является то, что для КИИ характерны принципиальные отличия целей безопасности и связанной с ними системы критериев. Кроме того, невозможно обоснование уровня допустимого остаточного риска, и отсутствует механизм исчисления реального ущерба от инцидента информационной безопасности. Существует попытка создания и использования общего языка для описания, понимания и управления рисками КИИ, как внешними, так и внутренними [2]. Целью его декларируется облегчение процесса идентификации и приоритизации активностей по компенсации рисков КИИ. При этом идентифицируются не угрозы возникновения рисков, и даже не сами риски, а активности по их компенсации. Развитие такого языка соответствует движению в сторону создания эталонной модели безопасности КИИ, дополняющей идентификацию рисков как проявления угроз возможностью идентифицировать риски без указания угрозы и уязвимости, например, связав его непосредственно с видом защитной активности.

Особое значение в методологии безопасности КИИ имеют место и роль модели угроз и вопросы эффективности различных методических направлений моделирования угроз применительно к КИИ.

Все известные методологии моделирования угроз явно или неявно включают догмат, утверждающий достаточную полноту модели, хотя неизвестны какие-либо методы доказательства этой полноты. Без этого догмата целью управления безопасностью КИИ становится не может быть достижение некоторого уровня защищенности (сбалансировать риски с затратами, привести некоторую производную меру (риска, доверия, экономических показателей) к заданному уровню или оптимизировать характеристики такого рода).

В условиях отказа от понятия остаточного риска затрудняется анализ степени снижения угрозы в результате

принятия мер безопасности, и целью обеспечения безопасности КИИ становится исчерпание потенциала защиты (сделать все, что можно) независимо от содержания и направленности агрессивных проявлений и при условии известных и ограниченных возможностей защитных активностей. Тогда, целевое состояние безопасности определяется не в терминах угроз и гармонизированных с ними сущностей (нарушитель, актив, уязвимость и т.д.), когда мы утверждаем, что некоторый (претендующий на исчерпывающую полноту) набор актуальных угроз нами скомпенсирован, а непосредственно в терминах видов нашей деятельности – активностей (претендующих все на ту же исчерпывающую полноту).

Обращает на себя внимание то, что ни в одном методическом нормативе КИИ нет категорической зависимости решений от состава и происхождения угроз. Поэтому можно сделать предположение, что, либо нужно отказаться от базирования методологии на моделировании угроз, либо использовать корректный механизм доказательства исчерпывающей полноты для используемой модели угроз. В первом случае, приходится сконцентрироваться не на угрозах, а на защитных активностях и реализовывать все те меры, эффективность которых положительна. В этом случае возникает нетривиальная задача обеспечения формальной полноты исходной номенклатуры активностей и метризации их эффективности в зависимости от условий, в т.ч. совместности применения. Во втором случае проблема заключается в том, что пока не решен глубокий вопрос исходной аксиоматики, на базе которой можно построить доказательство наличия или отсутствия угрозы.

Несмотря на это, необходимо иметь адекватное представления об агрессивном потенциале среды. В любом конкретном случае есть особенности структуры и формы такого представления и общим элементом всегда является типология проявления опасности, номенклатура идентифицированных и квалифицированных видов такого проявления, внешних (агрессивность среды) и внутренних (несовершенство объекта) событий и ситуаций, являющихся причиной возникновения ущерба, (т.н. проактивный аспект управления безопасностью, т.е. модель угроз).

Для анализа, проектирования и управления безопасностью КИИ используются статические многоуровневые модели основных типов КИИ. Эти модели используются для структурированного описания пространства, где протекают функциональные и информационные процессы, и выполняются процедуры управления этими процессами. Для безопасности статические модели КИИ важны именно в силу того, что они являются источником правил, условий и ограничений возникновения и распространения внутри уровня и между уровнями «неисправностей» КИИ, приводящих к аварийному инциденту. Основная функциональная нагрузка статической модели КИИ – выявить влияние критериев информационной безопасности на критерии функциональной безопасности.

Референсная модель [3] определяет пять функциональных уровней, но то, что обычно подразумевается под КИИ, занимает уровни со второго по нулевой. Эта модель ввиду высокого уровня своей концептуальности практически не использовалась в самостоятельном и недетализированном виде, и свое применение нашла в качестве основы для более развитых и специализированных моделей. Иногда привлекается модель физической архитектуры КИИ, предложенная и развитая в работе[4], которая описывает физические компоненты, объединенные информационной сетью управления.

Рациональным симбиозом этих двух моделей (референсной и физической архитектуры) является модель зонирования [5]. Эта модель, может быть платформой для анализа угроз, уязвимостей, рисков и контрмер (контролей и активностей) с учетом управленческих, информационных и вспомогательных функций КИИ. Модель зонирования представляет собой многоуровневую схему критического объекта и состоит из следующих уровней:

- Enterprise Systems – на этом уровне происходит управление критическим объектом в целом (стратегическое управление, иногда выделяют дополнительный уровень ERP Systems);
- MES – на этом уровне выполняется операционное управление критическим объектом (буферный уровень выполнения политик управления);
- SCADA – управление и мониторинг содержательных процессов (диспетчерский уровень);
- Control System, – локализованное управление процессами и оборудованием, включая функции безопасности;
- I/O – терминальный уровень управления процессами и оборудованием (сенсорные и исполнительные узлы и процедуры).

Нижний уровень модели представляют элементы сбора данных (сенсоры) и исполнительные устройства, средний – программные логические контроллеры, затем идут автоматизированные системы диспетчерского управления типа SCADA, взаимодействующие с оборудованием. С этим уровнем взаимодействуют MES-системы, собирающие данные о технологиях. Решения MES, в свою очередь, предоставляют агрегированную информацию для ERP-систем. В большие КИИ выделяется отдельный уровень Enterprise, который является центральным ядром всей системы управления.

Модель зонирования в исходном виде охватывает целиком информационную систему без разделения на «критическую» и «некритическую» части. На практике такое разделение может быть необходимым и для этого в модель добавляют один промежуточный уровень – уровень DMZ (демилитаризованная зона). Это сегмент сети, содержащий общедоступные сервисы и отделяющий их от критичных процессов. Уровень DMZ обеспечивает

связность этих двух зон и при этом обеспечивает разделение корпоративной ЛВС и КИИ. Сам он при этом содержит только некритичные системы, которым необходим доступ и к части общего назначения, и к КИИ. Большинство сервисов безопасности находится именно на этом уровне.

Обращает на себя внимание то, что общей отличительной чертой статических моделей КИИ является использование в качестве главного инструментального приема «расслоения» (стратификации) объекта – выделения иерархии управленческих, информационных и вспомогательных функций КИИ и размещения однотипных сущностей, участвующих в выполнении этих функций на фиксированном уровне. Предметом анализа в рамках такой модели становится взаимодействие этих сущностей как внутри соответствующего уровня, так и с сопряженными выше- и нижележащими уровнями.

Есть причинно-следственная протяженность (недетерминированная цепочка) между факторами агрессивного потенциала (угрозами) и инцидентом как фактом возникновения ущерба. В контексте критических объектов нас интересуют не столько источники происхождения вреда (угрозы), сколько форма и свойства реализации этого вреда. Динамические модели обеспечивают возможность исследования и управления процессами возникновения и распространения инцидентов безопасности в среде КИИ. Проведенный анализ известных практических методов [6] моделирования этих процессов на всем протяжении их жизненного цикла и на всем пространстве влияющих на них факторов и обстоятельств показал, что с помощью таких моделей возможно эффективно контролировать причинно-следственные цепочки развития инцидента.

Безопасность критических объектов рассматривает возможность возникновения дополнительных рисков в процессе реализации защиты и предусматривает не только устранение (ослабление) факторов угроз, но и активности в процессе развития и конечного проявления опасности (момента непосредственного возникновения ущерба независимо от угрозы, его вызвавшей). Таким образом, мы размещаем защитные активности по всему протяжению причинно-следственной цепочки реализации вреда.

Принципиальная распределенность факторов безопасности и распространение деятельности по обеспечению безопасности за пределы информационной инфраструктуры требуют решения вопросов о размещении и взаимодействии защитных активностей в КИИ. Дело в том, что невозможно обеспечить необходимые свойства безопасности применением единственной контрмеры или методики.

При этом вопрос собственно о составе активностей (защитных мер, контролей) стоит не столь остро, потому что существуют источники, нормативно [7] или конструктивно-методически [2, 8] поддерживающие и предоставляющие обширные номенклатуры активностей, полнота которых (номенклатур) не вызывает сомнения, и обсуждать можно лишь детализацию активностей в приложении к конкретной реализации КИИ. На первый план выдвигается проблема эффективного (адекватного и бесконфликтного) размещения активностей в соответствии с принятой (многоуровневой статической) моделью КИИ и выявленной (динамической) моделью распространения недопустимых отклонений (инцидента).

Одной из наиболее развитых стратегий решения такой проблемы является концепция «Defense in Depth» [9], предполагающая использование и применение большого числа контрмер в ступенчатом виде (деление на уровни). Смысл концепции заключается в том, что после проникновения, атакующего через один из защитных уровней, он встречается с новой, возможно, принципиально отличной защитой атакуемого объекта. Эта гибридная стратегия многоуровневой защиты реализует комплексный подход к безопасности в масштабе всего КИИ. По мнению ряда экспертов, в будущем данная концепция станет стандартом обеспечения безопасности в КИИ.

Концепция использует понятия контекста, зон, уровней и моделей безопасности. Контекст безопасности показывает, как различные элементы безопасности соотносятся между собой. Понятие безопасности распространяется на все компьютеры, сеть или различные программируемые компоненты системы (например, ПЛК). Контекст безопасности основан на представлениях угроз, рисков и контрмер, а также взаимосвязях между ними, но не исчерпывается этими понятиями. Контекст дает понимание, как соотносятся друг с другом факторы влияния на безопасность в рамках двух процессов – процесса оценки и анализа проявления угроз и развитий инцидента, с одной стороны, и процесса обеспечения информационной безопасности, с другой [10].

В зависимости от типа и масштаба системы, целесообразно сопоставить допустимый уровень безопасности системе целиком или определить уровни для определенных компонентов. Различия можно учитывать, используя понятие зоны безопасности или защищаемого участка. Зона безопасности представляет собой логическое объединение физических и информационных объектов, к которым предъявляются общие требования безопасности, причем некоторые системы входят в состав зоны безопасности, а остальные находятся за ее пределами.

Могут существовать также подзоны внутри зон, которые обеспечивают многоуровневую (ступенчатую и эшелонированную) защиту, соответствуя серии уровней требований безопасности. Эшелонированная защита может быть обеспечена за счет присвоения различных свойств ее зонам безопасности. Зоны можно рассматривать как надежные и ненадежные, и они могут быть определены в физическом или логическом смысле. Зоны определены посредством группировки объектов или их частей на основе функциональности или других характеристик.

Понятие уровней безопасности используется для того, чтобы квалифицировать безопасность по отношению к зонам, а не к отдельным устройствам или системам. Уровни безопасности обеспечивают систему критериев для принятия решений о применении контрмер и устройств с различающимися параметрами собственной

безопасности. Как правило, КИИ состоит из устройств и систем, которые функционируют в совокупности, обеспечивая целостные функции управления информационными и технологическими процессами. Аналогично тому, как функциональные возможности отдельных устройств влияют на возможности КИИ, параметры безопасности отдельных устройств и реализуемых контрмер должны быть согласованы между собой для достижения требуемого уровня безопасности зоны.

Методиками рекомендовано использование трех градаций уровней безопасности – целевой, достигнутый и потенциальный. Целевой уровень назначается зоне как минимально допустимый уровень безопасности, к которому нужно стремиться. Достигнутый уровень зависит от свойств контрмер, задействованных для предотвращения нарушения безопасности зоны. Основная задача – обеспечить достигнутым уровнем равенство или превышение целевого. Потенциальный уровень определен для контрмер и внутренне присущих свойств безопасности устройств и систем внутри зоны, вносящих вклад в безопасность зоны, что является степенью эффективности контрмеры, устройства или системы в отношении свойства безопасности, которое они затрагивают.

Таким образов эталонная модель безопасности КИИ может включать в себя:

- базовые модели угроз – идентифицированных и квалифицированных видов внешних (агрессивность среды) и внутренних (несовершенство объекта) событий и ситуаций, являющихся причиной возникновения инцидента;
- статические модели структурированного описания пространства, в котором протекают функциональные и информационные процессы, и выполняются процедуры управления этими процессами для выявления влияния критериев информационной безопасности на критерии функциональной безопасности;
- динамические модели возникновения и распространения инцидентов безопасности в среде КИИ, обеспечивающие возможность исследования и управления этими процессами;
- методика размещения защитных контролей и активностей в соответствии с принятой (многоуровневой статической) моделью КИИ и выявленной (динамической) моделью распространения недопустимых отклонений (инцидента)

Список литературы

[1] Федеральный Закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 №187-ФЗ.

[2] Framework for Improving Critical Infrastructure Cybersecurity. // National Institute of Standards and Technology, USA, April, 16, 2018

[3] ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration — Part 1: Models and Terminology

[4] NIST Special Publication 800-82 Revision 2 «Guide to Industrial Control Systems (ICS) Security», May 2015. 247 c.

[5] ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems

[6] ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска

[7] Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований к обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

[8] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," April 2013

[9] Defence in Depth in Nuclear Safety, INSAG-10, A report by the International Nuclear Safety Advisory Group, International Atomic Energy Agency, Vienna, 1996

[10] ГОСТ Р МЭК 61508-1-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования.