DOI:

АНАЛИЗ КИБЕРБЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Сакрутина Е.А., Калашников А.О.

Институт проблем управления им. В.А. Трапезникова РАН, Россия, г. Москва

ул. Профсоюзная д.65

consoft@ipu.ru, aokalash@ipu.ru

Аннотация: Количество событий кибербезопасности в мире значительно выросло, и наибольшее количество событий приходится на объекты критической информационной инфраструктуры. В статье рассмотрены вопросы формирования риска и его оценки.

Ключевые слова: кибербезопасность, критическая информационная инфраструктура, оценка риска.

Введение

На сегодняшний день взаимодействие между людьми и объектами, в том числе и промышленными, стала неотъемлемой частью нашей повседневной жизни. Коммуникации, финансы и все формы управления информацией и доступа к ней можно получить практически из любого места, используя компактные устройства. Например, операторы могут одновременно удаленно проводить мониторинг и контролировать операции на нескольких объектах, хирурги могут проводить операции на пациентах за тысячи километров, а производители автомобилей могут обнаружить, когда один из их автомобилей попал в аварию в течение нескольких секунд после того, как эта авария произошла. Благодаря распространению Интернета и беспроводных сетей передачи данных, именно взаимосвязь такого большого количества данных и стольких устройств быстро стала основой современного общества. В настоящий момент, можно констатировать, что мы стали обществом, основанным на знаниях, которое в значительной степени полагается на технологии для выполнения или поддержки практически всех задач и функций. Несомненно, это сильно расширило круг решаемых задач, но и одновременно общество стало гораздо более уязвимым.

Масштабы уязвимости объясняются тем фактом, что в какой-то момент большая часть производств разного рода, поддерживается вводом, хранением и извлечением данных / информации во взаимосвязанной сети жестких дисков и серверов данных, будь то локально или удаленно размещенных. И на каждом из этих этапов существует возможность украсть данные, обойти защиту, манипулировать или подменять информацию. Но также необходимо учитывать риски, связанные с непреднамеренными инцидентами, вызванными человеческими ошибками, системными сбоями, несовместимостью или другими неожиданными проблемами, а также и «стихийными бедствиями».

Безопасность компьютерных или кибер-систем, таким образом, является вопросом национальной безопасности. На самом деле эти угрозы настолько велики, что все больше и больше экспертов по безопасности утверждают, что защита кибер-систем и данных является более серьезной проблемой, чем терроризм, учитывая масштабы угрозы (в отношении кибер-атак) и фактический ущерб, который вызывается ежегодно (а также возможные последствия, если определенные системы и структуры подвергаются риску) [1, 2]. Хакеры показали себя способными взломать правительственные и бизнес-сайты, похищать личные данные, изменять схемы функционирования светофоров, ускорять и замедлять движение поездов и многое другое. Спонсируемые государствами кибер-команды достигли еще более значительных результатов, включая самоуничтожение в 2010 г. десятков центрифуг, поддерживаемых ядерной программой Ирана [3, 4]. Таким образом, киберпространство особенно трудно защитить из-за таких факторов, как например, способности злоумышленников действовать из любой точки мира, связей между киберпространством и физическими системами.

Общество все чаще сталкивается с тем, что группа или даже отдельное лицо, вооруженное сложным компьютерным вирусом, или знанием уязвимости в программном пакете или аппаратном обеспечении, может незаметно и на большом расстоянии вызвать значительные социальные или экономические потрясения, или, что еще хуже, физические разрушения, или угрозу жизни людей. Например, есть факты, опубликованные Financial Times 8 мая 2012 (http://on.ft.com/1wviXHW), что неизвестная группа годами пыталась проникнуть в системы управления сетями газопроводов США. В конце 2014 года Национальное управление океанических и атмосферных исследований США заявило, что хакеры из Китая успешно взломали и разрушили сети метеорологических спутников США, что послужило причиной потери сервисов, поддерживающих предсказание стихийных бедствий, авиацию, судоходство и другие отрасли в течение нескольких дней (http://wapo.st/1u7N9dJ).

КИИ государства является лишь одной из многих важных систем и сетей, которые создают наше современное общество. Поэтому государство и общество полностью зависят от функционирования различных объектов и субъектов КИИ, потеря целостности любого из которых может привести к разного рода нарушениям (прекращение выработки и передачи электроэнергии, разрывам в коммуникациях на коротких и больших расстояниях, неадекватный доступ к здравоохранению и многое другое). Каждое отдельное государство является отдельной критической информационной инфраструктурой, но взаимодействие между государствами происходит в рамках глобальной КИИ. Большие инвестиции в каждый из секторов КИИ привели к увеличению темпов развития экономик и повышению качества жизни.

1 Критическая информационная инфраструктура и кибербезопасность

К КИИ относятся физические и информационные объекты, сети и активы, которые в случае повреждения могут оказать серьезное влияние на благосостояние граждан, надлежащее функционирование государств и отраслей или другие неблагоприятные последствия. Энергоснабжение и системы связи могут рассматриваться как значимые объекты КИИ, поскольку от их функционирования зависит работа остальных объектов КИИ. Технический прогресс привел к большей автоматизации в управлении КИИ. Возросшая роль информации и наличие электронных средств для ее сбора, анализа и изменения превратили информацию и информационные системы как в бесценный актив, так и в прибыльную цель.

В настоящее время многие государства уделяют внимание методам и средствам выявления, систематизации и обеспечения безопасности значимых объектов КИИ. Потеря или нарушение нормального функционирования этих объектов может привести к значительным или даже непоправимым негативным последствиям для государственной безопасности. Деструктивные воздействия злоумышленников на отдельные объекты КИИ направлены не только на данные объекты, но и на КИИ в целом. Для применения адекватных методов защиты важно определить уровень важности объектов и субъектов КИИ. Критическая информационная инфраструктура [5, 6], включающая информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ и т.д., позволяет дистанционно контролировать и управлять сервисами, тем самым повышая эффективность. К сожалению, первоначально безопасность не считалась главным приоритетом КИИ.

Кибербезопасность можно определить, как деятельность, процесс, способность, возможность или состояние, при котором информационно-коммуникационные системы и содержащаяся в них информация защищены от повреждения, несанкционированного использования или модификации, или эксплуатации. Однако, наряду необходимо думать о практической стороне кибербезопасности с точки зрения вторичных, третичных и даже более удаленных систем, оборудования и процессов, которые защищены. Например, клапан на нефтепроводе часто не рассматривается как часть «информационной и коммуникационной системы», но при наличии надлежащих инструментов и знаний злоумышленник может манипулированием механизмами управления некоторых клапанов и регуляторов, вызвать утечку в трубопроводе, которая останется незамеченной, что далее приведет к экологической катастрофе. Таким образом, требуется полное понимание сложности и охвата КИИ и механизмов контроля и управления.

Кибер-инфраструктура включает в себя все информационные и коммуникационные системы и сервисы, аппаратные компоненты и программные системы, которые обрабатывают, хранят и передают эту информацию, а также различные комбинации этих компонентов, которые расположены таким образом, чтобы выполнять одну или несколько задач, или предоставить один или несколько сервисов.

Усилившаяся связность в сочетании с возросшей сложностью делает КИИ особенно уязвимой к стихийным бедствиям, человеческим ошибкам и техническим проблемам, а также к новым формам киберпреступности, т.е. КИИ стала особенно уязвима к действиям деструктивных элементов. Основными инструментами, используемыми для воздействия на КИИ, являются вредоносные программы (компьютерные вирусы, черви, трояны), которые изменяют и/или уничтожают информацию или блокируют компьютерные системы. Инструменты для прослушивания обмена информацией в компьютерных сетях, а также инструменты для изменения нормальной работы компьютерной сети и блокировки доступа к ее услугам также широко используются в деструктивных целях. Эти автоматизированные инструменты позволяют осуществлять вторжения из удаленных систем в течение нескольких секунд, что упрощает запуск интернет-атак и становится все более

сложным для отслеживания. Недооценка способностей, знаний и опыта киберпреступников (злоумышленников) может быть фатальной для объектов КИИ.

Обмен информацией и данными подвержен изменениям, которые происходят незаметно, но постоянно. Эти изменения означают, что придется по-новому взглянуть на такие вопросы, как конфиденциальность, защита данных и безопасность, а также адаптировать деятельность к новой кибер-реальности. Динамика изменений в среде организаций означает, что для поддержания непрерывности бизнеса организациям необходим иной взгляд на проблему бизнес-рисков в киберпространстве.

В современном сетевом мире информацию можно отправлять, совместно использовать и хранить в различных формах, как цифровых, так и физических. Поэтому информационная безопасность включает в себя защиту такой информации и технические методы передачи, совместного использования и хранения. В большинстве случаев информационная безопасность фокусируется в основном на триаде: конфиденциальность, целостность и доступность (КЦД) информации. Конфиденциальность относится к ситуации, в которой информация рассматривается только сторонами, имеющими соответствующее разрешение. Целостность означает, что данные защищены от ложных изменений или повреждения во время передачи и хранения. Доступность является гарантией того, что данные доступны пользователям в любое время, когда они необходимы, то есть без перерывов в обслуживании и ненужных простоев. КЦД фокусируется на безопасности самих данных и информационных систем, участвующих в обработке данных.

Современная кибербезопасность, основываясь на КЦД, использует множество технических средств, подходов, принципов и концепций управления рисками для защиты информации и систем, основанных на информационно-коммуникационных технологиях, и их пользователей от всех видов цифрового и физического ущерба и, следовательно, финансовых потерь вызванных изменением информации. Это отражено в следующих определениях кибербезопасности, которые чаще всего приводятся в литературе:

- ISO/IEC 27032:2012 [7] определяет «кибербезопасность» (или «безопасность в киберпространстве») как «*сохранение конфиденциальности, целостности и доступности информации в киберпространстве*», где «киберпространство» определяется как «*сложная среда, возникающая в результате взаимодействия людей, программного обеспечения и сервисов в среде Интернет посредством технических устройств и сетей, связанных с ним, которая не существует ни в какой физической форме*»;
- NISTIR 7298 rev.2 [8] определяет «кибербезопасность» как «предотвращение повреждения, защиты и восстановления компьютеров, систем электронной связи, сервисов электронной связи и проводной связи, включая содержащуюся в них информацию, гарантируя доступность, целостность, аутентификацию, конфиденциальность и невозможность отказа».

Следовательно, основными требованиями кибербезопасности являются конфиденциальность, целостность и доступность информации.

2 Объекты КИИ и процесс управления рисками: угрозы-уязвимости-последствия

Процесс управления рисками – это непрерывный процесс, который должен принимать форму упорядоченной последовательности событий, действий и решений, результатом которых является кибербезопасность объекта КИИ. Ключевой задачей обеспечения кибербезопасности является выявление потенциального риска. Для эффективного анализа рисков крайне важно определить объекты КИИ, угрозы, уязвимости и понимать природу кибер-атак, а также как можно точнее определить риск, выявляя его причины, масштабы, ограничения и тип потенциальных угроз, которые могут повлиять на достижение целей объекта КИИ. Взаимосвязь между различными злоумышленниками, угрозами, уязвимостями и их влиянием на информацию с последующими последствиями представлена на рис. 1. В настоящий момент каталог киберугроз [9] содержит как минимум: вредоносные программы, интернет-атаки, атаки веб-приложений, фишинг, отказ в обслуживании, спам, ботнеты, утечка данных, инсайдерская угроза, физические манипуляции, повреждение/кража/потеря информации, утечка информации, кража личных данных, криптоджекинг, вымогательство, кибершпионаж, бэкдоры, наборы эксплойтов.

Необходимо понимать, что анализ рисков является одним из элементов системы управления рисками, поскольку в процессе анализа рисков получаем информацию, необходимую для принятия правильных решений в части стратегии управления риском, эффективного выбора мер снижения риска, оценки обоснованности передачи, принятия или избежания риска.

Рис. 1. Влияние киберугроз и уязвимостей на кибербезопасность.

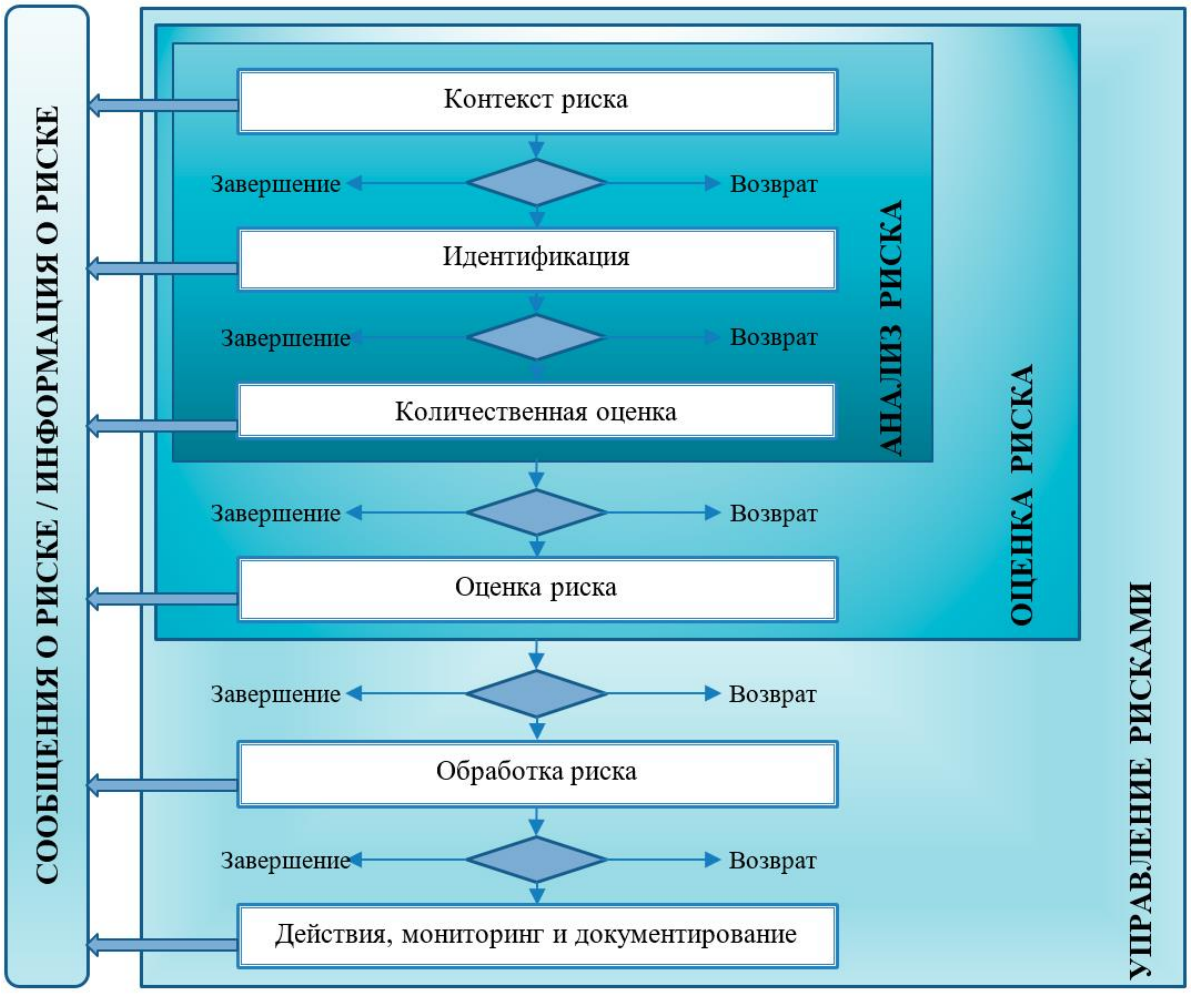

Рис. 2. Модель процесса управления рисками.

Как показано на рис. 2, процесс управления рисками, относящийся к безопасности объекта КИИ, может быть итеративным. Итеративный подход к процессу оценки риска может иметь форму повышения уровня детализации каждой итерации или остановки процесса. После каждой фазы/этапа существуют точки принятия решения (продолжение, завершение, возврат). Итеративный подход обеспечивает выгодный баланс между сокращением времени, усилий, затрачиваемых на выявление некоторых мер безопасности, и уверенность в правильной оценке рисков.

3 Оценка риска кибербезопасности

В связи с быстрым развитием технологий, изменением ландшафта киберугроз и ростом цифровизации объекты КИИ могут подвергаться повышенным рискам кибербезопасности, которые могут оказать негативное влияние на цели организации, отвечающей за объект КИИ. Таким образом, организациям необходимо эффективно управлять рисками кибербезопасности.

Оценка риска кибербезопасности (далее – «оценкой риска») является неотъемлемой частью процесса управления рисками организации. Проводя оценку рисков, организации смогут:

- определить, какие процессы могут идти не штатно и какие события, которые часто являются результатом действий со стороны субъектов угроз, могут привести к нежелательным последствиям для объекта КИИ;
- определить уровни риска, которому они подвергаются (хорошее понимание уровней риска позволит выделять адекватные действия и ресурсы для обработки рисков с наивысшим приоритетом).

Можно выделить следующие опасности при оценке риска:

- **Плохая формулировка сценариев риска** – сценарии риска, описывающие события «что может пойти не так», часто расплывчаты и носят общий характер, не содержат конкретные события угрозы, уязвимости, активы и последствия. В результате трудно понять степень рисков и связать их с организационным контекстом или определить целевые меры для их устранения.
- **Идентификация рисков с использованием подхода, ориентированного на соответствие** – идентификация рисков с точки зрения оценки мер безопасности (или их отсутствия), аналогично проведению аудита соответствия или анализа несоответствий на основе нормативных документов. Подход к оценке рисков, основанный на соблюдении нормативных требований, определяет поведение «контрольного списка», создавая ложное ощущение безопасности, что объект КИИ не подвержен никаким рискам до тех пор, пока он удовлетворяет всем соответствующим требованиям.
- **Отсутствие толерантности к риску** – часто планы управления рисками кибербезопасности объекта КИИ не включены в программу управления рисками организации. В результате толерантность к рискам кибербезопасности на уровне организации часто игнорируется, и руководство сталкивается с трудностями при принятии решения о соответствующем уровне риска для реализации своих бизнес-целей.
- **Определение вероятности риска на основе исторических или ожидаемых событий** – подход может быть неточным, если он основан на количестве случаев, когда событие произошло ранее, особенно в случае нехватки информации о прошлых событиях кибербезопасности. В контексте кибербезопасности вероятность события кибербезопасности не зависит от частоты прошлых событий.
- **Обработка рисков с помощью нерелевантных средств контроля / мер** – организации могут использовать общий подход при разработке мер по снижению выявленных рисков кибербезопасности, что приводит к внедрению мер контроля, которые не полностью устраняют основную причину. Данная проблема часто связана с плохим пониманием или формулированием сценариев риска.

3.1 Определение контекста риска

Установление контекста риска является важной предпосылкой для проведения последующей оценки риска. Этот шаг гарантирует, что внутренние и внешние заинтересованные стороны, участвующие в процессе оценки риска, имеют общее понимание того, как сформирован риск, допустимость риска для рассмотрения и ответственность владельца риска.

Пусть риск кибербезопасности (R) определяется как функция:

- вероятности (P) того, что данная угроза воздействует на уязвимость актива;
- результирующего влияния (V) возникновения угрозы

$$R(t) = F(R, V)$$

Определим каждый из факторов риска.

Угроза – любое событие, во время которого злоумышленник посредством вектора угрозы действует против актива так, что потенциально может причинить ему вред. В контексте кибербезопасности угрозы могут характеризоваться тактикой, методами и процедурами, применяемыми злоумышленниками.

Уязвимость – дефект в разработке, реализации и эксплуатации актива или во внутреннем управлении процессом.

Вероятность – возможность того, что данная угроза способна использовать данную уязвимость (или набор уязвимостей). Вероятность может быть получена на основе факторов, таких как обнаруживаемость, эксплуатируемость и воспроизводимость.

Влияние – величина ущерба, возникающего в результате угрозы, использующей уязвимость (или набор уязвимостей). Величина ущерба может быть оценена с точки зрения государства, организации или отдельного человека.

Толерантность к риску определяется как уровень принятия риска, приемлемый для достижения конкретной бизнес-цели. Определение толерантности к риску позволяет четко сформулировать, какой риск организация готова принять. В Таблице 1 приведен пример рассмотрения толерантности к риску, который может быть адаптирован в соответствии с контекстом каждой организации.

Таблица 1. Представление толерантности к риску

Уровень риска	Описание толерантности риска
Очень высокий	Уровень риска не может быть принят, так как его принятие приведет к таким серьезным последствиям, что связанная с ним деятельность должна будет немедленно прекращена. В качестве альтернативы необходимо немедленно принять стратегии смягчения последствий.
Высокий	Уровень риска не может быть принят. Стратегии, направленные на снижение уровня риска, должны быть разработаны и внедрены в течение следующего месяца.
Выше среднего	Уровень риска не может быть принят. Стратегии, направленные на снижение уровня риска, должны быть разработаны и внедрены в течение ближайшего полугодия.
Средний	Уровень риска может быть принят в случае отсутствия стратегий, которые могут быть легко и экономически реализованы. Этот риск должен постоянно контролироваться для гарантии того, что любое изменение будет обнаружено и принято соответствующее ему решение.
Низкий	Уровень риска может быть принят в случае отсутствия стратегий, которые могут быть легко и экономически реализованы. Этот риск должен периодически контролироваться для гарантии того, что любое изменение будет обнаружено и принято соответствующее ему решение.

3.2 Оценка риска

Оценка рисков заключается в выявлении рисков, специфичных для окружающей среды, и определении уровня выявленных рисков. Основными этапами оценки риска являются идентификация риска, количественное оценка риска (являющиеся элементами анализа риска) и качественная оценка риска (см. рис. 3).

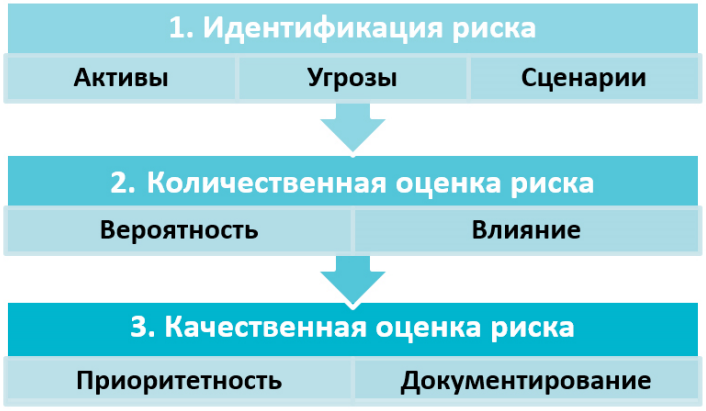

Рис. 3. Процесс оценки риска.

Задача идентификации риска включает следующие подзадачи:

а) Идентификация активов (идентифицировать и описать все активы, составляющие систему, которые относятся к данному риску). При определении активов важно выявить, какой из них

является основным, а также ресурсы, которые могут взять под контроль злоумышленники для достижения основного актива. Например, в распределенной системе управления электростанции программируемый логический контроллер (ПЛК), управляющий турбиной, вероятно, будет рассматриваться как основной актив, поскольку он напрямую влияет на выработку электроэнергии – общую бизнес-цель электростанции. Злоумышленник, желающий сорвать выработку электроэнергии, вероятнее всего, захочет манипулировать логикой работы ПЛК.

b) Идентификация угроз проводится на основе перечня ресурсов и диаграммы сетевой архитектуры с целью выявления угроз [10, 11], которые могут использовать уязвимости для каждого актива.

c) Построение сценариев риска – задача, направленная на создание сценариев, которые обеспечивают реалистичное и сопоставимое представление о рисках на основе бизнес-контекста, системной среды и соответствующих угроз. Сценарий риска должен включать следующие ключевые элементы: активы (*идентифицированы в задаче a)*), угрозы (*выявлены в задаче b)*), уязвимости (*могут быть выявлены при аудитах и/или тестах на проникновение, и могут иметь отношение к окружающей среде из-за использования определенных технологий*) и следствие (*прямой результат угрозы*).

Количественная оценка риска заключается в анализе элементов, составляющих каждый сценарий риска, для определения: вероятности возникновения сценария риска и влияния (т.е. величины ущерба) в результате возникновения сценария риска.

Историческое или ожидаемое возникновение события традиционно использовалось в качестве метрики для измерения вероятности риска. Однако использование такого показателя для измерения вероятности риска кибербезопасности может быть нецелесообразным из-за динамического характера угроз кибербезопасности. Система, которая не была скомпрометирована ранее, не означает, что она не будет скомпрометирована в будущем. Вероятность рисков кибербезопасности должна оцениваться с точки зрения угроз и уязвимостей. Один из способов определения вероятности риска кибербезопасности заключается в рассмотрении следующих факторов:

- Обнаруживаемость – «насколько легко злоумышленник сможет обнаружить уязвимость актива?». Этот фактор зависит от наличия информации об уязвимости и подверженности уязвимого актива.
- Возможность использования – «насколько легко злоумышленник может воспользоваться уязвимостью актива?». Этот фактор зависит от прав доступа, сложности средств, а также технических навыков, необходимых для проведения атаки.
- Воспроизводимость – «насколько легко злоумышленник сможет воспроизвести атаку на актив?». Этот фактор зависит от сложности настройки эксплойта и условий окружающей среды, необходимых для проведения атаки.

Проявление сценария риска может поставить под угрозу конфиденциальность, целостность и / или доступность активов (например, информации, оборудования, операций). Любой компромисс активов приведет к отрицательному воздействию на следующих уровнях:

- государственный (*влияние можно рассматривать как ущерб государственной безопасности и экономике*),
- организационный (*влияние можно рассматривать как нарушение бизнес-операций, ущерб репутации и потерю финансов*),
- индивидуальный (*влияние можно рассматривать как гибель людей и травматизм*).

Качественная оценка риска заключается в определении и понимании значимости уровня риска и включает в себя следующие задачи:

- определение и приоритеторизация рисков (*строится матрица рисков*),
- документирование рисков (внесение рисков в реестр с указанием выявленного сценария, даты, меры, остаточного риска и т.д.).

Заключение

Сложность киберфизических отношений в функционировании объектов КИИ представляет собой неосознанные системные зависимости. Проведение точной оценки рисков требует разработки моделей, обеспечивающих основу для анализа зависимостей и количественной оценки рисков. Наличие связи между характерными особенностями объектов КИИ способствует процессу анализа рисков и смягчения их последствий.

В статье представлен подход к оценке рисков кибербезопасности. Данный подход может быть применен в информационно-аналитической системе “Safety management system” [12], обеспечивающей идентификацию уязвимостей и оценку рисков (рискового потенциала) и упрощающей разработку управленческих решений для предотвращения событий, влияющих на кибербезопасность.

Литература

1. Critical Infrastructure: Cyber-attacks on the backbone of today’s economy. PandaSecurity, 2016.
2. PandaLabs Annual Report, PandaSecurity, 2017.
3. *Golovko V., Bezobrazov S., Melianchuk V.* Evalution of Immune Detectors in Intelligent Security System for Malware Detection // Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems. Vol. 2, 2011. – P. 722-726.
4. *McMillan R.* Siemens: Stuxnet worm hit industrial systems // COMPUTERWorld, Sept.14, 2010.
5. *Калашников А.О., Сакрутина Е.А.* Модель прогнозирования рискового потенциала значимых объектов критической информационной инфраструктуры // Информация и безопасность. 2018. Т. 21, № 4. – С. 465-470.
6. *Калашников А.О., Сакрутина Е.А.* Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа // Информация и безопасность. 2017. № 4, Т. 20. – С. 478-491.
7. ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity.
8. NISTIR 7298 rev.2, Glossary of Key Information Security Terms (05-2013).
9. ENISA, ENISA Threat Landscape Report 2018.
10. *Промыслов В.Г., Тимофеев М.Ю., Полетыкин А.Г., Бабаев Д.И.* Управление архитектурой кибербезопасности АСУ ТП АЭС // Проблемы управления. 2018. № 3. – С. 47–55.
11. *Промыслов В.Г., Семенков К.В., Шумов А.С.* Синтез архитектуры кибербезопасности для систем управления атомных станций // Проблемы управления. 2019. № 3. – С. 61-71.
12. *Калашников А.О., Сакрутина Е.А.* Концепция оценки рискового потенциала энергетических объектов в системе SMS / Материалы 12-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2019, Москва). – М.: ИПУ РАН, 2019. – С. 850-852.