К ВОПРОСУ УПРАВЛЕНИЯ РИСКАМИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Абдулова 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: В докладе предлагается нисходящая функциональная структура оценки и управления рисками критических информационных инфраструктур (КИИ), включающая определение области управления рисками, определение функций КИИ, анализ цепочки создания стоимости критических функций и взаимосвязей, оценку риска критических функций, расстановку приоритетов и обработку рисков критических функций.

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

Введение

Критические инфраструктуры (КИ) играют жизненно важную роль в обществе, обеспечивая выполнение многих ключевых функций и услуг. Концепция «критической инфраструктуры» постоянно развивается, отражает текущие проблемы и реагирует на новые вызовы, особенно с точки зрения кибербезопасности и устойчивости. Таким образом, защита критически важных инфраструктур от многочисленных угроз стала приоритетной задачей на национальном уровне многих государств [1-3].

Критические инфраструктуры, включая энергетические, коммуникационные и банковские сети, механизмы общественного здравоохранения и безопасности, как правило, представляют собой совокупность функций, выполняемых широким кругом заинтересованных сторон. Поэтому управление рисками для этих инфраструктур является общей ответственностью, требующей тесного и постоянного сотрудничества между заинтересованными сторонами.

Центральным принципом эффективной защиты КИ является необходимость разработки и поддержания надежной политики и планов, которые направляют и информируют заинтересованные стороны о работе по всему спектру мероприятий по защите критической инфраструктуры, включая управление рисками.

Наряду с надежными политиками и планами, эффективное управление рисками критической инфраструктуры требует сосредоточения внимания на устойчивости. «Устойчивость» относится к способности предотвращать или защищать от значительных рисков, а также минимизировать продолжительность и последствия произошедших инцидентов. Устойчивость требует всесторонней готовности ко всем опасным событиям, которые могут включать кибератаки, физические атаки, стихийные бедствия, механические поломки, человеческие ошибки или любую их комбинацию. Акцент на устойчивости критической инфраструктуры представляет собой отход от традиционной «защиты» КИ. Защита критической инфраструктуры подразумевает способность предотвращать и защищать от любых потенциальных сбоев, а не противостоять им. С другой стороны, устойчивость КИ признает важность успешного управления рисками и инцидентами [4-6], а не просто их избегания. Устойчивость включает в себя защиту, а также эффективное оперативное реагирование.

Эффективное управление рисками КИ фокусируется на повышении устойчивости на основе оценки критичности или важности данной инфраструктуры, а также характера и уровня рисков, с которыми она сталкивается. Заинтересованные стороны совместно определяют наиболее важные для них активы, а затем совместно оценивают, расставляют приоритеты и управляют соответствующими рисками.

Особенно важное значение имеют критические информационные инфраструктуры (КИИ), т.е. обширные и пересекающиеся сети информационно-коммуникационных технологий (ИКТ), которые связывают и эффективно обеспечивают надлежащее функционирование других ключевых инфраструктур. Фактически, КИИ не только поддерживают все другие критические инфраструктуры, но и способствуют наступлению «информационной эпохи».

Однако нефизический характер информационных инфраструктур делает их особенно трудно защищаемыми от возможных сбоев или атак. В результате для управления рисками критических информационных инфраструктур требуется уникальная структура, которая будет использоваться для обеспечения устойчивости традиционных физических инфраструктур.

В отличие от физических активов КИ, таких как здания, плотины или электростанции, критические информационные инфраструктуры являются виртуальными или «логическими» по своей

природе. То есть они состоят из сложных, распределенных систем программного обеспечения, оборудования и услуг, функционирующих вместе для достижения желаемого результата. Из-за такой сильно распределенной природы компьютерных сетей управление рисками для инфраструктур на основе ИКТ в корне отличается от управления рисками для традиционных физических инфраструктур. Структуру, ориентированную на уникальную виртуальную природу критических информационных инфраструктур, можно считать фундаментальной.

В докладе предлагается нисходящая функциональная структура оценки и управления рисками критических информационных инфраструктур (см. рис. 1).

Рис. 1. Управление рисками для критической информационной инфраструктуры

1 Определение области управления рисками

Как и в случае с традиционного управления рисками, управление рисками, ориентированное на значимые объекты КИИ, начинается с определения соответствующих целей и мероприятий по управлению рисками в трех последовательных направлениях:

- достижение консенсуса заинтересованных сторон в части миссии и видении;
- установление конкретных целей, задач и гарантий безопасности и устойчивости;
- определение основных услуг.

Заинтересованные стороны, как в отдельных организациях, так и в критических секторах информационной инфраструктуры, должны сначала определить, что они будут защищать и почему.

С другой стороны, заявление о миссии / видении информационной безопасности и устойчивости для отдельной организации может выглядеть следующим образом:

IT-среда, включающая службы, приложения и инфраструктуру, и которая неявно обеспечивает доступность, конфиденциальность и безопасность для любого пользователя, обеспечивает:

1) не скомпрометированность идентификационных данных,
2) безопасность и доступность ресурсов,
3) конфиденциальность и надежность данных и коммуникаций,
4) определение ролей и ответственности,
5) своевременное реагирование на риски и угрозы.

После формулирования миссии и видения заинтересованные стороны должны определить цели, вспомогательные задачи и гарантии безопасности и устойчивости. В этом контексте:

- цели описывают желаемый результат или возможности высокого уровня;
- вспомогательные задачи относятся к обеспечивающим мероприятиям, помогают достичь поставленные цели;

- гарантиями является государственное законодательство, направленное на укрепление уверенности в безопасности и устойчивости.

Цели обеспечения устойчивости КИИ могут охватывать различные сферы деятельности. Например, они могут включать конкретную программу управления рисками, обмен информацией, ситуационную осведомленность, или реагирование и восстановление. Достижение консенсуса по поставленным целям, вспомогательным задачам и гарантиям, которые их поддерживают, имеет важное значение в задачах управления рисками.

Для достижения консенсуса требуется:

- взаимодействие между заинтересованными сторонами из государственного и частного секторов экономики, поскольку их опыт и участие требуются на протяжении всего процесса управления рисками КИИ;
- поддержка со стороны исполнительной и законодательной ветвей власти, поскольку это свидетельствует о серьезной приверженности кибербезопасности и защите КИИ.

Результатом комплексирования разработанных целей, вспомогательных задач и гарантий обеспечения устойчивости КИИ являются принципы дальнейшей работы, которые можно охарактеризовать как фундаментальная концепция, используемая при проектировании, разработке и эксплуатации безопасных и устойчивых инфраструктур, функций, сетей и систем. Эти принципы:

- позволяют заинтересованным сторонам понять и включить концепции устойчивости и безопасности в проектирование, разработку и эксплуатацию в функции инфраструктуры;
- позволяют создать и распространить политики, требования и руководящие принципы для всей экосистемы КИИ;
- улучшить передачу информации о рисках безопасности между государственными и частными секторами, между отдельными внутренними секторами инфраструктуры, и другими секторами, зависящими от критических инфраструктур.

Особую важность разработки общих принципов для всех этапов жизненного цикла инфраструктуры подчеркивает факт возможности их использования заинтересованными сторонами при создании конкретной системы оперативного реагирования. В частности, они позволяют заинтересованным сторонам КИИ разрабатывать согласованные процессы для получения результатов в части оценки рисков, политики безопасности и отказоустойчивости, а также требования по управлению рисками.

Определение основных организационных «активов» – является еще одной ключевой составляющей определения приемлемых границ деятельности по управлению рисками. Эти «активы» представляют собой основные услуги, процессы или функции, которые позволяют организации добиваться успеха, достигать целей или удовлетворять потребности.

2 Определение функций КИИ

Выявление функций КИИ является следующим шагом в эффективном управлении рисками критической информационной инфраструктуры. На этом этапе заинтересованные стороны определяют, какие элементы информационной инфраструктуры, критические функции и ключевые ресурсы необходимы для предоставления основных государственных услуг, обеспечения упорядоченного функционирования экономики и обеспечения общественной безопасности.

Однако из-за виртуального и не центрированного характера природы функций критическую информационную инфраструктуру нельзя просто «инвентаризировать». Вместо этого функции должны быть определены в соответствии с тем, как они поддерживают основные услуги, включая общее видение заинтересованных сторон, цели и задачи в области безопасности.

Однако не всякая информационная инфраструктура является «критической». Некоторые сети ИКТ играют более важную роль в обеспечении основных функций, чем другие. Например, конкретная компьютерная сеть может не играть никакой роли в критической инфраструктуре, в то время как другая будет играть ключевую роль в предоставлении ключевых услуг, таких как транспорт или энергоснабжение. Используя нисходящую методологию управления рисками, основанную на функциях, заинтересованные стороны КИИ могут сосредоточиться на ключевых аспектах критических информационных инфраструктур, а именно на тех от которых зависят основные услуги, используя ограниченные ресурсы там, где они наиболее необходимы.

На рис. 2 ниже показана взаимосвязь между критическими и некритическими инфраструктурами, как физической, так и виртуальной.

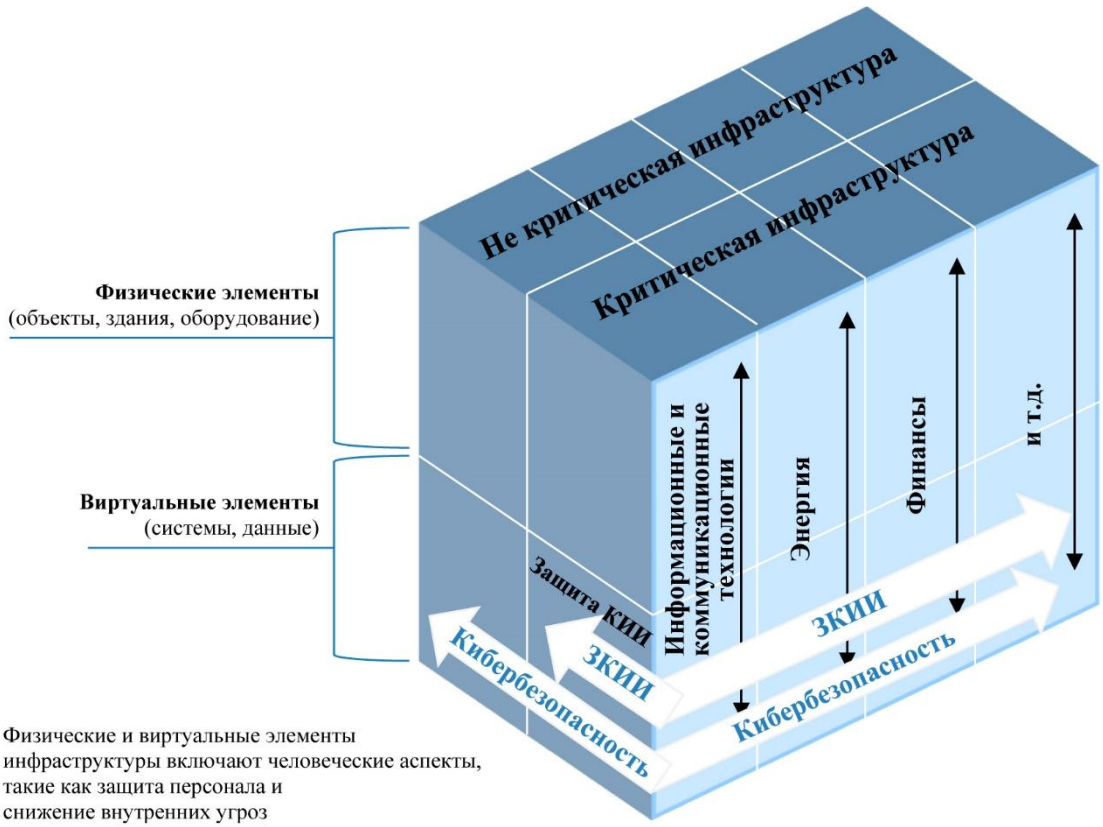

Рис. 2. Взаимосвязь между кибербезопасностью и защитой критической информационной инфраструктуры

Важнейшим компонентом идентификации заинтересованных сторон КИИ является перечисление критических функций на основе:

- выделения всего спектра необходимых элементов;
- группировки элементов ИКТ в логически организованные функциональные конструкции;
- постоянного пересчета критических функций.

Все элементы информационной инфраструктуры должны быть перечислены. В состав этих элементов входят не только физические и кибернетические элементы инфраструктуры, но и процессы и людей, которые непосредственно поддерживают ее деятельность.

После перечисления элементов инфраструктуры [7-9] их необходимо сгруппировать либо в соответствии с предоставляемыми услугами, либо в соответствии с деятельностью КИИ, которую они поддерживают. Например, группирование по предоставляемым услугам может сформировать такие категории, как маршрутизация, услуги интернет-контента и доставка широковещательной информации. С другой стороны, группировка в соответствии с поддерживаемыми видами деятельности критической информационной инфраструктуры может привести к таким категориям, как общесекторальное управление инцидентами или оперативное реагирование. В любом случае эти элементы организованы в соответствии с функциями, которые в случае нарушения могут оказать немедленное и ослабляющее воздействие на основные задачи или услуги инфраструктуры.

Поскольку критичность зависит от ситуации, все критические функции должны постоянно пересчитываться. Другими словами, то, что критично в одном случае, может не быть критичным в другом. В результате идентифицированная и приоритезированная критическая инфраструктура, а также и ключевые функции будут меняться по мере изменения основных услуг, а также по мере развития технологий, инфраструктуры и процессов.

Процесс перечисления критических функций приводит к выводам:

- важные функции, услуги или процессы будут иметь ключевую зависимость от критической информационной инфраструктуры. То есть основные системы ИКТ позволят выполнять эти функции и обеспечивать достижение их целей в области безопасности и устойчивости;
- функции будут состоять из сложных цепочек создания стоимости услуг, охватывающих множество взаимозависимых инфраструктур, одной из которых является КИИ.

Так, например, признанной критической функцией Internet является Служба доменных имен (DNS), состоящая из набора технологий и услуг, предоставляемых владельцами/операторами инфраструктуры и поставщиками, которые в целом обеспечивают критическую функциональность службам более высокого уровня, таким как преобразование имени в IP-адрес. Как и другие критические функции, DNS характеризуется сложной и взаимозависимой цепочкой создания стоимости.

Тем не менее, не существует универсального ответа га вопрос об определении множества функций КИИ. Они могут варьироваться в зависимости от государства или региона и зависят от того, как государство или регион выделяет свои специфические сектора. Ключевым моментом является выбор множества функций КИИ, которое лучше всего описывает зависимости других инфраструктур от рассматриваемой критической информационной инфраструктуры.

3 Анализ цепочки создания стоимости критических функций и взаимосвязей

Третьим шагом в управлении рисками для функций КИИ является понимание и анализ создания стоимости. Стоит отметить, что основные сервисы, процессы и функции не являются целостными сущностями, а скорее представляют собой совокупность интегрированных подкомпонентов, сервисов, процессов и функций, которые совместно обеспечивают достижение поставленной цели. В свою очередь, каждый из этих подкомпонентов состоит из цепочки создания стоимости или поставок (физической или логической), которая имеет важное значение для предоставления и функционирования этой услуги.

Понимание этих сложных и взаимозависимых цепочек создания стоимости не только помогает в анализе угроз, уязвимостей и последствий, но также помогает выявить заинтересованные стороны и ключевых поставщиков в цепочке создания стоимости, которые в противном случае могут быть проигнорированы.

Пример функции КИИ – DNS, рассмотренный ранее, представляет собой пример гипотетической цепочки создания стоимости. Как и большинство важных функций, служба DNS, от которой зависит Internet, не является целостной по своей природе и состоит из множества подфункций, которые совместно обеспечивают позволяют преобразование имен хостов и доменов Internet в IP-адреса. Например, существует подфункция, которая предоставляет услуги регистрации и реестра, позволяющие распознавать доменные имена в Internet. Также существует группа «корневых серверов» DNS, распределенных по всему миру, которые поддерживают информацию об инфраструктуре именования доменов, а также функцию управления DNS, предоставляемую Корпорацией по управлению доменными именами и IP-адресами (Internet Corporation for Assigned Names and Numbers) и другими организациями. Таким образом, всемирная инфраструктура DNS состоит из тысяч DNS-серверов и клиентов, развернутых на предприятиях, в государственных учреждениях, у поставщиков интернет-услуг и у конечных пользователей, на каждом из которых работает множество программ.

Как и все критические функции, функции DNS создают широкий спектр взаимозависимостей, которые необходимо рассматривать в конкретном контексте критичности. Кроме того, необходимо понимать зависимость этих служб от других функций КИИ, таких как маршрутизация и доступ в Internet, а также других секторов критической инфраструктуры, как например, энергетика и транспорт.

4 Оценка риска критической функции

На этапе 4 процесса управления рисками КИИ заинтересованным сторонам необходимо уделять особое внимание угрозам и уязвимостям критических функций [10]. Риск для КИИ является функцией угрозы, уязвимости и последствий, где:

- угроза относится к природным и антропогенным источникам, в части и их движущей силы, целей и возможностей, а также к вероятности того, что угроза существует или возникнет;
- уязвимость – это слабое место или ограничение, которое может быть использовано угрозой;
- последствия – стоимость и коэффициент потерь для оценки риска.

На рис. 3 показана взаимосвязь между риском, угрозами, уязвимостью и последствиями.

Риск критических функций можно оценивать с помощью различных моделей оценки. Фактически, заинтересованные стороны часто используют несколько методов моделирования оценки рисков, чтобы обеспечить полноту и разнообразие оценок. Взаимодополняющими методами моделирования рисков являются сценарный подход [11] и дерево угроз [12].

Сценарный подход моделирования риска для критических функций фокусируется на оценке рисков, возникающих от заранее определенных субъектов угрозы и уязвимостей. Эти субъекты угроз могут быть естественными или созданными руками человека, преднамеренными или непреднамеренными (другими словами, все опасности). Оценка критической информационной инфраструктуры на основе сценарного подхода может быть сосредоточена на конкретных проблемах или угрозах для критических функций. Например, в случае критической функции DNS заинтересованные стороны защиты критической инфраструктуры, вероятно, оценят риск для определенного набора сценариев, которые являются приоритетными для DNS. Они могут включать отравление кэша DNS, атаки с усилением или компрометацию корневого сервера.

Рис. 3. Иллюстрация оценки риска

Однако оценка рисков на основе сценарного подхода не является надежной. Хотя этот подход обеспечивает широкий охват приоритетных угроз и уязвимостей, он не включает сценарии, которые не продуманы теми, кто проводит оценку рисков. Поэтому, несмотря на то что оценка рисков на основе сценарного подхода занимает важное место в оценке рисков КИИ, ее необходимо дополнять оценками на основе других методов.

Метод «дерева угроз» для моделирования рисков КИИ использует концептуальные диаграммы для отображения потенциальных угроз и векторов атак на данную систему. Эти многоуровневые диаграммы или «деревья» состоят из одного «корня», представляющего цель злоумышленника (или нежелательные последствия атаки). «Ветви» этого дерева обозначают условия, которые должны быть выполнены для достижения цели злоумышленника. Изучив полное дерево, заинтересованные стороны могут оценить совокупность потенциальных угроз и уязвимостей для критической функции и принять соответствующие решения по управлению рисками. Эти решения включают принятие, снижение или передачу риска до тех пор, пока не будет достигнут приемлемый уровень.

Анализ дерева угроз является важным дополнением к управлению рисками на основе сценарного подхода, поскольку структура дерева угроз не ограничивается ограниченным набором сценариев, а исследует:

- все уязвимости критических функций;
- все потенциальные субъекты угроз этой критической функции (естественные, техногенные, преднамеренные и непреднамеренные);
- все цели атаки и нежелательные последствия.

Независимо от того, выбирают ли заинтересованные стороны дерево угроз, сценарный подход или комбинированную структуру для управления рисками, они должны направить свои усилия для создания системы оценок или рейтингов.

Одним из распространенных методов профилирования рисков является матрица рисков (также называемая «тепловой картой»), в которой используется таблица для иллюстрации вероятности данного риска и его потенциального воздействия. Другой метод профилирования – диаграмма

разброса рисков. Как и в случае с матрицей рисков, этот метод рассматривает риск с точки зрения вероятности и воздействия (или последствий), но делает это в рамках четырехквадрантного графика. Но независимо от того, как заинтересованные стороны предпочитают иллюстрировать риск, они должны в конечном итоге определить свой «риск-аппетит». Таким образом, после оценки вероятности и воздействия любых рисков заинтересованные стороны должны определить, какие риски являются приемлемыми, а какие нет.

5 Расстановка приоритетов и обработка рисков критических функций

Процесс профилирования и ранжирования рисков неизбежно приводит к множеству опасностей, которые находятся за пределами «риск-аппетита» заинтересованных сторон, что приводит к заключительному шагу в процессе управления рисками КИИ: приоритизации и постоянной обработке неприемлемого риска критической функции. И, конечно же, эти риски должны постоянно учитываться на каждом этапе непрерывного процесса защиты КИ, от предотвращения до готовности, реагирования и восстановления.

Обычно рассматривают 4 варианта непрерывной обработки рисков при защите критической инфраструктуры: снижение рисков, избежание риска, передача или принятие, которые описаны в Таблице 1.

Таблица 1. Варианты обработки риска

Варианты обработки риска	Описание/определение
Снижение риска	Выборочное применение соответствующих методов и принципов управления для уменьшения вероятности возникновения, его последствий или того и другого. К ним относятся планы и процессы, которые позволяют организации избегать, предотвращать или ограничивать влияние возникающего инцидента, в том числе посредством соблюдения корпоративной политики, стратегий смягчения последствий, поведения и программ.
Избежание риска	Принятие мер, полностью исключающих рассматриваемый риск.
Передача риска	Передача ответственности за риск другой стороне при сохранении существующего риска на основе законодательства, контракта, страхования или других средств.
Принятие риска	Обоснованное решение принять вероятность и влияние определенного риска.

Например, в типовом отделе информационной безопасности управление рисками может включать простое развертывание определенных элементов управления ИТ (таких как пароли или брандмауэры) для снижения вероятности или последствий риска. Однако в сфере КИИ обработка рисков является более тонким и сложным. Заинтересованные стороны КИИ рассматривают риск с точки зрения критических функций, а это означает, что варианты обработки рисков на этом уровне больше похожи на стратегии и приоритеты, чем на фактические средства контроля. Например, на этом уровне может быть принято решение о наборе стандартов и практик, которые повышают безопасность и устойчивость, и будут реализованы для всех критических функций информационной инфраструктуры.

Исследования также играют важную роль в обработке рисков, поскольку многие проблемы, связанные с обеспечением устойчивости КИИ, не решаются с использованием существующих технологий. Таким образом, определение приоритетов исследований является важным компонентом повышения безопасности и устойчивости в долгосрочной перспективе.

Заключение

В докладе рассматривается подход управления рисками критической информационной инфраструктуры, состоящий из следующих этапов:

1) определение области управления рисками,
2) определение функций КИИ,
3) анализ цепочки создания стоимости критических функций и взаимосвязей,
4) оценка риска критических функций,
5) расстановка приоритетов и обработка рисков критических функций.

Процесс управления рисками КИИ, с учетом меняющегося ландшафта угроз, развитие технологий и совершенствования политик, будет успешным только в контексте постоянной деятельности по управлению рисками на всем жизненном цикле защиты критической инфраструктуры, включающем предотвращение, готовность, реагирование и восстановление.

Литература

1. *Markopoulou D., Papakonstantinou V.* The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular // Computer Law & Security Review. Vol. 41. 2021, 105502.
2. *Alcaide J.I., Llave R.G.* Critical infrastructures cybersecurity and the maritime sector // Transportation Research Procedia. Vol. 45. 2020. – P.547-554.
3. Maglaras L.A., Kim K.H., Janicke H., Ferrag M.A., Rallis S., Fragkou P., Maglaras A., Cruz T.J. Cyber security of critical infrastructures. // ICT Express. Vol. 4. 2018, iss. 1. – P.42-45.
4. *Kalashnikov A.O, Sakrutina E.A.* Safety management system and Significant Plants of Critical Information Infrastructure / IFAC-PapersOnLine. 2019. Vol. 52, no. 13. – P.1391-1396.
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 рискового потенциала объектов критической инфраструктуры атомных электростанций // Труды 11-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD’2018, Москва) , под общей редакцией С.Н.Васильева, А.Д.Цвиркуна,– М.: ИПУ РАН, 2018. Т. 2. – С.457-461.
7. *Herrera L.C., Maennel O.* A comprehensive instrument for identifying critical information infrastructure services // International Journal of Critical Infrastructure Protection. Vol. 50. 2019. – P.50-61.
8. *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.
9. *Промыслов В.Г., Семенков К.В., Шумов А.С.* Синтез архитектуры кибербезопасности для систем управления атомных станций // Проблемы управления. 2019. № 3. – С. 61-71.
10. *Сакрутина Е.А., Калашников А.О.* Анализ кибербезопасности значимого объекта критической информационной инфраструктуры / Труды 13-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2020, Москва) , под общей редакцией С.Н.Васильева, А.Д.Цвиркуна, М.: ИПУ РАН, 2020. – С.1445-1452.
11. *Ahmad A., Maynard S.B., Desouza K.C., Kotsias J., Whitty M.T., Baskerville R.L.* How can organizations develop situation awareness for incident response: A case study of management practice // Computers and Security. Vol. 101:102122. 2021.
12. *Henriques de Gusmão A.P., Mendonça Silva M., Poleto T., Camara e Silva L., Cabral Seixas Costa A.P.* Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory // International Journal of Information Management. Vol. 43. 2018. – P.248-260.