Концепция предоставления услуг группами реагирования на инциденты в сфере безопасности (SIRT)

Версия 1.0

Концепция предоставления услуг SIRT

Введение

Ниже представлены перечень услуг, возможность предоставления которых для удовлетворения потребностей своих клиентов может рассмотреть группа реагирования на инциденты в сфере безопасности (SIRT), а также механизмы устранения пробелов в том, что касается обеспечения способности удовлетворения таких потребностей. Данный перечень направлен на то, чтобы охватить как традиционные услуги, предоставляемые SIRT, так и услуги, которые появились недавно и которые существующие группы и организации внедряют по мере их появления. В настоящем документе приведены те услуги, которые необходимо включить в Концепцию предоставления услуг SIRT.

Все представленные ниже услуги разделены на основные и второстепенные функции, способствующие предоставлению SIRT той или иной услуги в рамках выполнения более широких задач. Учтите, что многие из этих основных и второстепенных функций обеспечивают предоставление множества услуг и/или выполнение множества функций и могут быть взаимозаменяемыми, хоть в данном документе они и представлены как уникальные. Несмотря на то, что существование такой взаимосвязи признается в данном документе, на данном этапе ее определение не входит в его задачи.

В будущем группирование услуг будет осуществляться на основании предоставления схожих услуг в рамках той или иной сферы обслуживания. На первоначальном этапе внимание данного документа будет сосредоточено на трех видах групп реагирования на инциденты: национальная группа реагирования на нарушения компьютерной безопасности (CSIRT), отраслевая CSIRT (важнейшая инфраструктура) и ведомственная CSIRT (на уровне той или иной организации). В последующей версии данной концепции будут добавлены еще два дополнительных вида: группа реагирования на инциденты в сфере безопасности продукции (PSIRT) и региональная / многосторонняя группа реагирования на инциденты. Примеры всех видов групп, а также описание сфер обслуживания / услуг / функций, как правило, учитываемых при разработке базовой программы, будут приведены в будущих приложениях. Кроме того, для разработки учебных модулей будет издан дополнительный документ с общей информацией об основных и второстепенных задачах, а также о действиях, необходимых для обеспечения выполнения каждой из второстепенных функций. Достижение соответствующего уровня

зрелости координируется с несколькими сторонами, чтобы наши усилия на глобальном уровне были направлены на получение общего результата.

Цель

В Концепции предоставления услуг CSIRT описан комплекс услуг и функций, внедряемых CSIRT в рамках обслуживания своей клиентуры. Цель данного документа заключается в том, чтобы содействовать обеспечению функциональной совместимости CSIRT, проведению мероприятий по развитию потенциала на общемировом уровне, а также обучению и профессиональной подготовке, путем использования общепринятых терминологии и подходов в отношении деятельности CSIRT.

Историческая справка

Во многих случаях перечень услуг CERT/CC CSIRT служит источником согласованной и сопоставимой информации о CSIRT и предоставляемых ею соответствующих услуг. В ходе недавних исследований, направленных на изучение существующих услуг CSIRT, было установлено, что несмотря на свое широкое использование и адаптацию, перечень CERT/CC устарел, и в нем отсутствуют основные компоненты, составляющие стоящую перед современными CSIRT задачу. Стремясь содействовать развитию и становлению CSIRT по всему миру, FIRST признал, что это является одним из ключевых элементов формирования основы для разработки комплексной учебной программы в области CSIRT. Учитывая географическое и функциональное разнообразие членов FIRST, было установлено, что представляемое им сообщество является подходящим источником формирования характеристики и структуры предоставляемых CSIRT услуг. Кроме того, было установлено, что подобный подход необходимо применить и в отношении услуг PSIRT, включив его в будущем в последующую версию данной концепции.

Определения

Мы даем определения тем или иным терминам в контексте их использования в данном документе. Примите к сведению, что сферы обслуживания, услуги и функции указывают на то, *что* делается на том или ином уровне деятельности группы, в то время как задачи и действия указывают на то, *как* это делается на том или ином уровне ее деятельности. Информация по задачам и действиям публикуется в приложении и может / будет обновляться чаще:

- **Сфера обслуживания** – групповые услуги, связанные наличием общей характеристики. Они помогают упорядочить услуги путем их тщательного распределения на группы, чтобы сделать их более понятными. (В версии 2.0. данный раздел будет доработан)
- **Услуга** – комплекс узнаваемых, связанных между собой действий, направленных на достижение того или иного результата и проводимых от имени или в интересах

клиентуры группы реагирования на инциденты. Перечень функций, необходимых для предоставления услуги.

- **Функция** – средства или способы достижения цели или выполнения задачи в рамках той или иной услуги. Перечень задач, которые можно выполнить в рамках той или иной функции.

- **Задачи** – перечень действий, которые необходимо предпринять для выполнения той или иной задачи.

- **Действия** – перечень способов осуществления каких-либо процессов на различных уровнях деятельности группы / при различной степени ее зрелости.

- **Возможность** – измеряемая деятельность, которую можно осуществить в рамках функций и обязательств организации. В целях данной концепции предоставления услуг SIRT возможности могут быть определены либо как услуги в более широком контексте, либо как необходимые функции, подфункции, задачи или действия.

- **Потенциал** – количество случаев единовременного возникновения той или иной возможности, которой организация может воспользоваться до того, как ее ресурсы будут в той или иной степени исчерпаны.

- **Зрелость** – насколько эффективно организация использует ту или иную возможность в рамках поставленных перед ней задач и переданных ей полномочий. Это уровень квалификации, приобретаемой в ходе осуществления действий или выполнения задач или же в результате совокупности осуществления функций и предоставления услуг.

Виды групп реагирования на инциденты

- Национальная CSIRT (группа реагирования на нарушения компьютерной безопасности) – под национальной CSIRT подразумевается организация, учрежденная органом государственной власти для координации реагирования на нарушение кибербезопасности на национальном уровне. К ее клиентуре, как правило, принадлежат, среди прочего, все государственные департаменты и ведомства, правоохранительные органы и институты гражданского общества. Кроме того, такая CSIRT, как правило, является тем органом, который отвечает за взаимодействие с национальными CSIRT других стран, а также с региональными и международными игроками.

- Отраслевая CSIRT / CSIRT по важнейшей инфраструктуре – отвечает за мониторинг, управление и реагирование на инциденты в области кибербезопасности в конкретной отрасли (например, энергетика, электросвязь, финансы).

- Ведомственная (на уровне организации) CSIRT – под ведомственной CSIRT, как правило, подразумевается группа, отвечающая за мониторинг, управление и обработку

инцидентов в области кибербезопасности, оказывающих воздействие на внутренние услуги и инфраструктуру ИКТ конкретной организации.

- Региональная / многосторонняя CSIRT – под региональной / многосторонней CSIRT подразумевается группа, в том числе основная, отвечающая за мониторинг, управление и реагирование на инциденты в области кибербезопасности в конкретном регионе или ряде организаций.

- Группа реагирования на инциденты в сфере безопасности продукции (PSIRT) – под PSIRT подразумевается группа в структуре коммерческой организации (как правило, организации-поставщика), отвечающей за получение, рассмотрение, предоставление в рамках внутренней отчетности и обнародование информации об уязвимости защиты товаров или услуг, которые организация вводит в коммерческий оборот.

Услуга 1. Управление инцидентами

Функция 1.1. **Обработка инцидентов:** услуги по управлению киберинцидентами, включая оповещение клиентуры и координация действий по реагированию на инциденты, смягчению их последствий и восстановлению после них. Обработка инцидентов зависима от аналитической деятельности, описанной в разделе "Анализ".

Подфункция 1.1.1. **Сбор информации:** услуги по получению, каталогизации и хранению связанной с различными происшествиями и инцидентами информации, в том числе:

- **Сбор отчетности по инцидентам:** сбор отчетов касательно вредоносных и подозрительных происшествий и инцидентов, предоставляемых клиентами и третьими лицами (такими как другие группы по безопасности или источники коммерческой информации), независимо от формы подачи таких отчетов: ручной, автоматической или машиночитаемой.
- **Сбор цифровых данных:** сбор и каталогизация цифровых данных, которые могут, хоть и не гарантировано, оказаться полезными для понимания связанной с инцидентами деятельности (например, изображения диска, файлы, сетевые журналы/потоки сети).
- **Другие виды данных (нецифровых):** сбор и каталогизация нецифровых данных (журналы посещения в неэлектронной форме, архитектурные схемы, бизнес-модели, данные по оценке тех или иных объектов, политика, концепции управления корпоративными рисками и т. д.).

- **Сбор артефактов:** бизнес-процессы и технические процессы, необходимые для получения, каталогизации, хранения и отслеживания артефактов, которые, как считается, остались от враждебной деятельности.
- **Сбор доказательств:** деятельность, направленная на сбор информации и данных в целях возможного использования правоохранительными органами, что часто включает сбор метаданных относительно источника, метода сбора и собственника информации, а также обеспечение сохранности информации.

Подфункция 1.1.2. **Реагирование:** услуги по снижению степени воздействия инцидента и принятию мер, направленных на возобновление бизнес-функций клиентов.

- **Сдерживание:** прекращение нанесения прямого ущерба и снижение степени вредоносной деятельности путем осуществления краткосрочных тактических действий (например, блокирование и фильтрация трафика); также может предусматривать возвращение контроля над системами.
- **Смягчение последствий:** предотвращение нанесения дальнейшего ущерба путем устранения его источника, применения временных решений или внедрения более глубоких и комплексных стратегий сдерживания.
- **Ремонт:** внесение изменений в пострадавшей области, инфраструктуре или сети, необходимых для установления и предотвращения повторения такой деятельности в будущем. Такие действия предусматривают, среди прочего, усиление степени защиты и готовности организации путем внесения изменений в ее политику, а также проведения обучения и профессиональной подготовки.
- **Восстановление:** возобновление целостности пострадавших систем и возвращение затронутых данных, систем и сетей в нормальное функциональное состояние.

Подфункция 1.1.3. **Координирование:** обмен информацией с CSIRT и предоставление ей консультаций с привлечением как внутренних, так и внешних ресурсов. Такие действия, как правило, имеют место тогда, когда с целью осуществления действий, необходимых для смягчения последствий инцидента, CSIRT полагается на специальные знания и опыт, а также ресурсы, не находящиеся под ее непосредственным контролем. Предлагая услуги двустороннего или многостороннего координирования, CSIRT участвует в обмене информацией, чтобы дать возможность таким ресурсам предпринять соответствующие действия или помочь другим лицам выявить, предупредить или устранить существующую враждебную деятельность.

Подфункция 1.1.4. **Отслеживание инцидентов:** документирование информации о действиях, предпринятых для разрешения инцидента, включая собранную критическую информацию, данные о проведенном анализе, принятых мерах по устранению инцидента и смягчению его последствий, а также разрешению инцидента и закрытии соответствующего вопроса.

Функция 1.2. **Уязвимость, конфигурация и управление ресурсами:** услуги, связанные с пониманием и устранением уязвимостей, а также вопросами конфигурации и учета ресурсов.

Подфункция 1.2.1. **Исследование, направленное на выявление уязвимостей:** выявление новых уязвимостей методом изучения и экспериментирования (например, нечеткое тестирование и обратный инжиниринг).

Подфункция 1.2.2. **Сообщение об уязвимостях:** бизнес-процессы и технические процессы, направленные на получение, каталогизацию, хранение и отслеживание сообщений об уязвимостях.

Подфункция 1.2.3. **Координация работы с уязвимостями:** информирование соответствующих организаций о наличии уязвимости с целью воздействовать на проведение ремонтных работ и ограничить возможные последствия использования эксплойтов.

Подфункция 1.2.4. **Устранение основной причины уязвимости:** осуществление регламентированных корректирующих действий, необходимых для исправления выявленной уязвимости. Как правило, такие действия осуществляются поставщиком продукции.

Услуга 2. Анализ

Функция 2.1. **Анализ инцидентов:** услуги, связанные с определением и описанием информации о происшествиях и инцидентах, например информации о масштабе, пострадавших сторонах, вовлеченных системах, временных рамках (выявление, возникновение и информирование), статусе (продолжающийся или завершенный). [Примечание: более тщательный анализ инцидента проводится в рамках других, более специализированных аналитических задач, например задач по анализу артефактов, неправильной конфигурации, уязвимостей, сетей или данных для экспертно-технического анализа.]

Подфункция 2.1.1. **Проверка инцидента:** проведение достоверной проверки, направленной на установление того, что инцидент, о котором сообщалось, действительно имел место, оказав в некоторой степени воздействие на вовлеченные системы.

Цель: предоставить техническое доказательство того, что происшествие является инцидентом в сфере безопасности, ошибкой сети или аппаратного обеспечения, и установить возможное воздействие на безопасность и соответствующий ущерб в контексте конфиденциальности, доступности и/или целостности информационных ресурсов.

***Результат**: установить, действительно ли происшествие, о котором сообщалось, является инцидентом, требующим обработки, или же такое сообщение может быть зарегистрировано в соответствующих системах, и данный вопрос может быть закрыт без принятия дальнейших действий. Установить детали происшествий, в результате которых клиент посчитал, что действительно имел место инцидент в сфере безопасности, а также установить, является ли такой инцидент злонамеренным или же в его основе лежат другие причины, такие как неправильная конфигурация или отказ аппаратного обеспечения.*

Подфункция 2.1.2. **Анализ воздействия:** выявление и описание воздействия на бизнес-функцию, выполнение которой обеспечивается вовлеченными системами.

Цель: определить размер и масштаб инцидента, в том числе пострадавших частей инфраструктуры, услуг, данных, департамента или организации. По результатам данного анализа может быть применен общий подход к устранению инцидента.

***Результат**: установить (потенциальный) ущерб, который инцидент нанес или мог нанести. Учитывать не только технические аспекты, но и освещение в масс-медиа, потерю доверия или авторитета, а также какой-либо ущерб репутации.*

Подфункция 2.1.3. **Извлеченные уроки:** повторное рассмотрение после осуществления действий с целью определить улучшения в области процессов, политики, процедур, ресурсов и инструментов, способствуя таким образом смягчению последствий и предотвращению нарушений в будущем.

> **Цель:** установить, что пошло не так, принять превентивные меры и обменяться информацией об извлеченных уроках с сообществом в области безопасности путем опубликования такой информации и проведения соответствующих презентаций.
>
> ***Результат**: комплекс рекомендаций, которые необходимо рассмотреть в качестве потенциальных изменений в работе информационных систем, процессов и процедур соответствующего департамента пострадавшей организации.*

Функция 2.2. **Анализ артефактов:** услуги, связанные с пониманием возможностей и намерений артефактов (например, вредоносные программные средства, эксплойты, спам и файлы конфигурации), а также их исполнением, обнаружением и нейтрализацией.

> ***Цель:** в рамках процесса обработки инцидентов цифровые артефакты можно найти в пострадавших системах или в местах распространения вредоносных программных средств. Артефактами могут служить следы попыток несанкционированного доступа, такие как скрипты, файлы, изображения, файлы конфигурации, инструменты, результаты их использования, журналы и т. п. Анализ артефактов проводится, чтобы выяснить, как нарушитель мог использовать артефакт, например для получения доступа в системы или сети организации, или что нарушитель делал в системе. Анализ артефактов направлен на то, чтобы установить, как артефакт функционирует сам по себе или в комбинации с другими артефактами. Сделать это можно путем проведения различных мероприятий: анализ состояния поверхности носителя, обратный инжиниринг, динамический анализ и сравнительный анализ. Каждое мероприятие позволяет получить дополнительную информацию об артефакте. Методы анализа включают, среди прочего, определение вида и характеристик артефакта, его сравнение с известными артефактами, наблюдение за исполнением артефакта в динамике, а также разборку и интерпретацию двоичных артефактов. Анализируя артефакт(ы), аналитик стремиться воспроизвести и установить действия нарушителя, чтобы можно было оценить ущерб, разработать решения, позволяющие смягчить последствия использования артефакта, а также предоставить информацию клиентам и другим исследователям.*

Результат: *понять природу восстановленного цифрового артефакта, а также его связь с другими артефактами, атаками и использованными уязвимостями. Найти способы смягчения последствий использования анализируемого(ых) артефакта(ов), определив тактику, методы и порядок действия нарушителей, направленных на получение несанкционированного доступа к системам и сетям и осуществление вредоносной деятельности.*

Подфункция 2.2.1. **Анализ состояния поверхности носителя**: выявление и описание основной информации и метаданных об артефактах (например, тип файла, выходная строковая последовательность, криптографические хэши, размер файла, название файла), а также анализ общедоступной и частной информации об артефакте.

Цель: *являясь первым шагом в процессе сбора базовой информации, анализ состояния поверхности носителя позволяет сравнить полученную от артефакта информацию с информацией, полученной от других общедоступных и принадлежащих частным лицам артефактов, а также (или) от репозитория подписей. Вся известная информация (например, информация о возможном ущербе, функциональности и способах смягчения последствий) собирается и анализируется. Необходимость дальнейшего анализа зависит от того, какова задача текущего анализа.*

Результат*: определить характеристики и/или подпись цифрового артефакта, а также всю известную информацию о нем, включая информацию о его вредоносности, воздействии и способах смягчения последствий его использования.*[1] *(На основе такой информации можно определить последующие шаги.)*

Подфункция 2.2.2. **Обратный инжиниринг:** анализ статических характеристик артефакта определит, насколько полнофункциональным он является, независимо от среды, в которой может проходить его исполнение.

Цель: *для проведения более глубокого анализа вредоносных артефактов, включая обнаружение скрытых действий и команд инициирования. Обратный инжиниринг позволяет аналитику обойти любые запутанные места и компиляции (для бинарных артефактов) и обнаружить программу, скрипт или код, составляющий вредоносное программное средство, либо найдя исходный код, либо разобрав двоичный артефакт с целью установления и интерпретации языка его сборки. Полное определение машинного языка показывает, какие функции и действия*

может осуществлять вредоносное программное средство. Обратный инжиниринг представляет собой более глубокий анализ, проводимый тогда, когда анализ состояния поверхности носителя и динамический анализ не могут дать всю необходимую информацию.

***Результат**: установить полную функциональность цифрового артефакта, чтобы понять, как он функционирует, как осуществляемые им действия инициируются, какие в связанных системах существуют слабые места, которыми можно воспользоваться, каково полное воздействие артефакта и каков наносимый им потенциальный ущерб; на основании этого разработать решения, позволяющие смягчить последствия использования артефакта и при необходимости создать новую подпись для сравнения с другими образцами.*

Подфункция 2.2.3. **Динамический анализ:** понимание возможностей артефакта путем наблюдения за работой образца в реальной или эмулированной среде (например, тестовая или виртуальная среда, эмуляторы программного или аппаратного обеспечения).

***Цель:** дать представление о том, как работает артефакт. Использование эмулированной среды позволяет зафиксировать изменения хоста, сетевого трафика и результатов исполнения. Основная идея заключается в том, чтобы попытаться увидеть артефакт в действии в ситуации, максимально приближенной к реальной.*

***Результат**: получить дополнительную информацию о работе цифрового артефакта, наблюдая за его поведением в процессе исполнения, с целью определить изменения в системе пострадавшего хоста, взаимодействие других систем и полученный таким образом сетевой трафик, что позволит лучше понять ущерб, нанесенный системе, и воздействие на нее, а также создать новую(ые) подпись(си) артефакта и определить способы смягчения последствий его использования. (Примечание: динамический анализ не позволяет увидеть полную функциональность артефакта, так как не все разделы кода артефакта можно инициировать. Динамический анализ не позволяет аналитику увидеть каковы все возможности вредоносного программного средства, а лишь, что оно делает в тестовой ситуации.)*

Подфункция 2.2.4. **Сравнительный анализ:** анализ направлен на определение типовой функциональности и намерений, в том числе на основе анализа целого класса каталогизированных артефактов.

***Цель:** изучить связь артефакта с другими артефактами. Это может помочь выявить общие черты в отношении кода, образа действия, целей, намерений и авторов. На основании таких общих черт можно определить масштаб атаки (например, не преследует ли она более значимую цель, не использовался ли похожий*

код ранее и т. п.). Методы сравнительного анализа могут включать сравнение на основе аналогов или сравнение на основе общих черт кода. Сравнительный анализ дает более широкое представление о том, как артефакт или его аналоги использовались и как они изменились со временем, что помогает понять оценку вредоносного программного средства или других вредоносных видов артефактов.

***Результат**: определить общие черты или взаимосвязь между артефактами с целью выявить тенденции или сходство, что позволит лучше понять или получить дополнительную информацию о функциональности, воздействии и способах смягчения последствий использования цифровых артефактов.*

Функция 2.3. **Анализ мультимедийной информации:** услуги, предусматривающие, среди прочего, анализ соответствующих данных систем, сетей, цифровых запоминающих устройств и съемных носителей с целью лучше понять, как можно предотвратить, обнаружить схожие или взаимосвязанные инциденты, а также смягчить их последствия. Такие услуги могут способствовать предоставлению информации в целях проведения юридического и экспертно-технического анализа, анализа на нормативно-правовое соответствие, а также других видов статистического анализа информации.

***Цель:** собрать и проанализировать доказательства, полученные на основе носителей информации, таких как жесткие диски, мобильные устройства, съемные носители, облачные хранилища или носители другого формата, включая бумажные носители и видеоносители. Если результаты анализа предназначены для представления в юридическом контексте или контексте нормативно-правового соответствия, сбор такой информации необходимо осуществлять в соответствии с принципами экспертно-технического анализа, который позволяет сохранить целостность доказательств с соблюдением правил передачи ответственности. Такие доказательства могут включать артефакты, такие как оставленные вредоносные программные средства; изменения в состоянии файлов, регистры и другие системные компоненты; данные учета сетевого трафика и другие файлы регистрации, а также информация в памяти. Учтите, что анализ мультимедийной информации направлен на поиск доказательств того, что произошло, и он отличается от анализа артефактов, цель которого – понять один артефакт и касающиеся его взаимосвязи. Тем не менее методы анализа артефактов можно применять в рамках анализа мультимедийной информации. Кроме того, к таким услугам можно прибегнуть не только в случае киберинцидентов, но и при рассмотрении вопросов, связанных с людскими ресурсами, или других правовых или организационных вопросов.*

***Результат:** представить выводы, 1) обеспечивающие учет информационных ресурсов (например, найденная интеллектуальная собственность или другая конфиденциальная*

информация); 2) отображающие хронологию событий, которая может выявить какие-либо дополнения, изменения или удаления в отношении мультимедийных ресурсов, вовлеченных в инцидент, а также установить, кто осуществил или что осуществило соответствующие действия, если это возможно, и как все эти доказательства, во взаимосвязи между собой, объясняют степень и воздействие инцидента.

Функция 2.4. **Анализ уязвимостей / использования эксплойтов:** услуги, направленные на обеспечение более глубокого понимания уязвимостей, вызвавших киберинцидент.

Подфункция 2.4.1. **Анализ технической уязвимости (вредоносных программных средств) / эксплойтов:** понимание слабых(ой) сторон(ы), использованных для создания инцидента, и вредоносных навыков, примененных для использования таких слабых сторон.

Цель: проинформировать клиентуру обо всех известных уязвимостях (стандартных точках входа для нарушителей) с целью обеспечить обновление и мониторинг систем на наличие эксплойтов, минимизировав таким образом любое негативное воздействие.

***Результат**: иметь полное представление об уязвимости и о том, каким образом злоумышленники смогут воспользоваться такой уязвимостью для проникновения и эксплуатации систем.*

Подфункция 2.4.2. **Анализ основных причин:** понимание дефектов разработки и внедрения, позволивших атаке произойти.

Цель: определить основную причину и точку нарушения, что поможет полностью устранить проблему.

***Результат**: иметь четкое представление об обстоятельствах, допускающих наличие уязвимости и таким образом позволяющих нарушителю использовать такую уязвимость.*

Подфункция 2.4.3. **Анализ способов устранения:** понимание того, какие шаги необходимы для устранения основополагающих дефектов, позволивших атаке произойти, и предотвращения такой атаки в будущем.

Цель: установить проблему, в результате которой нарушение стало возможным, осуществить корректировку уязвимости, изменить процедуру или дизайн, обеспечить оценку способов устранения третьей стороной и определить, не было ли на этапе устранения допущено появление каких-либо новых уязвимостей.

***Результат**: разработать план действий, направленный на усовершенствование процессов, инфраструктуры и дизайна для блокирования конкретной направленности атаки и предотвращения такой атаки в будущем.*

Подфункция 2.4.4. **Анализ способов смягчения последствий:** анализ, направленный на определение способов снижения (предупреждения) рисков, возникших в результате атаки или уязвимости, без необходимости устранения основополагающего дефекта, допустившего такую атаку или уязвимость.

Услуга 3. Обеспечение безопасности информации

Функция 3.1. **Оценка рисков / нормативно-правового соответствия:** услуги, связанные с оценкой рисков или нормативно-правового соответствия. К таким услугам может относиться как проведение непосредственно оценки, так и помощь в анализе результатов оценки. Как правило, проводится в рамках выполнения требования о соответствии (например, ISO 27XXX, COBIT).

Цель: улучшить процесс определения возможностей и угроз; улучшить механизмы контроля; улучшить процесс предотвращения потерь и управления инцидентами, а также обеспечения информационной безопасности и выполнения других соответствующих функций.

Результат: **последовательный процесс оценки и управления информационными рисками в отношении ключевых активов и данных; содействие оценке рисков; определение соответствующих вариантов работы с рисками, включая при необходимости управление инцидентами и экспертно-технический анализ.**

Подфункция 3.1.1. **Учет особо важных активов/данных:** определение ключевых активов и данных, имеющих решающее значение для выполнения миссии организации. Такие активы и данные необязательно должны принадлежать организации (например, поставщик облачных услуг или внешний набор данных). Данные действия предусматривают, среди прочего, определение местоположения и владельца таких активов и данных, уровня их конфиденциальности, функции обеспечения выполнения их миссии, а также их текущего статуса / уровня.

Цель: регулярно определять такие активы и данные, если управление инцидентами необходимо организации для выполнения своей миссии наряду с осуществлением соответствующей деятельности.

Результат: *регулярно обновляемый реестр, список или база данных ключевых активов и данных для использования организацией при проведении оценки рисков.*

Подфункция 3.1.2. **Определение стандарта проведения оценки:** получение руководителями высшего звена политик(и) управления рисками организации и перечисленных/установленных стандартов для проведения оценки уровня/статуса безопасности. Предложение критериев оценки или установления контрольных показателей на рассмотрение менеджерам по вопросам рисков и главным директорам по информационной безопасности предприятия. К примерам стандартов, среди прочего, могут относиться Базель II, COBIT, ITIL, сертификация и аккредитация.

Цель: помогать в выборе утвержденной методики оценки информационных рисков для использования в организации, а также предоставлять входные данные для проведения более широкой оценки рисков и управления рисками на уровне организации в целом.

Результат: *выбранная методика оценки информационных рисков, используемая на всех уровнях организации; поддержка и помощь на уровне руководства высшего звена по внедрению выбранной методики; политики организации, предусматривающие в соответствующих случаях применение выбранной методики оценки рисков; согласованные мероприятия, шаблоны и промежуточные результаты; согласованные процесс и процедуры оценки информационных рисков; согласованные механизмы внедрения результатов оценки информационных рисков в меры по управлению рисками и в процесс принятия решений на уровне организации.*

Подфункция 3.1.3. **Проведение оценки:** помогать в осуществлении анализа и содействовать участию в проведении оценок с целью обеспечения выполнения / учета требований относительно риска и безопасности.

Цель: осуществлять максимально полную оценку информационных рисков в отношении выбранного ключевого актива или данных с использованием утвержденной методики.

Результат: *осуществленная оценка информационных рисков в отношении выбранного ключевого актива или данных.*

Подфункция 3.1.4. **Выводы и рекомендации:** выработка и предоставление результатов оценки, отчетов и/или рекомендаций (напр., составление отчета, использование соответствующих заданий в публикации или информации).

Цель: содействовать осуществлению полного документирования результатов проведенной оценки рисков, а также перечислить действия, которые следует предпринять, и рекомендации, которые следует учесть по итогам оценки.

Результат: *официальный, утвержденный отчет, содержащий подробную информацию о важнейшем активе или данных, реализованном процессе оценки рисков, данных, использованных при оценке рисков, итоги, рекомендации, действия, планы и временные рамки распространения отчета.*

Подфункция 3.1.5. **Отслеживание:** оказывать содействие главному директору по информационной безопасности и/или менеджеру по вопросам рисков в отслеживании как статуса оценок, так и дальнейшего внедрения рекомендаций.

Цель: обеспечить соблюдение планов, осуществление действий и выполнение рекомендаций в соответствии с зафиксированными временными рамками.

Результат: *регулярный анализ планов и временных рамок; перечень предпринятых действий; внесение изменений во временные рамки в случае несвоевременного осуществления действий; отчет о проделанной работе в сравнении с планами и установленными временными рамками.*

Подфункция 3.1.6. **Тестирование:** активное тестирование на соответствие уровням риска. Может включать в себя тест на проникновение, сканирование и оценку уязвимостей, а также оценку, тестирование приложений, аудит и верификацию и т. п.

Цель: проверить, соответствует(ют) ли поставленной цели выбранная(ые) и внедренная(ые) мера(ы) в отношение риска, реализована(ы) ли она (они) правильно, а также были ли приняты ожидаемые меры по снижению рисков.

Результат: *задокументированный план теста с ожидаемыми результатами; задокументированные тесты и результаты; сопоставление с ожидаемыми результатами; действия и временные рамки по исправлению любых несоответствий с ожиданиями.*

Функция 3.2. **Управление корректировками:** услуги, содействующие обеспечению клиентов необходимыми возможностями для управления определением инвентарного списка, систем, подлежащих корректировке, развертывания и верификации установки корректировок.

Цель: помогать при определении, приобретении, установке и верификации корректировок для продукции и систем, а также осуществлять оценку рентабельности и воздействия корректировок с точки зрения управления инцидентами.

Результат: *осведомленность об организации и понимание необходимых корректировок; понимание корректировок, которые должны применять поставщики услуг; понимания воздействия корректировок на информационные риски; понимание их воздействия на управление инцидентами.*

Функция 3.3. **Управление эксплуатационной политикой:** услуги по разработке, эксплуатации, институционализации и применению концепции осуществления деятельности организации, а также других политик.

Цель: выступать в качестве надежного консультанта для клиента или отрасли по вопросам обеспечения непрерывной деятельности и восстановления после бедствий путем предоставления объективных, основывающихся на фактах консультаций с учетом рассматриваемой возможности или проблемы, среды, в которой может быть применен предоставленный совет, а также любых применимых ограничений в отношении ресурсов.

Результат: *решения относительно деятельности компании, учитывающие особенности обеспечения непрерывной деятельности и восстановления после бедствий; управление инцидентами в качестве надежного консультанта; члены группы по управлению инцидентами участвуют, в соответствующих случаях, в принятии решений относительно деятельности компании.*

Функция 3.4. **Анализ рисков/консультации по вопросам восстановления после бедствий с обеспечением непрерывной деятельности:** услуги, предоставляемые клиенту, связанные с мерами по обеспечению непрерывной деятельности организации с учетом выявленных рисков. К ним может относиться ряд мер по управлению рисками: от проведения оценки до содействия анализу при оценке и снижении уровня воздействия результатов оценки.

> **Цель:** выступать в качестве надежного консультанта для клиентуры или отрасли по вопросам информационной безопасности и управления инцидентами путем предоставления объективных, основывающихся на фактах консультаций с учетом рассматриваемой возможности или проблемы, среды, в которой может быть применен предоставленный совет, а также любых применимых ограничений в отношении ресурсов.

> ***Результат:*** *решения относительно деятельности компании, учитывающие особенности информационной безопасности и управления инцидентами; управление инцидентами в качестве надежного консультанта; члены группы по управлению инцидентами участвуют, в соответствующих случаях, в принятии решений относительно деятельности компании.*

Функция 3.5. **Консультации по вопросам безопасности:** услуги по консультированию клиента или отрасли по вопросам осуществления или внедрения соответствующих операций или функций обеспечения безопасности.

Услуга 4. Информированность о ситуации

Цель: информированность о ситуации представляет собой ряд мер, направленных на обеспечение осведомленности организации касательно среды своей деятельности. Информированность о ситуации включает в себя определение важнейших элементов, способных оказывать воздействие на миссию организации, мониторинг таких элементов и использование таких знаний в принятии решений и при осуществлении других действий.

Результат: *обеспечение необходимой информированности о мероприятиях и действиях как внутри организации, так и вокруг нее, которые могут повлиять на возможность своевременного и безопасного осуществления организацией своей деятельности.*

Функция 4.1. **Работа датчиков/метрические операции:** услуги, направленные на разработку, развертывание и эксплуатацию систем, а также методик анализа, с целью определения действий, которые необходимо расследовать.

Цель: создавать инфраструктуру и процессы сбора информации, необходимые для обеспечения информированности организации о ситуации.

Результат: *инфраструктура для сбора оперативной информации (т. е. датчики), предоставляющая данные для обеспечения информированности о ситуации.*

Подфункция 4.1.1. **Разработка требований:** понимание потребностей клиента и обеспечение разрешений, согласно которым может работать CSIRT.

Цель: в процессе разработки требований определяются потребности организации в отношении информированности о ситуации, после чего такие требования картируются с учетом типов информации, необходимой для достижения соответствующих целей.

Результат: *с точки зрения информации, понимание уровня осведомленности, который необходим организации и ее клиентуре. Кроме того, обеспечение получения организацией всех необходимых политико-правовых разрешений на сбор информации.*

Подфункция 4.1.2. **Определение необходимых данных:** определение данных, необходимых для выполнения требований.

Цель: функции датчиков могут выполнять разные агенты – от автоматизированных систем до человека. Такие источники информации (данных) используются для обеспечения информированности организации о ситуации. Процесс «Определение необходимых данных» предусматривает картирование требований относительно информированности о ситуации применительно к потенциальным источникам информации (т. е. датчикам).

Результат: *определение данных необходимо для выполнения требований относительно информированности о ситуации организации. Некоторые из таких источников данных уже могут существовать, в то время как другие, возможно, необходимо будет выработать и/или приобрести.*

Подфункция 4.1.3. **Методы получения данных:** определение методов, инструментов, техник и технологий, используемых для сбора необходимых данных.

Цель: в ходе этого процесса определяются методы сбора, обработки и хранения собранной информации (данных).

Результат: *определение тех или иных подробностей того, каким образом будет осуществляться сбор, хранение, обработка и удаление информации.*

Подфункция 4.1.4. **Управление датчиками**: техническое обслуживание и постоянное повышение качества работы датчиков в соответствии с установленными требованиями.

Цель: осуществлять техническое обслуживание и мониторинг датчиков для обеспечения надлежащей функциональности и точности.

Результат: *внедрение программы управления датчиками и обеспечения устойчивости жизненного цикла.*

Подфункция 4.1.5. **Управление результатами:** сортировка информации и показателей датчиков в зависимости от приоритетов и распространение такой информации и показателей. Как правило, распространение осуществляется с использованием информационной панели для ознакомления на разных уровнях организации.

Функция 4.2. **Синтез/корреляция:** услуги, предусматривающие проведение анализа и объединение разных источников данных. Использование потоков данных независимо от источника и сведение их воедино для отображения общей картины ситуации (информированность о ситуации).

Цель: определить новые взаимосвязи между инцидентами, показателями и участниками, позволяющие повысить эффективность мер по смягчению последствий или реагированию на инциденты в области безопасности.

***Результат**: обеспечить последовательный процесс обработки организацией новой информации об угрозах и объединение ее с полученной ранее информацией, содержащейся в хранилище данных организации. Итоговым результатом такого процесса является улучшенный массив данных, обеспечивающий для CSIRT возможность принятия более эффективных и точных решений.*

Подфункция 4.2.1. **Определить алгоритмы синтеза информации**: обозначить методы и техники (алгоритмы) или технологии, используемые в анализе (синтезе) информации.

Цель: в контексте обработки инцидентов важно, чтобы CSIRT сохраняла эффективное оперативное понимание информации, поступающей из разных источников. Синтез позволяет обрабатывать информацию таким образом, чтобы CSIRT могла оперативно учитывать новую информацию по мере ее получения, а также полностью увязывать ее с контекстом и делать ее доступной для использования в процессе обработки инцидентов.

***Результат**: выработать внутренний процесс, дающий возможность получения новой информации, ее оценки в контексте уже существующей информации и успешного использования полученной в результате этого информации, предоставленной CSIRT, в контексте инцидента.*

Подфункция 4.2.2. **Синтез и анализ:** анализ (синтез) источников данных с использованием данных в системе управления знаниями с целью определения общих характеристик и взаимосвязей в массиве данных.

Цель: в процессе обработки инцидентов CSIRT необходимо постоянно сохранять понимание угрозы, создаваемой в результате того или иного инцидента в отношении организации. Для этого группе необходимо поддерживать актуальную осведомленность, как о самом инциденте, так и о тактиках, техниках и процедурах, применяемых злоумышленником. Ей необходимо осуществлять постоянный сбор информации и оценивать ее в сопоставлении с уже существующей информацией. Подфункция 4.2.2 отвечает за применение алгоритмов синтеза, выбранных в подфункции 4.2.1, для проведения анализа информации об угрозе, полученной из внешних источников.

***Результат**: понимать воздействие новой информации об угрозе, собранной на основе произошедших инцидентов, а также осуществить подготовку организации к любым изменениям в TTP, внесенным злоумышленником, или обеспечить*

возможность постоянного обновления методов смягчения последствий и реагирования с целью принятия более эффективных мер в ответ на инциденты.

Функция 4.3. **Разработка и управление информацией о безопасности:** услуги, предоставляемые внутренним и внешним клиентам с целью разработки и управления источниками информации о безопасности, являющимися третьими лицами. Информацию о безопасности можно определить как сведения о безопасности и угрозах, предоставляющие оперативную аналитическую информацию или информацию о тех или иных угрозах. Среди прочего, к таким услугам может относиться анализ, разработка, распространение и управление информацией о безопасности, включая показатели угроз и модели их обнаружения, например правила противодействия вредоносным программным средствам и соответствующие подписи, а также тактику, методы и процедуры, применяемые злоумышленниками. Эти услуги зависят от действий по обмену информацией, описанных в разделе 5.6, "Информационно-пропагандистская деятельность/информационное взаимодействие".

Цель: информация, получаемая от внешних объектов, является чрезвычайно важной для обеспечения достаточного уровня информированности о ситуации. CSIRT нужен большой объем информации высокого качества, связанной с ее деятельностью; тем не менее затраты и нагрузка, необходимые для ее получения, указывают на то, что соответствующие усилия необходимо направлять выборочно на те или иные источники.

Результат: *система управления данными (функция 4.4) принимает множественные, высококачественные потоки данных, охватывающие все области, относящиеся к деятельности CSIRT – в первую очередь, путем полностью автоматизированных процессов. Еще одним результатом является наличие процессов обнаружения аномалий и изменений в тенденциях информационных потоков, поступающих от внешних источников.*

Подфункция 4.3.1. **Определение и учет источников**: постоянное выявление, поддержка и интеграция источников информации в процессы управления знаниями и анализа.

Цель: получить актуальную, высококачественную информацию из внешних источников для принятия мер реагирования на инциденты, а также для упреждающего повышения информированности о ситуации (и общего состояния безопасности организации). Данные из внешних источников дополняют данные, собранные внутри организации: отчеты об инцидентах (функция 1.1), отчеты об уязвимостях (функция 1.2), а также

данные датчиков, используемых CSIRT (функция 4.1).

Результат: *получение высококачественной, относящейся к безопасности информации из внутренних, внешних, открытых и/или коммерческих источников. Вся собранная информация храниться в системе управления данными (функция 4.4).*

Подфункция 4.3.2. **Сбор и каталогизация контента источников:** сбор материалов из источников информации об угрозах. Эти источники могут быть внутренними, внешними, открытыми и/или платными.

Цель: оценить качество собранной информации. Наблюдать изменения в характеристиках (в т. ч. в количестве) данных, полученных из внешних источников, с целью обнаружения аномалий и/или новых тенденций.

Результат: *документация, содержащая оценку качества источников. Автоматизированный или полуавтоматизированный процесс обнаружения основных изменений в общих характеристиках информации, полученной из внешних источников.*

Функция 4.4. **Управление данными и знаниями:** услуги, предлагаемые клиентам в целях фиксации, разработки, совместного использования и эффективного применения знаний организации с учетом разметки данных (например, STIX, TAXII, IODEF, TLP), баз данных показателей и каталогов вредоносных программных средств/уязвимостей.

Цель: клиентам нужны данные и знания о кибербезопасности того уровня качества и в тех временных рамках, которые соответствуют их потребностям. Данные о кибербезопасности включают в себя информацию, предназначенную для обработки системами с целью содействия автоматизации процесса обеспечения безопасности. К знаниям в области кибербезопасности относится информация, предназначенная для аналитиков/операторов по кибербезопасности. Кроме того, данные и знания о кибербезопасности нужны для предоставления других услуг и выполнения функции CSIRT. Такой информацией лучше всего управлять как общим ресурсом CSIRT при условии, что большая часть информации используется повторно при предоставлении нескольких разных услуг и выполнении функций.

Результат*: данные и знания в области кибербезопасности требуемого качества своевременно предоставляются клиентам. Данные и знания, необходимые для предоставления других услуг и выполнения других функций CSIRT, можно легко получить из одного источника внутри CSIRT.*

- **Управление представлением данных:** стандартизация представления данных и обмена ими (например, STIX, TAXII, IODEF, RID и т. п.)
- **Управление хранением данных:** разработка, введение в эксплуатацию и обслуживание систем управления хранением данных.
- **Освоение данных:** процессы и системы, используемые для ввода, проверки и хранения информации.
- **Извлечение данных:** процессы, политики и технические методы извлечения информации.
- **Оценка инструментов:** оценка и интеграция инструментов, используемых для управления данными, анализа и совместной работы.

Функция 4.5. **Показатели организации:** услуги, направленные на определение, установление, сбор и анализ сведений о достижении организацией целевых показателей результативности, а также оценку эффективности организации.

Цель: в настоящее время основным направлением усилий групп реагирования на инциденты в области компьютерной безопасности (CSIRT) и организаций, занимающихся управлением инцидентами, является определение того, насколько успешно они выполняют возложенную на них задачу по управлению инцидентами в области кибербезопасности. По мере того, как группы становятся более зрелыми с точки зрения продолжительности оперативной деятельности, они задаются вопросом: "Насколько успешно мы работаем на самом деле?" Группы ищут способы оценки своих операций не только для определения сильных и слабых сторон процессов, технологий и методов, но и для сравнения показателей своей деятельности с успехами других, аналогичных им групп. Они ищут количественные доказательства и показатели, свидетельствующие о том, являются ли они эффективными в вопросах предупреждения, обнаружения, анализа и реагирования на происшествия и инциденты в области кибербезопасности. Эта функция направлена на определение того, на какие вопросы (информацию) необходимо дать ответы руководству, группам CSIRT и заинтересованным сторонам, среди прочего, чтобы оценить свою деятельность и доказать свою значимость; на создание механизмов сбора параметров в целях обеспечения необходимых показателей, а также последующего сбора, анализа и представления результатов.

Результат: *обеспечить необходимую осведомленность и эмпирические доказательства, демонстрирующие то, насколько организация по управлению инцидентами соответствует своей миссии и насколько эффективно выполняет ее. Использовать эту информацию для содействия принятию решений и повышения уровня эффективности и подотчетности.*

Услуга 5. Информационно-пропагандистская деятельность/информационное взаимодействие

Функция 5.1. **Консультации по вопросам политики в области кибербезопасности:** услуги, способствующие разработке и принятию политики в области кибербезопасности с целью сформировать благоприятную для CSIRT, ее клиентуры и других заинтересованных лиц среду путем предоставления лицам, ответственным за принятие решений, экспертных консультаций по рассматриваемым вопросам.

Подфункция 5.1.1. Внутренние

- **Консультации по политико-правовым вопросам:** предоставление данных о политико-правовых последствиях касательно полномочий и мандата организации и клиентуры.
- **Разработка политики:** разработка политики по вопросам, касающимся или влияющим на деятельность и полномочия организаций или клиентуры.

Подфункция 5.1.2. Внешние

- **Предоставление данных по политическим вопросам:** предоставление рекомендаций по вопросам политики в технической области и области безопасности, которые могут оказать воздействие на организацию, ее клиентуру или других партнеров.
- **Оказание воздействия на политику:** предоставление достоверной информации или экспертных данных по рассматриваемым вопросам для использования в качестве ориентира при пересмотре политики, регламентарных положений или законов. Такие действия могут предусматривать, среди прочего, представление доказательств в законодательных, научных или других органах, составление документов с изложением позиции, написание правительственных информационных документов или статей, ведение блога, участие в работе социальных сетей, проведение встреч с заинтересованными лицами и т. п.
- **Разработка стандартов или примеров передового опыта:** содействовать деятельности организаций, отвечающих за разработку отраслевых, международных, региональных и национальных стандартов или примеров передового опыта (IETF, ИСО, FIRST), направленной на упорядочивание процессов / примеров передового опыта с целью обеспечения максимально возможной совместимости, в том числе функциональной, а также безопасности, возможности воспроизведения и качества.

Функция 5.2. **Управление отношениями:** услуги, направленные на установление и поддержание отношений в интересах организации.

Подфункция 5.2.1. **Управление отношениями с аналогичными организациями:** развитие и поддержание отношений с организациями, которые могут способствовать выполнению CSIRT своей миссии. Такие действия могут предусматривать обеспечение функциональной совместимости или содействие сотрудничеству между организациями.

Подфункция 5.2.2. **Управление отношениями с клиентами:** разработка и внедрение практики, стратегий и технологий, предназначенных для определения, распознавания, понимания и оценки деятельности клиентуры и заинтересованных сторон, а также отслеживания такой деятельности и управления ею.

Подфункция 5.2.3. **Организация связи:** управление списками, предназначенными для рассылки объявлений, оповещений или предупреждений об опасности, потоков данных или других публикаций, а также совместного использования информации.

Подфункция 5.2.4. **Организация безопасной связи:** управление механизмами безопасной связи, предназначенными для использования электронной почты или веб-сайтов, мгновенного обмена сообщениями, а также обеспечения голосовой связи.

Подфункция 5.2.5. **Конференции / семинары-практикумы:** предоставление CSIRT и ее клиентам возможности собираться вместе для обсуждения стоящих перед ними угроз и вызовов, укрепления доверительных взаимоотношений, поддержания взаимных контактов и обмена примерами передового опыта и извлеченными уроками.

Подфункция 5.2.6. **Привлечение заинтересованных сторон/отношения с заинтересованными сторонами:** это предусматривает, среди прочего, координирование деятельности с отраслевыми / вертикальными организациями, а также обеспечение функционирования официальных центров координирования деятельности как с внутренними, так и с внешними заинтересованными сторонами. Привлечение руководства организации к информированию о ее миссии и обеспечению понимания безопасности и осведомленности о ней.

Функция 5.3. **Повышение осведомленности в вопросах безопасности:** услуги, оказываемые клиентам с целью повысить коллективное понимание стоящих перед ними угроз, а также действий, которые можно предпринять для снижения вызванного такими угрозами риска.

Функция 5.4. **Брендинг/маркетинг:** услуги, целью которых является обеспечение осведомленности заинтересованных сторон и клиентуры о CSIRT и предоставляемых ею возможностях, а также о том, каким образом им следует взаимодействовать с CSIRT, чтобы донести до нее информацию о своих потребностях.

Функция 5.5. **Совместное использование информации и публикации:** услуги, направленные на широкое информационное взаимодействие, включая предоставление клиентам уведомлений со стороны организации в целях обеспечения своей деятельности. Среди примеров таких действий – уведомление о проведении учебных мероприятий, о различных событиях, а также о политике и процедурах организации.

Подфункция 5.5.1. **Объявления службы общественной информации:** распространение относящейся к вопросам безопасности информации с целью повысить уровень осведомленности и соблюдения практики обеспечения или общественной безопасности или безопасности организации, ее клиентов, отрасли.

Подфункция 5.5.2. **Обнародование информации:**

- **Сбор информации о потребностях:** определение того, какую информацию необходимо распространить и кому, а также каким способом и в какие временные рамки это необходимо сделать (анализ объема работ). Примечание: такая публикация может быть предназначена для ограниченного круга лиц, или же это может быть более подробная информация для партнеров.

- **Разработка:** определение формата и предназначения информационной продукции в соответствии с потребностями.
- **Написание:** тщательный подбор информации, которую целевая аудитория могла бы с легкостью усвоить (например, представление результатов экспертно-технического анализа, а также мероприятий по устранению инцидентов, уязвимостей и вредоносных программных средств).
- **Проверка:** проверка публикации с целью установить, насколько четкой и точной она является, отвечает ли она правилам грамматики и орфографии, принципам соблюдения конфиденциальности и раскрытия информации, а также окончательное утверждение публикации.
- **Распространение:** предоставление информации целевой аудитории с использованием необходимых и надлежащих каналов.

Услуга 6. Создание потенциала

Цель: обеспечение эффективного процесса обработки инцидентов и принятия мер реагирования, а также эффективного подхода к ним, должно быть всегда ориентированным на создание потенциала. Это играет ключевую роль для деятельности и эффективности организации в целом. Организации должны более взвешенно подходить к осознанию того, какие функциональные возможности на самом деле оказывают воздействие на их CSIRT и на успех деятельности в целом, и приводить свои программы профессиональной подготовки в соответствие с этим. По результатам опроса, проведенного компанией McKinsey, около 60% респондентов отметили, что создание потенциала является главным приоритетом для их организации. Тем не менее когда речь шла о времени, уделяемом решению наиболее актуальных вопросов, оказалось, что лишь менее 30% респондентов имеют программы профессиональной подготовки, ориентированные на развитие потенциала, создающие наибольшую ценность и обеспечивающие то, что было необходимо для осуществления оптимальной деятельности.

Потенциал можно определить как что-то, что организация делает эффективно и что обеспечивает значимые результаты в ее деятельности. Организациям нужен потенциал, играющий важнейшую роль в их деятельности в целом и в эффективности работы групп; кроме того, им необходимо понимать, почему их усилия сосредоточены на выбранных ими аспектах потенциала. Культура также играет свою роль в том, какие из своих возможностей организация определяет как приоритетные и развивает. В то время как руководители высшего звена обычно участвуют в формировании общего направления и видения в отношении развития потенциала организации, наиболее успешные из них согласовывают потенциал на уровне организации с потенциалом, необходимым и требуемым на уровне подразделения или группы.

***Результат**: понять, оформить и выполнить план, а также иметь возможность использовать и измерять результаты и взаимосвязи разных возможностей для создания потенциала как на уровне отдельной группы специалистов, так и на уровне готовности всей организации в целом. Определить практику системного подхода, которая становится частью общего процесса планирования кадровых ресурсов.*

Функция 6.1. **Обучение и профессиональная подготовка:** потенциал предусматривает некий уровень функциональных возможностей на том или ином уровне зрелости. Таким образом, потенциал является краеугольным камнем предоставления услуг CSIRT. Работа по созданию потенциала предусматривает проведение обучения и профессиональной подготовки клиентов CSIRT (к которым могут относиться сотрудники организации, но не включая такие функциональные аспекты, как профессиональная подготовка людских ресурсов для группы) в области кибербезопасности, обеспечения безопасности информации и реагирования на инциденты.

Цель: обычно программа обучения и профессиональной подготовки является первым шагом на пути к определению и учреждению объекта, занимающегося созданием потенциала. Этого можно добиться за счет разного рода действий, в том числе благодаря профессиональной подготовке и обучению, документированию требуемых знаний, навыков и функциональных возможностей, распространению разработанных учебно-подготовительных материалов, наставничеству, профессиональному росту и развитию навыков, а также практическим и лабораторным занятиям. Каждый из этих видов деятельности в комплексе будет содействовать развитию потенциала организации в целом и той или иной группы специалистов в частности.

***Результат**: понять структуру программы обучения и профессиональной подготовки, а также ее связь с созданием потенциала группы CSIRT. Быть в состоянии понять и задокументировать различные виды результатов деятельности группы и организации, а также KPI, чтобы иметь возможность оценить уровень достигнутого прогресса.*

Подфункция 6.1.1. **Сбор информации о потребностях в отношении знаний, навыков и способностей:** сбор информации о потребностях в отношении знаний, навыков и способностей, а также компетенции клиента с целью определения того, какое обучение и профессиональную подготовку необходимо ему предоставить.

Цель: надлежащим образом оценить, определить и задокументировать потребности CSIRT в отношении обязательных знаний, навыков и способностей, чтобы члены группы были сильными и готовыми к работе.

***Результат:** определить необходимые характеристики знаний, навыков и способностей, а также процесс, с помощью которого CSIRT сможет удовлетворить потребности своей деятельности и сравнить их с другими группами, являющимися лучшими в своем классе. Это поможет установить, на каком уровне работает группа, а также есть ли возможности для улучшения ее работы, и если да, то в каких сферах.*

Подфункция 6.1.2. **Разработка учебно-подготовительных материалов:** создание или приобретение учебно-подготовительных материалов, таких как презентации, лекции, демонстрации, моделирование и т. п.

Цель: разработка учебно-подготовительных материалов осуществляется CSIRT с целью содействовать обеспечению уровня осведомленности пользователей, держать группу в курсе быстро меняющейся ситуации и угроз и содействовать информационному взаимодействию между CSIRT и ее клиентами.

***Результат**: учебно-подготовительные материалы CSIRT соответствующего качества, которые удовлетворяют потребностям динамично развивающейся среды CSIRT и основаны на разнообразных и эффективных методиках и платформах презентации информации.*

Подфункция 6.1.3. **Передача контента:** передача знаний и контента "учащимся". Такую передачу можно осуществлять разными методами, такими как обучение с помощью компьютерных технологий/онлайновое обучение, обучение с инструктором, конференции, презентации, лабораторные занятия и т. п.

Цель: формальный процесс передачи знаний поможет группе определить прозрачный подход к тому, каким образом члены CSIRT смогут наиболее эффективно проходить профессиональную подготовку.

***Результат:** структура процесса предоставления контента, опирающаяся на все доступные методы; презентация, изучение технических и личных навыков и процессов; применение всех альтернативных подходов, в том числе практическая лабораторная работа, дистанционное обучение с помощью компьютерных технологий, очная профессиональная подготовка и т. п.*

Подфункция 6.1.4. **Наставничество:** обучение у опытного персонала, на основе установившихся отношений, может предусматривать посещение объектов, ротацию (обмен), учебное дублирование и обсуждение мотивации тех или иных решений и действий.

Цель: обычно программа наставничества является первым шагом на пути к определению и учреждению объекта, занимающегося созданием потенциала. Она может обеспечить как формальные, так и неформальные механизмы передачи

наставником ученику знаний об обучении и развитии навыков, наблюдений, а также жизненного и профессионального опыта, вне рамок официальных взаимоотношений подчинения и структуры группы.

Результат: *группа CSIRT повысила уровень удержания членов, лояльности, уверенности и общей способности принимать обоснованные решения.*

Подфункция 6.1.5. **Профессиональный рост:** оказание помощи сотрудникам в успешном и корректном планировании и развитии их карьеры. Может включать посещение конференций, прохождение углубленной профессиональной подготовки, перекрестное обучение и т. п.

Цель: группа CSIRT содействует профессиональному росту с целью обеспечения непрерывного процесса получения новых знаний, навыков и способностей, связанных с профессиональной сферой обеспечения безопасности, специфическими служебными обязанностями, а также общей средой деятельности группы.

Результат*: выработка характеристик профессионального роста с тем, чтобы группа не только имела уверенность, но и обладала необходимыми знаниями, навыками и способностями, которые можно было бы применить непосредственно на практике, а также имела в своем распоряжении актуальную информацию относительно должностных обязанностей и потребностей.*

Подфункция 6.1.6. **Развитие навыков:** проведение профессиональной подготовки персонала организации по вопросам инструментов, процессов и процедур, связанных с выполнением ежедневных функций.

Цель: после того, как будут определены соответствующие навыки, группа CSIRT должна осуществить ряд действий, которые определят способности или подготовленность ее членов.

Результат: *развитый и подготовленный персонал, владеющий необходимыми техническими, личностными навыками и понимающий соответствующие процессы. Члены группы CSIRT, которые уже занимаются решением ежедневных рабочих вопросов, оказывая поддержку как группе, так и ее клиентам.*

Подфункция 6.1.7. **Проведение практических занятий**: проведение тестирования уровня подготовленности учащихся клиентов для определения их способности применять на практике полученные в процессе профессиональной подготовки знания и выполнять должностные обязанности или функции. Может осуществляться посредством использования виртуальной среды, моделирования, проведения испытаний в полевых условиях, теоретических занятий, инсценировок или нескольких из перечисленных методик в комплексе.

Цель: благодаря тренировочным/практическим занятиям группа CSIRT повысит степень своей уверенности в правильности плана работы CSIRT организации, а также его реализуемости.

***Результат**: Максимально готовая к соответствующей работе группа, обеспечивающая соблюдение процессов формирования знаний, навыков и способностей, а также успешное совместное выполнение всех работ. Кроме того, это поможет установить, на каком уровне работает группа, а также то, есть ли возможности для улучшения ее работы, и если да, то в каких сферах.*

Функция 6.2. **Организация практических занятий:** услуги, предлагаемые организацией клиентам с целью содействия разработке, проведению и оценке практических занятий по вопросам кибербезопасности, предназначенных для профессиональной подготовки и/или оценки способностей как отдельных клиентов в частности, так и всей клиентуры в целом. Такого рода практические занятия можно применять для того, чтобы:

- **испытать политики и процедуры:** группа оценивает наличие адекватных политик и процедур, соответствующих тому или иному происшествию. Как правило, это занятие, предусматривающее упражнения, которые выполняются на бумаге/теоретическое занятие;
- **проверить оперативную готовность:** группа оценивает наличие адекватных сотрудников для принятия мер в ответ на происшествие, а также правильность выполнения процедур. Обычно такие действия предусматривают практические упражнения на выполнение процедур.

Цель: практические занятия проводятся с целью повышения эффективности и результативности услуг и функций обеспечения кибербезопасности. Эта функция и связанные с ней подфункции ориентированы на удовлетворение потребностей как организации, так и ее клиентов. В частности, с помощью моделирования происшествий/инцидентов в области кибербезопасности практические занятия можно использовать для достижения одной или нескольких из перечисленных ниже целей:

- демонстрация: наглядно показывать услуги и функции, а также уязвимости, угрозы и риски, с целью повысить осведомленность;

- профессиональная подготовка: обучить персонал новым инструментам, методам и процедурам;
- практическое занятие: предоставить персоналу возможность применять инструменты, методы и процедуры, по которым они уже прошли профессиональную подготовку. Практические занятия необходимы для поддержания навыков, которые быстро теряются; кроме того, они помогают повышать и сохранять эффективность;
- оценка: проанализировать и сформировать понимание уровня эффективности и результативности услуг и функций обеспечения кибербезопасности;
- подтверждение: определить, можно ли достичь обозначенного уровня эффективности и/или результативности услуг и функций обеспечения кибербезопасности.

***Результат**: эффективность и результативность услуг и функций обеспечения кибербезопасности будет напрямую повышена, а также будут извлечены уроки в целях обеспечения дальнейших улучшений. В зависимости от тех или иных целей практического занятия, можно познакомить с темой кибербезопасности и заинтересованные стороны, провести профессиональную подготовку персонала, а также оценить и/или подтвердить эффективность и результативность услуги функций. Наряду с этим, можно определить возможности для улучшения практических занятий в дальнейшем.*

Подфункция 6.2.1. **Требования:** понимание цели практического занятия, в частности, задач, стоящих перед всеми его участниками, чтобы учесть их пожелания при разработке занятий.

Цель: цель участия в проведении практических занятий заключается в повышении эффективности и результативности услуг и функций обеспечения кибербезопасности.

Участие может иметь одной из следующих форм:

- наблюдатель: сотрудники наблюдают за проведением практического занятия, не являясь частью его целевой аудитории и не принимая участия в выполнении упражнений в рамках занятия, а также не получая оценку своему участию. Наблюдение без непосредственного участия может в некоторой степени способствовать повышению эффективности и результативности услуг и функций CSIRT. Кроме того, оно может содействовать проведению практических занятий в будущем;
- целевая аудитория, на которую ориентировано практическое занятие: сотрудники принимают участие в практическом занятии в качестве целевой аудитории, на которую оно ориентировано, выполняя задачи в ходе практического занятия, а также могут проходить оценивание.

В зависимости от форм практического занятия, сотрудники могут как лично присутствовать на практических занятиях, так и принимать участие в них дистанционно, находясь на своем рабочем или в другом подходящем месте. Наряду с этим на практическом занятии может быть создана специальная среда, либо участники

могут принимать участие в своей собственной среде практических занятий или своей обычной рабочей среде.

***Результат**: повышение эффективности и результативности услуг и функций обеспечения кибербезопасности, а также определение возможностей для дальнейших улучшений. В зависимости от тех или иных целей практического занятия, можно познакомить с темой кибербезопасности и заинтересованные стороны, провести профессиональную подготовку персонала, а также оценить и/или подтвердить эффективность и результативность услуги функций. Наряду с этим, можно определить возможности для улучшения практических занятий в дальнейшем.*

Подфункция 6.2.2. **Разработка сценария и создание среды**: разработка планов практических занятий в соответствии с задачами клиентов.

Цель: целью проведения практических занятий является предоставление целевой аудитории возможности для повышения эффективности и результативности ее услуг и функций путем обработки моделируемых происшествий/инцидентов в области кибербезопасности.

***Результат**: та или иная аудитория повысила эффективность и результативность своих услуг и функций, а также нашла возможности для их дальнейшего улучшения. Наряду с этим, были определены возможности для улучшения практических занятий в дальнейшем.*

Подфункция 6.2.3. **Участие в практических занятиях:** организация может участвовать в практическом занятии на разных уровнях ввиду уровня ее зрелости.

- **Оценка:** оценить результаты проведения практического занятия, получить отзывы и предложения и сделать выводы, основанные на наблюдении за ходом практического упражнения.
- **Наблюдение:** наблюдать за практическим занятием, которое проводит третья сторона.
- **Координирование:** координировать проведение практического занятия.
- **Участие:** принять участие в практическом занятии на тему кибербезопасности. Участнику предоставлен выбор уровня его участия и отдачи от практического занятия (например, привлечь третью сторону к оценке его участия).

Подфункция 6.2.4. **Определение извлеченных уроков:** разработать отчет о дальнейших мерах, включив в него описание извлеченных уроков или результатов / примеров передового опыта на основе практического занятия.

Функция 6.3. **Системы и инструментарий для поддержки клиентуры:** услуги, ориентированные на предоставление клиентуре рекомендаций, а также разработку, предоставление и приобретение инструментов и услуг, связанных с обеспечением кибербезопасности. Все эти системы и инструменты связаны с CSIRT/безопасностью, а не информационными технологиями в целом; к ним могут относиться порталы для обмена сообщениями / оповещения об угрозах.

***Результат**: CSIRT внедрила процессы и системы, направленные на определение требований и возможностей клиентов, и приобретает, предоставляет или разрабатывает платформы с целью выполнения таких требований.*

Функция 6.4. **Поддержка услуг заинтересованных сторон:** услуги по расширению технических возможностей, предлагаемые CSIRT с целью содействовать созданию функциональных возможностей, потенциала и обеспечить полноценность услуг CSIRT, предоставляемых заинтересованным сторонам. Это означает повышение уровней обслуживания.

Цель: в процессе создания и расширения функциональных возможностей клиентуры CSIRT отдельное внимание уделяется оказанию помощи в разработке, приобретении, управлении, эксплуатации и техническом обслуживании их инфраструктуры.

***Результат:** разработать системный подход к оценке потребностей в отношении инфраструктуры, определения требований, разработки структуры, приобретения, подтверждения соответствия, технического обслуживания и обновлений, профессиональной подготовки по оперативным вопросам, а также внутренних и внешних аудиторских проверок.*

Подфункция 6.4.1. **Проектирование и техническая разработка инфраструктуры:** содействие при проектировании и технической разработке инфраструктуры с целью выполнения требований клиентуры.

Цель: предоставить общее понимание методики проектирования, знание соответствующих стандартов и норм, а также осветить примеры передового опыта в проектировании и технической разработке инфраструктуры на основе комплексной оценки потребностей и анализа требований клиентуры.

***Результат:** практический опыт разработки и сопоставления подходов и альтернатив в контексте проектирования инфраструктуры, основанный на*

международных примерах передового опыта с учетом соответствующих стандартов и норм.

Подфункция 6.4.2. **Закупка объектов инфраструктуры:** оказание помощи при закупке объектов инфраструктуры, будь то помощь в разработке требований и стандартов в отношении зрелости системы оценки рисков или помощь в разработке минимальных требований и стандартов безопасности (например, требование соответствия тому или иному стандарту, такому как сертификация продукта).

Цель: прийти к глубокому пониманию разработки технического задания для закупки объектов инфраструктуры с учетом институциональных, технических и операционных требований.

Результат: *понимание процесса закупки объектов инфраструктуры с соблюдением соответствующих стандартов и норм, а также принятие во внимание разных технических мер и процедур заключения контрактов, которые необходимо выполнить.*

Подфункция 6.4.3. **Оценка связанного с инфраструктурой инструментария:** оценка инструментов от имени клиентуры.

Цель: оказание помощи при оценке функциональности и соответствия требованиям разных инструментов, в том числе аппаратного и программного обеспечения, а также пользовательских приложений.

Результат: *анализ эффективности инструментов, а также их соответствия стандартам, нормам и предварительно выработанному техническому заданию.*

Подфункция 6.4.4. **Обеспечение инфраструктуры ресурсами**: содействие в приобретении необходимых ресурсов инфраструктуры. (Например, поставщики оборудования, услуг и т. п.)

Цель: указать ключевые факторы успешного обеспечения инфраструктуры ресурсами и разработать механизмы построения устойчивых и эффективных взаимосвязей с поставщиками решений и продавцами, основанных на принципах четко определенной ответственности и подотчетности.

Результат: *выработать ключевые показатели деятельности (KPI) в отношении обеспечения инфраструктуры ресурсами с заключением соответствующих соглашений об уровне услуг, которые могут гарантировать эффективное и результативное обеспечение инфраструктуры ресурсами.*

Услуга 7. Научно-исследовательская деятельность

Функция 7.1. **Разработка методик обнаружения/анализа/устранения уязвимостей/анализа основных причин**: услуги, способствующие определению и выявлению новых функциональных возможностей, улучшению методик предоставления услуг в связи с уязвимостями или координирования других организаций либо коммерческих практик, способных обеспечить вышеуказанное.

Цель: некоторые организации работают исключительно путем получения информации об уязвимостях из внешних источников, в то время как другим организациям нужны/желательны собственные функциональные возможности для обнаружения и анализа уязвимостей. Цель этой функции состоит в описании того, как организация может разработать такие функции поиска уязвимостей.

Результат: *при необходимости определить методики, которые организация может применять в целях более глубокого понимания уязвимостей.*

Функция 7.2. **Разработка процессов сбора/синтеза/сопоставления информации о безопасности**: услуги по определению и выявлению новых функциональных возможностей, а также повышению эффективности методик информационного анализа и услуг совместного использования информации в контексте оперативных аналитических сведений и информации об угрозах.

Цель: чтобы любая функция работы с информацией о безопасности была успешной, она должна предусматривать возможность осуществления сбора информации, а также предоставления соответствующей информации третьим сторонам. Сбор информации часто зависит от человеческих взаимоотношений между сторонами, совместно использующими информацию, которые предусматривают уровень доверия, достаточный для обеспечения возможности совместного использования конфиденциальной информации. Аналитик должен уметь развивать такие взаимоотношения, определять соответствующие массивы информации, которые необходимо передать другой стороне, определять протоколы, наиболее подходящие для автоматизированного обмена данными, заниматься управлением отношениями и совместными расследованиями, а также оценивать эффективность источника информации.

***Результат**: в организации внедрены процессы и процедуры сбора, анализа, синтеза и оценки соответствия поступающей от внешних источников информации с описанием угроз активам в области информационной безопасности. Организация сама способна создавать новые источники и привлекать новых партнеров к совместному использованию информации.*

Функция 7.3. **Разработка инструментария**: услуги по определению и развитию новых функциональных возможностей, а также по предоставлению сведений о подходах к использованию нового инструментария и автоматизации выполнения процессов, связанных с деятельностью CSIRT.

***Результат**: инструментарий, разработанный CSIRT для содействия автоматизации выполняемых CSIRT задач, является масштабируемым и надежным, обеспечивает четкие результаты, а также не ухудшает силы и средства обеспечения безопасности CSIRT, которая применяет данный инструментарий. Высвобождение аналитических ресурсов для выполнения нештатных задач.*

Вспомогательные материалы

FIRST - https://www.first.org

CERT/CC - http://www.cert.org

STIX/TAXII - https://stix.mitre.org

TLP - https://www.us-cert.gov/tlp

IETF - https://www.ietf.org

ISO/IEC 27035 -
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

Глоссарий

Тестирование приложений – исследование, направленное на то, чтобы предоставить заинтересованным сторонам информацию о качестве тестируемой продукции или услуг.

Базель II – второе из Базельских соглашений, представляющих собой рекомендации относительно законов и регламентарных положений в области банковского дела, изданные Базельским комитетом банковского надзора.

Возможность – измеряемая деятельность, которую можно осуществить в рамках функций и обязательств организации. В целях данной концепции предоставления услуг CSIRT возможности могут быть определены либо как услуги в более широком контексте, либо как необходимые функции, подфункции или задачи.

Потенциал – количество случаев единовременного возникновения той или иной возможности, которой организация может воспользоваться до того, как ее ресурсы будут в той или иной степени исчерпаны.

CERT/CC – Координационный центр групп реагирования на компьютерные инциденты.

CISO – главный директор по информационной безопасности.

Облако – среда распределенных вычислений, позволяющая прикладному программному обеспечению работать с использованием управляемых через интернет устройств.

COBIT – задачи управления для информационной технологии и технологий, связанных с ней.

Криптографический хэш – хэш-функция, инвертирование которой, т. е. воссоздание входных данных на основе лишь значения хэш-функции, как считается, практически невозможно.

CSIRT – группа реагирования на нарушения компьютерной безопасности.

Внешний набор данных – данные, собранные третьей стороной.

FIRST – Форум групп реагирования на инциденты и обеспечения безопасности.

- **Функция** – средства или способы достижения цели или выполнения задачи в рамках той или иной услуги.

Нечеткое тестирование – метод тестирования программного обеспечения, зачастую автоматический или полуавтоматический, который предусматривает введение в компьютерную программу неверных, непредвиденных или случайных данных.

Эмулятор аппаратного / программного обеспечения – аппаратное или программное обеспечение, позволяющее одной компьютерной системе (именуемой "хост") выдавать себя за

1501 другую компьютерную систему (именуемую "гость"). Как правило, используется для применения
1502 на хост-системе программного обеспечения или периферических устройств, предназначенных для
1503 гостевой системы.

1504 **МЭК** – Международная электротехническая комиссия.

1505 **IETF** – Целевая группа по инженерным проблемам интернета.

1506 **IODEF** – формат обмена описаниями инцидентов как объектов, т. е. представление данных,
1507 являющееся основой для совместного использования информации об инцидентах в области
1508 компьютерной безопасности, обмен которой, как правило, осуществляется между группами
1509 реагирования на нарушения компьютерной безопасности (CSIRT).

1510 **ИСО** – Международная организация по стандартизации.

1511 **ISO/IEC 27000-(ISO27k)** – стандарты информационной безопасности, представляющие собой
1512 разработанные на основе передового опыта рекомендации касательно управления
1513 информационной безопасностью, рисков и элементов управления в рамках общей системы
1514 управления информационной безопасностью (ISMS), которая по своему предназначению схожа с
1515 системами управления обеспечением качества (ISO 9000) и защитой окружающей среды (ISO
1516 14000).

1517 **ITIL** – библиотека по инфраструктуре информационных технологий, представляющая собой набор
1518 методов управления ИТ-услугами (ITSM), направленный на приведение ИТ-услуг в соответствие с
1519 бизнес-потребностями.

1520 **Зрелость** – насколько эффективно организация использует ту или иную возможность в рамках
1521 поставленных перед ней задач и переданных ей полномочий.

1522 **Открытый исходный код** – модель разработки, обеспечивающая всеобщий доступ на основе
1523 бесплатной лицензии к проекту или концепции продукции, а также всеобщее распространение
1524 такого проекта или концепции, включая последующие усовершенствования, независимо от того,
1525 кто их внедрил.

1526 **Тест на проникновение** – атака на компьютерную систему с целью найти слабые места в ее
1527 безопасности и возможно получить доступ к ней, ее функционалу и данным.

1528 **Обратный инжиниринг** – процесс извлечения из объекта искусственного происхождения данных,
1529 в том числе проектных, а также воспроизведение такого объекта или чего-либо другого на основе
1530 извлеченных данных.

1531 **RID** – межсетевая защита в реальном времени, т. е. метод межсетевой связи для содействия
1532 совместному использованию данных обработки инцидентов с интегрированным применением
1533 существующих механизмов обнаружения, отслеживания, определения источников и смягчения
1534 последствий, что позволяет обеспечить комплексный подход к обработке инцидентов.

Тестовая среда – механизм обеспечения безопасности, направленный на разделение выполняемых программ.

Услуга – действие, направленное на содействие работе или выполнение работы от имени или в интересах клиентуры.

STIX (Structured Threat Information eXpression) – совместные усилия сообществ, направленные на определения и развитие стандартизированного языка для передачи структурированной информации об угрозах.

Выходная строковая последовательность – конечная последовательность символов либо в виде литерной константы, либо в виде некоей переменной.

TAXII – доверительный автоматизированный обмен информацией о показателях, т. е. комплекс услуг и действий по обмену сообщениями, который при внедрении позволяет обеспечить совместное использование актуальной информации о киберугрозах между организациями, а также связанными с продукцией/услугами субъектами.

TLP – протокол маркировки информации. Применяется для обеспечения обмена конфиденциальной информацией с соответствующей аудиторией.

Виртуальная среда – эмуляция конкретной компьютерной системы.

Сканирование и оценка уязвимостей – метод обеспечения безопасности, предназначенный для обнаружения слабых мест в безопасности компьютерной системы.

Приложение – структура услуг

Как уже говорилось в предыдущих разделах, устанавливаемая данной концепцией структура услуг предполагает определение трех уровней (сферы обслуживания, услуги и функции), позволяющих ответить на вопрос "что", а также двух дополнительных уровней (задачи и действия), позволяющих ответить на вопрос "как".
Упрощенно общая структура выглядит следующим образом: