Version 2.1

TLP:WHITE

Ноябрь 2019 года

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

Версия 2.1

Уведомление. В настоящем документе описаны методы работы, которые, по мнению Форума групп реагирования на инциденты и обеспечения безопасности (FIRST.Org), являются оптимальными. Это описание преследует исключительно информационные цели. FIRST.Org не несет ответственности за ущерб любого рода, вызванный использованием этой информации или связанный с ее использованием.

Содержание

Концепция предоставления услуг CSIRT

1 Цель

Концепция предоставления услуг группами реагирования на инциденты в сфере компьютерной безопасности (CSIRT) – это документ высокого уровня, содержащий структурированное описание ряда услуг в сфере кибербезопасности и связанных с ними функций, которые могут быть предоставлены группами реагирования на инциденты в сфере компьютерной безопасности и другими группами реагирования на инциденты в смежных сферах. Разработчиками этой концепции являются признанные специалисты из экспертного сообщества FIRST, активную поддержку которым оказывало сообщество экспертов Целевой группы CSIRT (ЦГ-CSIRT) и Международный союз электросвязи (МСЭ).

Миссия и цель концепции предоставления услуг CSIRT – содействовать формированию CSIRT и повышению эффективности их работы, особенно в части помощи группам, выбирающим, расширяющим или совершенствующим портфель своих услуг. Здесь описываются услуги, которые потенциально могут предоставлять CSIRT. Ни от одной CSIRT нельзя требовать оказания всего спектра описываемых здесь услуг. Каждой группе необходимо будет выбрать услуги, способствующие выполнению ее миссии и удовлетворению потребностей клиентов, как предусмотрено ее мандатом.

В задачи концепции входит помощь группам путем выделения и определения основных категорий услуг и их составляющих. Для этого дается название и описание каждой услуги, подуслуги, функции, а в случае необходимости – и подфункции. Настоящий документ – это отправная точка для разработки всеобъемлющей концепции предоставления услуг, которая предусматривает стандартный набор терминов и определений для использования в рамках сообщества. Следует отметить, что в этом документе не говорится о том, каким образом следует создавать CSIRT или подобную группу или повышать эффективность их работы. Такого рода сведения можно найти в других документах, часть из которых упомянуты в Приложении 1 в качестве источников дополнительной информации.

Концепция предоставления услуг CSIRT не содержит предложений или рекомендаций относительно возможностей, потенциала, зрелости или качества CSIRT того или иного типа. Такого рода вопросы важны с точки зрения значимости CSIRT для ее клиентов, однако мы намеренно не рассматриваем их в рамках этого документа. Кроме того, в этом документе не рассматриваются вопросы осуществления и не предлагаются конкретные способы оказания той или иной услуги. Важно понимать, что такие услуги можно осуществлять множеством разных способов, обеспечивая при этом удовлетворение обоснованных ожиданий клиентов и заинтересованных сторон.

2 Введение и справочная информация

Группа реагирования на инциденты в сфере компьютерной безопасности – это подразделение (иногда виртуальное) или ресурс, которые в соответствии с их миссией предоставляют услуги и поддержку определенному кругу клиентов в деле предупреждения, обнаружения, рассмотрения и ликвидации инцидентов в сфере компьютерной безопасности.

Должным образом организованная CSIRT имеет четкий мандат, систему управления, соответствующую ее мандату концепцию предоставления услуг, технологии и процедуры, позволяющие предоставлять, измерять и постоянно совершенствовать определенные услуги.

За годы работы различные структуры сообщества CSIRT создали собственные перечни услуг или концепции их предоставления. Сообщество понимало, что по мере изменения технологий, инструментов и процедур появлялись темы и направления деятельности, не предусмотренные существующими перечнями. Стремясь содействовать развитию и становлению CSIRT по всему миру, FIRST признал, что ключевым элементом здесь является создание "общего языка" для всех CSIRT и других структур, сотрудничающих с CSIRT. Учитывая географическое и функциональное разнообразие членов FIRST, было установлено, что сообщество, которое они представляют, является подходящим источником формирования характеристики и структуры предоставляемых CSIRT услуг. Исходя из этого для разработки обновленной концепции предоставления услуг CSIRT был избран подход, основанный на инициативе сообществ, и в 2017 году была опубликована первоначальная версия концепции.

С тех пор аналогичный подход применялся в работе над концепцией предоставления услуг группами реагирования на инциденты в сфере безопасности продукции (PSIRT), хотя при этом учитывалось также, что многие аспекты их деятельности предусматривают необходимость иного набора услуг и соответствующих мероприятий. Все Концепции предоставления услуг размещены на веб-сайте FIRST[1].

Настоящий документ является обновленным вариантом второй версии концепции предоставления услуг CSIRT. Данное издание было переработано и там, где это необходимо, расширено с учетом мнения специалистов, работавших над первым вариантом этого документа. В частности, были удалены разделы о внутренней деятельности, поскольку они не касаются услуг, предоставляемых клиентам. Внутренние и внешние мероприятия по поддержке любой предлагаемой услуги на протяжении всего цикла ее существования можно подразделить на услуги и функции точно так же, как и услуги, которые предполагается предоставлять клиентам. Такие услуги и функции чаще всего называют вспомогательными услугами. К их числу относятся, например, административная деятельность, такая как найм и увольнение сотрудников, возмещение командировочных расходов или организация учебных мероприятий[2].

Наш опыт показывает, что существует множество способов оказания подобных вспомогательных услуг, и в большинстве случаев они зависят от того, в рамках какой организации действует CSIRT

[1] Материалы, касающиеся CSIRT, доступны по адресу https//www.first.org/standards/frameworks/csirts/.

[2] См. обсуждение вопроса о внутренних вспомогательных услугах и их связи с другими услугами в работе [Kossakowski 2001].

или какие услуги ею оказываются. Например очевидно, что вопрос о найме и увольнении сотрудников важен для деятельности CSIRT, однако он относится к числу обычных организационных вопросов и касается не только CSIRT.

Хотя внутренние услуги и функции создают основы, позволяющие любой группе или подразделению выполнять свою миссию, такие вспомогательные услуги не входят в сферу рассмотрения настоящего документа и не будут в дальнейшем описываться или рассматриваться в рамках концепций предоставления услуг, подготовленных FIRST.

По мере того как CSIRT, стремясь защитить своих клиентов от вновь появляющихся угроз, будет сталкиваться со все новыми проблемами, перечень услуг, охватываемых настоящей концепцией, в следующих версиях будет по мере необходимости пересматриваться, сокращаться, дополняться или изменяться[3].

[3] Для организации работы над концепцией предоставления услуг CSIRT в рамках FIRST была создана специальная группа (SIG).

3 Различия между CSIRT и PSIRT

Ориентация на клиентов, равно как и на предоставляемые услуги, определяет основные отличия CSIRT какой-либо организации от других групп по обеспечению безопасности, действующих в рамках той же организации, например PSIRT. В целом основная особенность, определяющая отличия PSIRT от любой другой группы по обеспечению безопасности, действующей в рамках организации, в том числе и CSIRT, – это работа с продуктами.

В рамках организации структура CSIRT занимается безопасностью компьютерных систем и сетей, образующих инфраструктуру организации. Если в крупной организации действуют несколько групп по обеспечению безопасности и CSIRT, то одна из них может выступать в качестве координатора и единого контактного центра для внешних сторон. Такие группы называют координационными CSIRT.

Подобные координационные CSIRT создаются также и в качестве самостоятельных структур, работающих с конкретным кругом лиц и/или организаций, именуемых клиентурой. Организации, относящиеся к определенной клиентуре, обладают некоторыми общими характеристиками (например, входят в состав национальной исследовательской сети или действуют в конкретной стране). Координационная CSIRT является единым контактным центром для всей группы и занимается общими вопросами безопасности данных организаций.

Сегодня создаются координационные CSIRT нового типа – национальные CSIRT, в задачи которых входит содействие, а зачастую и координация деятельности CSIRT, действующих в той или иной стране, или предоставление ограниченного спектра услуг всем гражданам, конкретным подразделениям важнейших инфраструктурных предприятий этой страны и т. п.

Хотя между всевозможными CSIRT и PSIRT существуют важные различия, необходимо учитывать, что между этими двумя структурами есть и синергия. Большое значение имеет тот факт, что ни CSIRT, ни PSIRT не действуют в отрыве друг от друга; например, многие CSIRT предупреждают своих клиентов об уязвимостях с точки зрения безопасности. Почти всегда в основе таких предупреждений лежат сведения, которые предоставляют PSIRT поставщиков.

4 Структура концепции предоставления услуг CSIRT

Структура Концепции предоставления услуг CSIRT основана на взаимосвязях между четырьмя основными элементами:

СФЕРЫ ОБСЛУЖИВАНИЯ → УСЛУГИ → ФУНКЦИИ → ПОДФУНКЦИИ

Эти элементы определяются следующим образом.

СФЕРЫ ОБСЛУЖИВАНИЯ

Сферы обслуживания объединяют услуги, связанные наличием общей характеристики. Они помогают упорядочить услуги путем тщательного распределения на группы, чтобы сделать их более понятными и упростить коммуникации. Определение для каждой сферы обслуживания включает раздел "Описание" – текст общего характера с описанием сферы обслуживания, а также перечень услуг в рамках данной сферы обслуживания.

УСЛУГИ

Услуга – это комплекс узнаваемых, связанных между собой действий, направленных на достижение конкретного результата. Такие результаты могут быть ожидаемы клиентами или заинтересованной стороной той или иной структуры либо востребованы ими или от их имени.

Определение услуги дается по следующей схеме:

- раздел "Описание", в котором описывается характер услуги;
- раздел "Цель", в котором описывается назначение услуги;
- раздел "Результат", в котором описываются измеримые результаты услуги.

ФУНКЦИИ

Функция – это действие или набор действий, обеспечивающие достижение цели той или иной услуги. Любая функция может быть распределенной и использоваться применительно к разным услугам.

Определение функции дается по следующей схеме:

- раздел "Описание", в котором описывается функция;
- раздел "Цель", в котором описывается назначение функции;
- раздел "Результат", в котором описываются измеримые результаты функции;
- перечень подфункций, которые можно выполнить в рамках той или иной функции.

ПОДФУНКЦИИ

Подфункция – это действие или набор действий, обеспечивающие достижение цели той или иной функции. Любая подфункция может быть распределенной и использоваться применительно к разным функциям и/или услугам. Подфункции могут выполняться факультативно или быть необходимыми для любой из таких функций и/или услуг.

Определение подфункции также дается по следующей схеме:

- раздел "Описание", в котором описывается подфункция;
- раздел "Цель", в котором описывается назначение подфункции;
- раздел "Результат", в котором описываются измеримые результаты подфункции.

В рамках концепции предоставления услуг CSIRT полного описания подфункций не дается. Приводится только краткая характеристика каждой подфункции.

На рисунке ниже представлены сферы обслуживания и услуги, описанные в концепции предоставления услуг CSIRT. Полный перечень сфер обслуживания, услуг и функций приводится в Приложении 4.

5 Сфера обслуживания: управление событиями в сфере информационной безопасности

Задача управления событиями в сфере информационной безопасности заключается в выявлении инцидентов в области информационной безопасности путем сопоставления и анализа данных о событиях в области безопасности и контекстуальных данных, которые поступают из широкого круга источников. В более крупных организациях эта сфера обслуживания иногда полностью или частично отнесена к сфере ведения центра обеспечения безопасности (SOC), который может также заниматься управлением инцидентами в сфере информационной безопасности первого и даже второго уровня, например инициировать меры по смягчению или корректировке систем контроля безопасности. Поскольку работа любой структуры, занимающейся управлением инцидентами в сфере информационной безопасности, зависит от качества и достоверности данных о событиях в области информационной безопасности, взаимодействие между SOC и соответствующей CSIRT имеет решающее значение[4].

В данной сфере обслуживания предполагается предоставление следующих услуг:

- мониторинг и обнаружение;
- анализ событий.

5.1 Услуга: мониторинг и обнаружение

Цель: внедрить автоматизированный непрерывный процесс обработки поступающих из широкого круга источников сведений о событиях в сфере информационной безопасности и контекстуальных данных, чтобы выявлять информацию о возможных инцидентах в сфере информационной безопасности, таких как атаки, проникновения, утечки данных или нарушения политики безопасности.

Описание: на основании данных регистрации, данных NetFlow, IDS-оповещений, сенсорных сетей, внешних источников или другой имеющейся информации о событиях в области информационной безопасности применять широкий спектр методов – от простой логики или правил сопоставления случаев до применения статистических моделей или машинного обучения – для выявления возможных инцидентов в сфере информационной безопасности. Это может быть сопряжено с обработкой больших массивов данных, что в большинстве случаев, хотя и не всегда, требует применения таких специальных инструментов, как технология управления информацией и событиями безопасности (SIEM) или платформы больших данных. Важная цель постоянного повышения эффективности заключается в сведении к минимуму частоты ложных тревог, которые подлежат анализу в рамках услуги анализа.

[4] Хотя данная концепция предоставления услуг не ставит своей задачей определение концепции предоставления услуг SOC, очевидно, что услуги в рамках управления как событиями, так и инцидентами в сфере информационной безопасности могут быть полезны и использованы напрямую при определении услуг, предоставлением которых занимается SOC.

Результат: выявление потенциальных инцидентов в области информационной безопасности для последующего анализа в рамках услуги анализа.

В рамках данной услуги следует предполагается осуществление следующих функций:

- управление журналами регистрации и датчиками;
- управление моделями обнаружения;
- управление контекстуальными данными.

5.1.1 Функция: управление журналами регистрации и датчиками

Цель: управление журналами регистрации и датчиками.

Описание: оперативное управление датчиками и журналами регистрации должно осуществляться на всем протяжении срока их эксплуатации. Необходимо осуществлять их установку, предоставлять к ним доступ и выводить из эксплуатации. Должны выявляться и решаться проблемы, связанные с перебоями в их работе, качеством/объемом данных и конфигурацией. Если датчики требуют какого-либо конфигурирования, например на основе определений шаблонов, такую конфигурацию необходимо поддерживать, чтобы обеспечивать эффективность их работы. Кроме того, датчики могут включать внешние службы обнаружения и системы расследования на основе открытых информационных источников (OSINT), если на них основываются модели обнаружения.

Результат: возможность получения массива достоверной информации о событиях в области информационной безопасности в качестве исходных данных для моделей обнаружения.

5.1.2 Функция: управление моделями обнаружения

Цель: управление портфелем моделей обнаружения на всем протяжении их жизненного цикла.

Описание: новые подходы к обнаружению предусматривают разработку, тестирование, совершенствование и, в конечном счете, внедрение в практику моделей обнаружения. Необходимо разрабатывать инструкции для аналитической сортировки, квалификации и определения соотношений, например в форме наборов сценариев или типовых регламентов (TP). Неэффективные модели обнаружения, то есть имеющие неудовлетворительное соотношение между выгодами и затраченными усилиями, необходимо совершенствовать, пересматривать или отказываться от них. Портфель моделей обнаружения необходимо расширять основанными на анализе рисков методами и с учетом данных упреждающего контроля.

Результат: разработка портфеля эффективных моделей обнаружения, учитывающих интересы клиентов.

5.1.3 Функция: управление контекстуальными данными

Цель: управление источниками контекстуальных данных, применяемых для обнаружения и подкрепления.

Описание: управление различными источниками контекстуальных данных, применяемых для обнаружения и подкрепления, должно осуществляться на всем протяжении их жизненного цикла. Ручного управления могут требовать, в частности, действующие в режиме реального времени API для загрузки данных в другие IT-системы или экспорта данных из них, например база данных управления конфигурацией (CMDB), управление определением идентичности и доступом (IAM) или системы анализа угроз безопасности либо совершенно отдельные наборы данных. В последнем случае для отсеивания ложноположительных результатов можно использовать списки индикаторов, списки отслеживания и белые списки.

Результат: доступность новейших контекстуальных данных, которые могут быть использованы для обнаружения и подкрепления.

5.2 Услуга: анализ событий

Цель: сортировка выявленных возможных инцидентов в области информационной безопасности и их отнесение либо к категории инцидентов в области информационной безопасности для дальнейшей передачи в сферу обслуживания управления инцидентами в сфере информационной безопасности, либо к категории ложных тревог.

Описание: вся поступающая информация об обнаруженных возможных инцидентах в области информационной безопасности должна быть отсортирована, и каждый такой случай квалифицируется средствами ручного и/или автоматического анализа либо как инцидент в области информационной безопасности (истинно положительный), либо как ложная тревога (ложноположительный). В зависимости от модели обнаружения для этого может потребоваться ручной или автоматизированный сбор дополнительных данных. Приоритет следует отдавать анализу потенциально более серьезных инцидентов в области информационной безопасности, чтобы обеспечить своевременное реагирование там, где это наиболее важно. Структурированная квалификация выявленных потенциальных инцидентов в области информационной безопасности позволяет целенаправленно и на постоянной основе принимать эффективные меры по улучшению положения дел за счет выявления моделей обнаружения, источников данных или процедур, испытывающих проблемы с качеством.

Результат: классифицированные и коррелированные инциденты в области информационной безопасности передаются в сферу обслуживания по управлению инцидентами в сфере информационной безопасности, а ложноположительные определяются как таковые, что способствует дальнейшему повышению качества этой работы.

В рамках данной услуги предполагается осуществление следующих функций:

- корреляция;
- классификация.

5.2.1 Функция: корреляция

Цель: выявление событий, непосредственно связанных с другими потенциальными или происходящими инцидентами в области безопасности.

Описание: потенциальные инциденты в области информационной безопасности, которые касаются одних и тех же ресурсов (например, систем, услуг, клиентов) или лиц (например, пользователей) либо иным образом непосредственно связаны с другими потенциальными инцидентами в области информационной безопасности, во избежание дублирования усилий сводятся в одну группу и передаются далее как единый инцидент в области информационной безопасности. Вновь выявленные потенциальные инциденты в области информационной безопасности, непосредственно связанные с текущими инцидентами в области информационной безопасности, объединяются с ними и не рассматриваются как новый отдельный инцидент в области информационной безопасности.

Результат: группировка связанных между собой потенциальных инцидентов в области информационной безопасности для их общей классификации или обновления данных по инциденту в области информационной безопасности, работа по которому уже ведется в рамках сферы обслуживания по управлению инцидентами в сфере информационной безопасности.

5.2.2 Функция: классификация

Цель: сортировка и классификация выявленных потенциальных инцидентов в области информационной безопасности, с тем чтобы идентифицировать и распределить по категориям и степени приоритетности истинно положительные инциденты.

Описание: потенциальные инциденты в области информационной безопасности необходимо отсортировать, классифицировав каждый из них либо как инцидент в области информационной безопасности (истинно положительный), либо как ложную тревогу (ложноположительный). Учитывая, что аналитики могут изучить лишь ограниченное количество потенциальных инцидентов в области информационной безопасности, а также чтобы не допустить притупления внимания, необходимо автоматизировать эти процессы. Хороший инструментарий способствует эффективности сортировки, обеспечивая при этом учет контекстуальной информации и рейтинговую оценку степени риска, исходя из значимости данной проблемы для затронутых систем и идентификационных данных, и/или автоматически выделяя связанные с этим события в сфере информационной безопасности. Необходимо выделять повторяющиеся случаи, допускающие автоматизацию, и автоматизировать их анализ. Анализ более значимых потенциальных инцидентов в области информационной безопасности должен предшествовать анализу менее серьезных случаев. Помимо разделения инцидентов на истинно положительные и ложноположительные, более детальная классификация может стать важным вкладом в постоянное совершенствование моделей обнаружения, а также управление журналами регистрации, датчиками и источниками контекстуальных данных. Более подробная классификация может способствовать также более качественному определению KPI для оценки степени успешности работы в этой сфере обслуживания.

Результат: классификация потенциальных инцидентов в области информационной безопасности для дальнейшей работы с ними в сфере обслуживания по управлению инцидентами в сфере информационной безопасности.

6 Сфера обслуживания: управление инцидентами в сфере информационной безопасности

Эта сфера обслуживания является основной для любой CSIRT и предусматривает услуги, жизненно важные для оказания помощи клиентам в случае атаки или инцидента. CSIRT должны быть готовы оказать помощь и поддержку. Благодаря своему уникальному положению и опыту эти группы могут не только получать и оценивать отчеты об инцидентах в сфере информационной безопасности, но и анализировать соответствующие данные и проводить подробный технический анализ самого инцидента и примененных артефактов.

На основании этого анализа можно рекомендовать меры по смягчению и преодолению последствий инцидента, а клиенты получат помощь в осуществлении этих рекомендаций. Это также требует координации усилий с внешними структурами, например родственными CSIRT или специалистами по безопасности, поставщиками или PSIRT, по всестороннему изучению этих вопросов и сокращению в будущем числа успешных атак.

Уникальный опыт, которым обладают CSIRT, играет огромную роль и в преодолении кризисных ситуаций (в сфере информационной безопасности). Хотя зачастую кризисным управлением занимается не CSIRT, она может оказывать содействие любой подобной работе. Например, поделившись своими контактами, группа может существенно повысить качество осуществления необходимых мер смягчения последствий или улучшить работу механизмов защиты.

Использование знаний и имеющейся инфраструктуры для оказания помощи клиентам – это залог общего повышения качества управления инцидентами в области информационной безопасности.

В данной сфере обслуживания предполагается предоставление следующих услуг:

- получение отчетов об инцидентах в сфере информационной безопасности;
- анализ инцидентов в сфере информационной безопасности;
- анализ артефактов и данных экспертиз;
- смягчение и преодоление последствий;
- координация реагирования на инциденты в сфере информационной безопасности;
- поддержка управления в кризисных ситуациях.

6.1 Услуга: получение отчетов об инцидентах в сфере информационной безопасности

Цель: получение и обработка отчетов клиентов, служб по управлению событиями в сфере информационной безопасности или третьих лиц о потенциальных инцидентах в сфере информационной безопасности.

Описание: важнейшей задачей CSIRT является получение отчетов о событиях в сфере информационной безопасности и потенциальных инцидентах в сфере информационной безопасности, затрагивающих сети, компьютерные устройства, компоненты, пользователей, организации или инфраструктуру (именуемые также объектами атаки) в рамках клиентуры

группы. CSIRT необходимо помнить о том, что отчеты о потенциальных инцидентах в сфере информационной безопасности могут поступать из разных источников, в разных форматах и передаваться как вручную, так и автоматически.

Чтобы клиенты CSIRT могли эффективнее сообщать об инцидентах в области информационной безопасности, группе необходимо предоставить в их распоряжение один или несколько механизмов, а также рекомендации или инструкции относительно того, о чем следует сообщать и как можно безопасно передавать отчеты об инцидентах в сфере информационной безопасности. Механизмы передачи отчетов могут предусматривать возможность использования электронной почты, веб-сайта, заполнения специального формуляра об инциденте в области информационной безопасности или выхода на соответствующий портал, а также использования других методов, обеспечивающих безопасность и защищенность передаваемых отчетов. Рекомендации по порядку представления отчетов, если они не включены в формуляр отчета об инциденте в области информационной безопасности, следует представлять в виде отдельного документа или размещать на веб-сайте; в них следует указать, какую конкретную информацию желательно включать в отчет.

Ввиду того что потенциально большой объем данных о потенциальных инцидентах в сфере информационной безопасности, выявленных в рамках услуги по управлению событиями в сфере информационной безопасности, будет передаваться автоматически, необходимо заранее подумать об использовании соответствующих интерфейсов или о предоставлении клиентам возможности их использовать[5].

Результат: получение каждого отчета об инциденте в сфере информационной безопасности, а также их первоначальная оценка и классификация происходят профессионально и организованно.

В рамках данной услуги предполагается осуществление следующих функций:

- прием отчетов об инцидентах в сфере информационной безопасности;
- сортировка и обработка отчетов об инцидентах в сфере информационной безопасности.

6.1.1 Функция: прием отчетов об инцидентах в сфере информационной безопасности

Цель: прием или получение информации об инцидентах в сфере информационной безопасности, поступающей от клиентов или третьих лиц.

Описание: для успешного приема отчетов об инцидентах в сфере информационной безопасности необходимы механизмы и процедуры получения отчетов от клиентов, заинтересованных сторон и третьих лиц (например, лиц, обнаруживающих уязвимости,

[5] Очевидно, что все услуги по приему информации и данных имеют между собой очень много общего. Поэтому обычно такие услуги, относящиеся к разным сферам обслуживания, сводятся в единую услугу/функцию. Поскольку это не обязательно и так как единого набора сфер обслуживания не существует, мы решили не объединять эти услуги в концепции предоставления услуг CSIRT, хотя каждая группа вправе выбрать ту организационную модель, которая лучше всего подходит для нее.

исследователей, центров анализа и обмена информацией (ISAC), других CSIRT). В отчетах об инцидентах в сфере информационной безопасности могут приводиться сведения о затронутых устройствах/сетях/пользователях/организациях, о ранее выявленных обстоятельствах, например использованных уязвимостях, последствиях как технического, так и делового характера, а также о мерах, которые необходимо принять для того, чтобы приступить к устранению и/или смягчению последствий, а в дальнейшем – и к устранению причин инцидента. Иногда информация об инциденте в сфере информационной безопасности может поступать в составе исходных данных для других услуг, чаще всего для услуги получения отчетов об уязвимостях (например, если в отчете речь идет об инциденте в сфере информационной безопасности, выявленном в ходе анализа отчета об уязвимости). Необходимость или отсутствие необходимости подтверждения получения автоматически переданных отчетов определяется применяемыми интерфейсами и протоколами.

Результат: обеспечивается должная обработка отчетов об инцидентах в сфере информационной безопасности, поступающих от клиентов или третьих лиц, включая инициирование их документального оформления или проверки.

В рамках данной функции предполагается осуществление следующих подфункций:

- регулярный мониторинг каналов связи и проверка работоспособности заявленных средств связи с CSIRT и возможности направлять по ним отчеты;
- направление лицу, представляющему отчет об инциденте в сфере информационной безопасности, первоначального подтверждения получения отчета, запрос дополнительной информации в случае необходимости и совместное определение желаемых результатов.

6.1.2 Функция: сортировка и обработка отчетов об инцидентах в сфере информационной безопасности

Цель: первоначальное изучение, классификация, приоритизация и обработка отчетов об инцидентах в сфере информационной безопасности.

Описание: отчеты об инцидентах в сфере информационной безопасности изучаются и сортируются, чтобы получить первоначальное представление о соответствующем инциденте в сфере информационной безопасности. Особенно важно понять, имел ли он реальные последствия для информационной безопасности объекта атаки и может ли привести (или уже привел) к нарушению конфиденциальности, доступности, целостности и/или аутентичности информационных или иных ресурсов. Степень подробности и качество информации, представленной в первоначальном отчете, могут позволить или не позволить понять, имел ли место реальный инцидент в сфере информационной безопасности или же в его основе лежат другие причины, такие как неправильная конфигурация или отказ аппаратного обеспечения. Предварительная оценка позволит определить следующий шаг (например, обработка отчета для последующего анализа; запрос на предоставление дополнительной информации от лица, представившего отчет, или из иных источников; принятие решения о том, что отчет не требует дальнейших действий или является ложной тревогой).

Существует вероятность того, что атаку может осуществлять некто из числа клиентов CSIRT, что ее клиенты могут являться объектами атаки или что клиенты окажутся затронутыми лишь побочно. Если CSIRT не предоставляет выявленным объектам атаки услуги по управлению информационной безопасностью, то отчет следует безопасным образом передать для принятия дальнейших мер внешней группе, например затронутой организации (организациям) или CSIRT.

В случае если нет оснований отклонять отчет об инциденте в сфере информационной безопасности или если он не был передан в другую структуру, ответственную за его рассмотрение, отчет следует передать в службу анализа уязвимостей для дальнейшего изучения, анализа и обработки.

Результат: есть возможность определить, действительно ли случай, о котором идет речь в отчете, является инцидентом в сфере информационной безопасности, который подлежит рассмотрению силами CSIRT или передаче в другую соответствующую структуру.

В рамках данной функции предполагается осуществление следующих подфункций:

- обработка отчетов и представленных данных, включая отдельные артефакты или материалы, для защиты целостности рабочей среды и недопущения применения подобных средств для успешных атак на CSIRT;
- повторное выражение признательности за отчет путем предоставления определенной информации о дальнейших мерах по итогам классификации и приоритизации;
- добавление новой информации об уже рассмотренных инцидентах в сфере информационной безопасности к ранее полученным данным, чтобы обеспечить последовательный анализ и обработку.

6.2 Услуга: анализ инцидентов в сфере информационной безопасности

Цель: анализ и понимание сути подтвержденного инцидента в сфере информационной безопасности.

Описание: эта услуга предусматривает функции, позволяющие понять суть инцидента в сфере информационной безопасности и его реальные и потенциальные последствия, чтобы выявить соответствующие факторы, уязвимости или слабые места (основные причины), позволившие произвести успешную атаку, нарушение или эксплойт.

Детальный анализ зачастую сложен в проведении и занимает много времени. Задача состоит в том, чтобы выявить и описать инцидент в сфере информационной безопасности настолько подробно, насколько этого требует или это предполагает имеющееся на данный момент представление о его последствиях. Инциденты в сфере информационной безопасности могут быть описаны с точки зрения их масштабов, затронутых структур, использованных инструментов или методов атаки, временных рамок и т. д. Работа в рамках этой услуги может проводиться параллельно с осуществлением услуг и функций по координации реагирования на инциденты в сфере информационной безопасности и принятием мер по смягчению/преодолению последствий.

Чтобы лучше понять, что именно произошло и какие меры следует принять для возмещения потерь или ущерба, CSIRT может воспользоваться другой информацией и данными собственного анализа (см. варианты ниже) или сведениями, полученными от поставщиков, групп реагирования на инциденты в сфере безопасности продукции или исследователей, занимающихся проблемами безопасности.

Результат: увеличение объема знаний о ключевых деталях инцидента в сфере информационной безопасности (например, описание, последствия, масштабы, атаки/эксплойты и пути решения проблемы).

В рамках данной услуги предполагается осуществление следующих функций:

- сортировка инцидентов в сфере информационной безопасности (приоритизация и классификация);
- сбор информации;
- координация процесса подробного анализа;
- анализ основных причин инцидента в области информационной безопасности;
- сопоставление инцидентов.

6.2.1 Функция: сортировка инцидентов в сфере информационной безопасности (приоритизация и классификация)

Цель: классификация, приоритизация и первоначальная оценка инцидента в сфере информационной безопасности.

Описание: осуществление услуги по анализу инцидентов в сфере информационной безопасности начинается с обзора имеющейся информации, чтобы провести классификацию и приоритизацию этого инцидента и оценить его последствия для затронутых систем, относящихся к сфере ведения CSIRT. Если сведения об инциденте в сфере информационной безопасности были переданы в CSIRT клиентом или третьей стороной, некоторая часть этой работы может быть проведена в рамках осуществления функции по сортировке и обработке отчетов об инцидентах в сфере информационной безопасности, относящейся к услуге получения отчетов об инцидентах в сфере информационной безопасности.

Если предварительная сортировка еще не завершена, данные об инциденте в сфере информационной безопасности могут быть переданы соответствующему эксперту, который может предоставить техническое подтверждение того, что инцидент имел определенные последствия для затронутых систем и что он относится к сфере ведения CSIRT (то есть может оказать воздействие на безопасность сетей или систем, что может повлечь за собой нарушение конфиденциальности, доступности или целостности информационных ресурсов, которые, в соответствии с мандатом CSIRT, относятся к сфере ее ведения).

Результат: проведены классификация, приоритизация и обновление данных об инциденте в сфере информационной безопасности.

6.2.2 Функция: сбор информации

Цель: прием, каталогизация, хранение и отслеживание сведений об инциденте в сфере информационной безопасности и любых относящихся к нему данных о событиях в сфере информационной безопасности.

Описание: обеспечение сбора всей ценной информации, позволяющей глубже понять сопутствующие обстоятельства, чтобы иметь возможность должным образом оценить и маркировать происхождение и содержание информации для любой последующей обработки.

В процессе сбора информации необходимо знать и соблюдать согласованную политику и ограничения в отношении того, какие данные можно использовать, в каком контексте или для какого вида обработки. Кроме того, механизмы и процедуры сбора информации должны предусматривать необходимую маркировку и фиксацию ее источников, чтобы дать возможность в дальнейшем подтвердить ее происхождение, пригодность или аутентичность.

Результат: наличие структурированной информации о собранных цифровых и нецифровых данных или метаданных, а также информации об отслеживании и пунктов контроля ее целостности в процессе обработки и хранения. В зависимости от того как планируется использовать полученные результаты в дальнейшем – для последующего (неформального) анализа или в рамках деятельности правоохранительных органов – предъявляются различные требования к соблюдению официального порядка передачи и хранения улик, которые позднее могут фигурировать в ходе судебного разбирательства.

В рамках данной функции предполагается осуществление следующих подфункций:

- анализ и проверка источников, из которых поступают данные и информация;
- сбор отчетов касательно вредоносных и подозрительных происшествий, событий в сфере информационной безопасности, потенциально серьезных инцидентов в сфере информационной безопасности и/или отчетов об инцидентах в сфере информационной безопасности, 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 и каталогизация цифровых данных, которые могут, хотя это и не гарантировано, оказаться полезными для понимания связанной с инцидентами деятельности (например, образ диска и копии содержимого памяти, файлы, содержащие метаданные или контрольные суммы, характеристики архитектуры сети, сетевые журналы); к их числу относятся, среди прочего, артефакты, которые могут рассматриваться как свидетельства враждебной деятельности;
- сбор и каталогизация нецифровых данных (например, журналов посещений в неэлектронной форме, архитектурных схем, бизнес-моделей, данных по оценке тех или иных объектов, политики, концепции управления корпоративными рисками);
- сбор и каталогизация метаданных об источниках, методах сбора, лицах, проводивших обработку данных или объектов, о собственнике информации, а также об обеспечении сохранности информации, особенно если в дальнейшем это может быть использовано как свидетельства для экспертизы или для деятельности правоохранительных органов.

6.2.3 Функция: координация процесса подробного анализа

Цель: инициирование и отслеживание любых других видов технического анализа в отношении инцидента в сфере информационной безопасности.

Описание: ввиду того что может возникнуть необходимость в более подробном техническом анализе, такой анализ могут проводить другие эксперты (являющиеся или не являющиеся сотрудниками основной организации или CSIRT) или третьи лица (например, поставщик услуг, специализирующийся на проведении такого анализа). Для этого необходимо инициировать такого рода мероприятия и отслеживать их проведение вплоть до завершения требуемого анализа.

Результат: наличие перечня требуемых анализов, которые, по мнению лица, координирующего меры по устранению того или иного инцидента в сфере информационной безопасности, следует проводить силами сторонних организаций.

6.2.4 Функция: анализ основных причин инцидента в сфере информационной безопасности

Цель: установление основных причин инцидента в сфере информационной безопасности путем выявления обстоятельств, в силу которых использованные уязвимости имели место или стало возможным успешное применение эксплойтов (включая, в частности, поведение пользователя).

Описание: эта функция предусматривает выполнение процедур и проведение мероприятий, необходимых для того, чтобы понять, какие именно недочеты архитектуры, использования или реализации обусловили или позволили подвергнуть системы, пользователей, организации и т. д. атаке либо воздействию эксплойта или несанкционированного доступа, осуществленным в отношении объектов инцидента в сфере информационной безопасности. Кроме того, при этом изучаются обстоятельства, при которых злоумышленник мог получить несанкционированный доступ к большему количеству систем, используя первоначально полученный доступ для того, чтобы расширить его в дальнейшем.

Иногда, с учетом характера инцидента в сфере информационной безопасности, CSIRT может столкнуться с проблемами в попытке должным образом осуществить эту функцию. Во многих случаях лучше всего такую функцию может осуществить сам объект атаки, особенно если CSIRT, занимающиеся вопросами координации, не имеют достаточных технических знаний о системах или сетях, подвергшихся взлому.

Результат: изучена информация об инциденте в сфере информационной безопасности и о способах, которыми злоумышленник получил первоначальный доступ и в дальнейшем расширил его, что позволяет определить методы преодоления или смягчения последствий и благодаря устранению основных причин свести к минимуму риск нарушения безопасности или использования эксплойтов в будущем.

6.2.5 Функция: сопоставление инцидентов

Цель: обеспечение возможности использования всей имеющейся информации, чтобы в максимальной степени понять сопутствующие обстоятельства и выявить взаимосвязи, которые в противном случае остались бы скрытыми и в отношении которых не было бы предпринято никаких действий.

Описание: эта функция предполагает сопоставление всей имеющейся информации о различных инцидентах в сфере информационной безопасности в целях выявления взаимосвязей, тенденций или возможных мер по смягчению последствий, успешно применявшихся в ходе уже закрытых инцидентов в сфере информационной безопасности, с тем чтобы повысить эффективность реагирования на инциденты в сфере информационной безопасности, обработка которых осуществляется в настоящее время.

Результат: обеспечено понимание ситуации в более широком плане на базе детального изучения сходства и подтвержденных или предполагаемых взаимосвязей с другими инцидентами в сфере информационной безопасности, никак не связанными с данным.

6.3 Услуга: анализ артефактов и данных экспертиз

Цель: анализ и понимание сути артефактов, имеющих отношение к подтвержденному инциденту в сфере информационной безопасности, с учетом необходимости обеспечить сохранность данных экспертиз.

Описание: услуги, связанные с изучением возможностей и назначения артефактов (например, вредоносных программных средств, эксплойтов, дампов энергозависимой памяти или копий дисков, прикладных кодов, журналов регистрации, документов), механизмов их доставки, их распространения, обнаружения, смягчения их воздействия, их обезвреживания или нейтрализации. Услуги применяются в отношении любых форматов и источников – компьютерного оборудования, встроенных программ, памяти, программного обеспечения и т. д. Все артефакты и все данные следует сохранять и собирать, не допуская их изменения, и хранить отдельно. Учитывая, что некоторые артефакты и данные могут приобретать характер улик в процессе работы правоохранительных органов, в их отношении могут применяться особые правовые нормы или требования.

Даже в отсутствие официальной процедуры обеспечения сохранности эта услуга, как правило, предполагает решение сложных и трудоемких задач и требует наличия опыта, обеспечения специальных и контролируемых условий для анализа, допускающих или не допускающих доступ извне по обычным проводным или беспроводным сетям (например, проведения экспертиз в герметичном помещении или клетке Фарадея), регистрацию мероприятий и соблюдение процедур.

В рамках процесса обработки инцидентов в сфере информационной безопасности цифровые артефакты можно обнаружить в затронутых системах или в местах распространения вредоносных программных средств. В качестве артефактов могут выступать следы попыток несанкционированного доступа, такие как исполняемые файлы, скрипты, файлы, изображения, файлы конфигурации, инструменты, результаты их использования, журналы регистрации, активные или недействующие элементы кода и т. п.

Целью проведения этого анализа является выявление всей перечисляемой ниже информации или ее части, притом что данный список не является исчерпывающим:

- условия, при которых артефакт может работать и выполнять поставленные задачи, будь то вредоносные или нет;
- возможные способы использования артефакта для атаки: загрузка в сеть, выгрузка из сети, копирование, исполнение или создание в рабочей среде или компонентах организации;
- какие системы использовались на месте и дистанционно для содействия в распространении и приведении в действие;
- что нарушитель сделал для получения доступа к системе, сети, организации или инфраструктуре – от пассивного сбора данных до активного сканирования и передачи данных в целях организации их утечки либо получения новых запросов о действии, самообновления или применения метода бокового смещения для проникновения во взломанную (местную) сеть;
- что было сделано пользователем, процессором пользователя или системой пользователя после того, как аккаунт или устройство пользователя были взломаны;
- каковы особенности поведения артефакта или взломанных систем, будь то при работе в автономном режиме, во взаимосвязи с артефактами или компонентами, при подключении к местной сети или интернету либо в любой иной комбинации;
- каким образом артефакты или взломанные системы устанавливают связь с объектом атаки (например, путь проникновения, первоначальная цель или методы уклонения от обнаружения);
- какая архитектура связи была использована (одноранговая, командование и управление, обе одновременно);
- какие действия предприняли злоумышленники, как можно отследить их сеть и системы;
- каким образом злоумышленники или артефакты избежали обнаружения (даже в течение длительных периодов времени, иногда включая перезагрузку или повторную инициализацию).

Сделать это можно путем проведения различных мероприятий, к числу которых относятся:

- анализ мультимедийной информации или состояния поверхности носителя;
- обратный инжиниринг;
- анализ в ходе выполнения или динамический анализ;
- сравнительный анализ.

Каждое мероприятие позволяет получить дополнительную информацию об артефактах. Методы анализа включают, среди прочего, определение вида и характеристик артефакта, его сравнение с известными артефактами, наблюдение за работой артефакта в динамике или в естественных условиях, а также разборку и интерпретацию двоичных артефактов.

Анализируя артефакты, аналитик стремится воспроизвести и установить действия нарушителя, чтобы можно было выявить использованную уязвимость, оценить ущерб, разработать решения, позволяющие смягчить последствия использования артефактов, а также предоставить информацию клиентам и другим исследователям.

Результат: изучены природа выявленных цифровых артефактов и проанализированные данные экспертиз, а также их взаимосвязь с другими артефактами, внутренними или внешними объектами или компонентами, атаками на объектные структуры, инструментами и использованными уязвимостями. Сформулированы рабочие гипотезы или найдены доказательства действий злоумышленника и поведения артефактов. Эта информация имеет огромное значение для оценки потерь, ущерба, последствий для бизнеса и т. д., а также для разработки стратегий сдерживания и смягчения или преодоления последствий. Изучены тактика, методы и процедуры, которые нарушители или злоумышленники применяли для получения несанкционированного доступа к системам, пользователям, сетям, организациям и/или инфраструктурам. При этом объектом изучения являются, в числе прочего, тактика, методы и процедуры, применявшиеся для распространения, переноса, обновления, модификации или фальсификации своего поведения, данных, автоматического удаления следов своей деятельности или совершения других вредоносных действий.

В рамках данной услуги предполагается осуществление следующих функций:

- анализ мультимедийной информации и поверхности носителя информации;
- обратный инжиниринг;
- анализ в ходе выполнения и/или динамический анализ;
- сравнительный анализ.

6.3.1 Функция: анализ мультимедийной информации и поверхности носителя информации

Цель: сопоставление информации, извлеченной из артефакта, с другими публичными или частными артефактами и/или репозиториями подписей.

Описание: данная функция предполагает выявление и описание основной информации и метаданных об артефактах, включая, в частности, типы файлов, выходные строковые последовательности, криптографические хеши, сертификаты, размеры файлов, названия файлов/каталогов. По мере сбора и дальнейшего анализа всей имеющейся информации она может быть использована для изучения хранилищ информации из всех публичных/открытых или частных/закрытых источников, чтобы получить более полное представление об артефакте или его поведении, поскольку такого рода информация может быть использована для определения последующих шагов.

Результат: определены характеристики и/или подпись цифрового артефакта, а также выявлена вся известная информация о нем, включая информацию о его вредоносности, воздействии и способах смягчения последствий его использования.

6.3.2 Функция: обратный инжиниринг

Цель: более глубокий анализ статических характеристик артефакта, чтобы определить, насколько полнофункциональным он является независимо от среды, в которой может проходить его исполнение.

Описание: проводится более глубокий анализ вредоносных артефактов, включая обнаружение скрытых действий и команд инициирования. Обратный инжиниринг позволяет аналитику обойти любые запутанные места и компиляции (в двоичных артефактах) и обнаружить программу, скрипт или код, составляющие вредоносное программное средство, либо найдя исходный код, либо разобрав двоичный артефакт в целях установления и интерпретации языка его сборки. Аналитик выявляет все открытые функции и действия машинного языка, которые может осуществлять вредоносное программное средство. Обратный инжиниринг представляет собой более глубокий анализ, проводимый тогда, когда анализ поверхности и динамический анализ не могут дать всей необходимой информации.

Результат: установлена полная функциональность цифрового артефакта, позволяющая понять, как он функционирует, как запускается, каковы связанные с этим слабые места системы, которыми можно воспользоваться, каковы совокупное воздействие артефакта и наносимый им потенциальный ущерб, что дает возможность разработать решения, позволяющие смягчить последствия применения артефакта и, при необходимости, создать новую подпись для сравнения с другими образцами.

В рамках данной функции предполагается осуществление следующих подфункций:

- статический анализ;
- обратный инжиниринг кода;
- анализ и описание потенциального поведения;
- возможная структура подписи.

6.3.3 Функция: анализ в ходе выполнения или динамический анализ

Цель: получение представления о том, как действует артефакт.

Описание: эта функция предполагает изучение возможностей артефакта путем наблюдения за работой образца в реальной или эмулированной среде (например, тестовая или виртуальная среда, эмуляторы программного или аппаратного обеспечения).

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: наблюдение за поведением цифрового артефакта в процессе исполнения позволяет получить дополнительную информацию о его работе, чтобы выявить изменения в системе затронутого хоста, взаимодействие других систем и обусловленный этим сетевой трафик, что позволяет лучше понять ущерб, нанесенный системе, и воздействие на нее, а также создать новую подпись (новые подписи) артефакта и определить способы смягчения последствий его использования.

Примечание. Анализ в ходе выполнения не позволяет увидеть полную функциональность артефакта, так как не все разделы его кода можно инициировать. Анализ в ходе выполнения позволяет аналитику увидеть не все возможности вредоносного программного средства, а лишь то, что оно делает в тестовой ситуации.

В рамках данной функции предполагается осуществление следующих подфункций:

- подготовка среды для анализа (реальной/ограниченной/закрытой, эмулированной/ симулированной);
- подготовка средств сбора данных, датчиков и/или образцов;
- сбор первоначальных данных о поведении и метаданных;
- тестирование артефакта несколько раз в разных условиях;
- анализ поведения систем и/или сетей в течение как краткого, так и длительного промежутка времени;
- формулирование выводов на основании оценки всех полученных результатов и данных, сравнение различных результатов и изучение имеющихся баз знаний в целях сопоставления имеющихся технических результатов с полученными данными.

6.3.4 Функция: сравнительный анализ

Цель: проведение анализа, направленного на выявление одинаковой функциональности или умысла, в том числе на основе анализа целого класса каталогизированных артефактов.

Описание: эта функция предполагает изучение связи артефакта с другими артефактами. Это может помочь выявить сходство кода или образа действия, объектов атаки, умысла 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: определены общие черты или взаимосвязь между артефактами, что позволяет выявить тенденции или сходство и таким образом лучше понять или получить дополнительную информацию о функциональности, воздействии и способах смягчения последствий использования цифровых артефактов.

В рамках данной функции предполагается осуществление следующих подфункций:

- определение исходных показателей для параметров и обнаруживаемых характеристик;
- поиск таких же или сходных параметров в имеющихся хранилищах/базах знаний;
- внесение в существующие хранилища/базы знаний вновь выявленных или ранее неизвестных признаков, вариантов поведения и/или подписей, которые могут быть использованы для дальнейшей классификации изучаемого артефакта.

6.4 Услуга: смягчение и преодоление последствий

Цель: максимальное сдерживание (локализация) инцидента в сфере информационной безопасности, чтобы сократить количество пострадавших, снизить потери и устранить причиненный ущерб, пресечь новые атаки и новые потери, устранив использованные уязвимости или слабые места, и повысить уровень кибербезопасности в целом.

Описание: после того как анализ подтвердит возможный инцидент в сфере информационной безопасности и будет разработана стратегия реагирования, на этой основе следует разработать план реагирования. Меры индивидуального характера могут приниматься даже до завершения работы над планом реагирования. Эта услуга предполагает также инициирование и отслеживание любых мер, которые принимаются до тех пор, пока инцидент в сфере информационной безопасности не будет считаться завершенным либо пока не будет получена новая информация, требующая дальнейшего анализа и способная в дальнейшем изменить содержание стратегии и плана реагирования.

Результат: последствия инцидента в сфере информационной безопасности смягчены и ситуация в сфере кибербезопасности улучшилась. Восстановлена целостность систем, пострадавших от направленных на нее атак или деятельности злоумышленника, равно как и работоспособность взломанных сети и систем. Утраченные данные по возможности восстановлены.

В рамках данной услуги предполагается осуществление следующих функций:

- разработка плана реагирования;
- меры индивидуального характера и локализация;
- восстановление систем;
- содействие другим структурам, занимающимся проблемами информационной безопасности.

Если CSIRT занимается вопросами координации, то она не может осуществлять все эти функции. Ее задачей является "содействие другим структурам, занимающимся проблемами информационной безопасности", однако иногда она может также помочь с "разработкой плана реагирования".

6.4.1 Функция: разработка плана реагирования

Цель: разработка и обеспечение реализации плана восстановления целостности затронутых систем и возвращения затронутых данных, систем и сетей в нормальное рабочее состояние с полным восстановлением функциональности затронутых услуг, но без воссоздания условий, при которых могла бы вновь возникнуть первоначальная проблема в области безопасности.

Описание: действенное реагирование невозможно, если не удастся полностью понять последствия для бизнеса и требования к смягчению последствий и восстановлению. Поскольку при этом имеет место конфликт интересов – отследить атаку, чтобы получить больше оперативной информации, или пресечь атаку, чтобы не допустить дальнейших потерь, – необходимо принять во внимание все интересы и разработать план реагирования, позволяющий учесть все известные факты и получить желаемые результаты в пределах требуемых временных рамок.

Как и в случае любых других планов, нельзя забывать о том, что при поступлении новых результатов анализа потребуется пересмотреть вновь сделанные выводы. В реальности для того чтобы план реагирования служил ориентиром и руководством на постоянной основе, как правило, в него требуется вносить изменения. Однако без такого плана – если только вопросами

реагирования не занимается одна небольшая организационная группа, практически не нуждающаяся во взаимодействии с внешними структурами или другими организациями, – отсутствие координации может привести к тому, что принимаемые меры будут неэффективными и недейственными.

Результат: подготовлен согласованный план реагирования, отвечающий потребностям бизнеса при наличии соответствующих ресурсов и поддержки, который впоследствии будет осуществлен. CSIRT осуществляет отслеживание и координацию в рамках услуги координации.

В рамках данной функции предполагается осуществление следующих подфункций:

- определение последствий инцидента в сфере информационной безопасности для бизнеса;
- определение требований со стороны бизнеса и временны́х рамок успешного восстановления;
- определение процедур и критериев принятия решений (если они ранее не были определены в рамках политики);
- определение объектов, подлежащих восстановлению, – среда, системы, приложения, комплексные функции и т. д.;
- определение необходимой поддержки и действий внутренних и внешних структур;
- разработка плана реагирования, обеспечивающего содержательное реагирование с учетом требований со стороны бизнеса и необходимых временных рамок на основании имеющихся ресурсов и технической сферы применения требуемых мер.

6.4.2 Функция: меры индивидуального характера и локализация

Цель: принятие мер, не позволяющих инциденту в сфере информационной безопасности распространиться, то есть ограничивающих его рамками уже затронутых систем, пользователей и/или доменов, чтобы не допустить дальнейших потерь (в том числе утечек документов, изменения баз данных или данных), и т. д.

Описание: в случае инцидента в сфере информационной безопасности первоочередной задачей является пресечение возможности его распространения. Пока не устранено несанкционированное проникновение в системы либо пока вредоносное программное средство функционирует в системах конечных пользователей, продолжается утрата данных и несанкционированный доступ. Обычно главной целью атак, в том числе атак (в частности с использованием техники бокового смещения) на другие организации как внутри, так и вне организации, затронутой инцидентом в сфере информационной безопасности, являются конкретные данные и системы. Чтобы остановить вредоносную деятельность или дальнейшие потери или по крайней мере ограничить их масштабы, необходимы краткосрочные меры, например блокирование или фильтрование трафика и закрытие доступа к тем или иным услугам или системам, что может также привести к отключению критически важных систем.

Пресечение дальнейшего доступа к данным, потенциально важным в качестве улик, даст возможность провести полный анализ таких улик. Пресечение дальнейшего доступа к другим

системам и сетям снизит также степень юридической ответственности за ущерб, причиненный другим организациям.

Пресечение нанесения непосредственного ущерба и снижение масштабов вредоносной деятельности путем принятия оперативных тактических мер (например, блокировки или фильтрации трафика) также может позволить восстановить контроль над системами. В течение всего времени, пока злоумышленники или вредоносное программное обеспечение имеют доступ к большому количеству систем или сетей, возвращение к нормальной операционной деятельности будет невозможно.

Результат: восстановлен контроль над затронутыми системами и сетями. Злоумышленники или вредоносное программное обеспечение не имеют доступа к данным, системам и сетям, что позволяет избежать новых атак и/или увеличения количества взломанных систем и данных.

В рамках данной функции предполагается осуществление следующих подфункций:

- временный отказ в доступе для пользователей/систем/услуг/сетей;
- временное отключение систем или сетей от сетей или магистральных сетей;
- временное отключение услуг;
- требование изменить пароли или секретные учетные данные пользователей;
- мониторинг признаков несанкционированного проникновения и получения несанкционированного доступа;
- проверка и подтверждение, что никакие пользователи/системы/услуги/сети не пострадали.

6.4.3 Функция: восстановление системы

Цель: внесение изменений в затронутой области, инфраструктуре или сети, необходимых для установления и предотвращения повторения такой деятельности в будущем.

Описание: восстановление целостности затронутых систем и возвращение затронутых данных, систем и сетей в нормальное рабочее состояние с полным восстановлением функциональности затронутых услуг. Поскольку интересы бизнеса, как правило, требуют как можно более быстрого возвращения систем в нормальное функциональное состояние, существует риск того, что не все средства получения несанкционированного доступа удастся успешно ликвидировать. Поэтому до получения результатов анализа даже восстановленные сети нуждаются в тщательном контроле и управлении. В случае если (пока) отсутствует возможность устранить выявленные уязвимости и слабые места, необходимо использовать усовершенствованные механизмы защиты и обнаружения, чтобы не допустить тех же самых, или сходных, или типичных инцидентов в области информационной безопасности.

Результат: принимаются меры для полного восстановления работоспособности, равно как и потенциала систем и услуг. Принимаются меры к ликвидации любых обнаруженных уязвимостей и слабых мест, способствовавших первоначальному инциденту в сфере информационной безопасности. Меры обнаружения и реагирования совершенствуются в соответствии с рекомендациями, изложенными в анализе и плане реагирования.

В рамках данной функции предполагается осуществление следующих подфункций:

- восстановление данных пользователей/системных данных с помощью проверенных резервных носителей;
- восстановление конфигураций с помощью проверенных резервных носителей или воссозданного контента;
- подключение отключенных услуг и восстановление доступа для пользователей/систем/сетей;
- проведение функциональных тестов для проверки возможности и потенциала систем/услуг/сетей на уровне как инфраструктуры, так и приложений.

6.4.4 Функция: содействие другим структурам, занимающимся проблемами информационной безопасности

Цель: предоставление клиентам возможности осуществлять управленческие и технические мероприятия, необходимые для эффективного смягчения и преодоления последствий инцидента в сфере информационной безопасности.

Описание: CSIRT может предоставлять непосредственную (на месте) помощь клиентам в восстановлении после ущерба и устранении уязвимостей. Это может представлять собой непосредственное расширение предлагаемых на месте аналитических услуг (см. выше). С другой стороны, CSIRT может сделать выбор в пользу оказания персоналу клиента помощи в реагировании на инцидент в сфере информационной безопасности в виде более подробных разъяснений, рекомендаций и т. д.

Результат: реакция со стороны клиентов стала более действенной, и преодоление последствий осуществляется быстрее. Благодаря наращиванию существующей базы знаний в дальнейшем появляется возможность повысить эффективность и результативность соответствующих мероприятий. Кроме того, это помогает оказывать поддержку тем структурам среди клиентуры, которые не имеют технической подготовки, достаточной для принятия необходимых мер реагирования.

6.5 Услуга: координация реагирования на инциденты в сфере информационной безопасности

Цель: обеспечение своевременного направления уведомлений и распространения достоверной информации; поддержка потока информации и отслеживание статуса мероприятий, проводимых структурами, которым поручено или предложено реагировать на инцидент в области информационной безопасности; а также обеспечение осуществления плана реагирования и своевременного учета изменений, происходящих вследствие как задержек, так и поступления новой информации.

Описание: всем заинтересованным сторонам и вовлеченным организациям крайне важно получать информацию и быть в курсе подробностей инцидента в области информационной безопасности и работы, ведущейся в его отношении. Поскольку для проведения мероприятий, необходимых для успешного смягчения и преодоления последствий, может понадобиться

разрешение руководства, необходимо заблаговременно наладить соответствующие системы предупреждения и оповещения, чтобы затем можно было эффективно и действенно реагировать на любой инцидент в области информационной безопасности. По мере того как CSIRT анализирует всю поступающую информацию, координация позволяет доводить уведомления и информацию до сведения соответствующих контактных лиц, отслеживать их реакцию и добиваться, чтобы все стороны, участвующие в этой работе, предоставляли отчеты, позволяющие получать четкое представление о ситуации до тех пор, пока инцидент в области информационной безопасности не будет признан исчерпанным и не требующим дальнейшей координации.

Заинтересованные стороны должны иметь возможность задавать вопросы, проверять статус инцидентов в области информационной безопасности и сообщать CSIRT о проблемах. Для взаимодействия с внутренними заинтересованными сторонами CSIRT следует создавать каналы связи, по которым будет передаваться информация о ситуации с ликвидацией инцидентов в области информационной безопасности. Для взаимодействия с внешними заинтересованными сторонами CSIRT необходимо использовать каналы связи с другими CSIRT и сообществами CSIRT, способными дать рекомендации или оказать техническую поддержку.

Результат: обеспечена успешная координация мер реагирования путем эффективного информирования структур, участвующих в реагировании на инцидент в области информационной безопасности.

В рамках данной услуги предполагается осуществление следующих функций:

- связь;
- рассылка уведомлений;
- рассылка актуальной информации;
- координация деятельности;
- представление отчетов;
- связь со средствами массовой информации.

6.5.1 Функция: связь

Цель: эффективное взаимодействие с заинтересованными сторонами и создание соответствующих разнообразных каналов связи, обеспечивающих необходимый уровень конфиденциальности.

Описание: при подготовке и обнародовании информационных сообщений CSIRT следует ориентироваться на наиболее заинтересованную целевую аудиторию. Соответственно CSIRT также необходимо быть готовой к поддержанию обратной связи и поступлению отчетов, комментариев и вопросов, направляемых из самых разных источников в связи с распространяемой группой информацией.

Политикой обеспечения безопасности и политикой обмена информацией могут устанавливаться жесткие рамки для работы с информацией. CSIRT должна иметь возможность обмениваться

информацией с заинтересованными сторонами – как внешними, так и внутренними – надежно, безопасно и с сохранением конфиденциальности.

Необходимо как можно более заблаговременно заключить соглашения о неразглашении и соответствующим образом настроить системы коммуникации. Кроме того, можно использовать понятие "информация на условиях неразглашения". В связи с этим необходимо также определить политику хранения данных, которая обеспечивала бы должную обработку данных, используемых для представления информации, и самой этой информации, обмен ими и их хранение при определенных ограничениях – например, временны́х – до тех пор, пока эти ограничения не будут сняты и информация не будет обнародована.

С учетом потребностей заинтересованных сторон и клиентов могут применяться разные каналы связи. Вся передаваемая информация должна маркироваться в соответствии с требованиями политики обмена информацией. Возможно применение протокола маркировки информации (TLP).

Результат: действуют все каналы связи, соответствующие требованиям безопасности всех сторон – получателей и отправителей информации.

В рамках данной функции предполагается осуществление следующих подфункций:

- создание внутренних каналов связи;
- создание внешних каналов связи.

6.5.2 Функция: рассылка уведомлений

Цель: уведомление структур, затронутых инцидентом в области информационной безопасности или имеющих возможность оказать содействие в реагировании на него, и предоставление этим структурам информации, необходимой для того, чтобы определить степень их участия, а также то, в какой мере можно рассчитывать на сотрудничество с ними и поддержку с их стороны.

Описание: инцидент в области информационной безопасности затрагивает многие внутренние, а возможно, и внешние структуры, а иногда системы и сети. Поскольку CSIRT являются основными точками приема сообщений о возможных инцидентах в области информационной безопасности, они выступают также в качестве центров уведомления о них уполномоченных контактных лиц. В уведомлении, как правило, приводятся не только необходимые сведения технического характера, но и информация об ожидаемой реакции, а также контактные данные для дальнейшей связи.

Результат: информация об инциденте в области информационной безопасности доведена до сведения структур, которые обязаны участвовать в реагировании на него или должны быть уведомлены о нем.

6.5.3 Функция: рассылка актуальной информации

Цель: поддержание контактов с выявленными структурами и предоставление им соответствующей имеющейся информации, для того чтобы дать возможность этим структурам

воспользоваться имеющимися данными и накопленным опытом, применять более эффективные методы реагирования или принимать новые меры индивидуального характера.

Описание: в процессе реагирования на инцидент в области информационной безопасности появляется все больше результатов анализов и отчетов, в том числе от других специалистов по безопасности, CSIRT или пострадавших.

Целесообразной может быть передача некоторой доли информации и накопленного опыта в сферу обслуживания передачи знаний (если она поддерживается), чтобы повысить качество учебной и технической документации, а также помочь в обеспечении необходимого уровня осведомленности, особенно в случае выявления новых тенденций в области атак и инцидентов.

Результат: имеющаяся информация предоставляется тем, кто должен либо участвовать в реагировании, либо быть в курсе хода работы и текущего положения дел.

6.5.4 Функция: координация деятельности

Цель: отслеживание статуса всех видов информационного взаимодействия и всех мероприятий.

Описание: поскольку потенциально реагированием на инцидент в области информационной безопасности может заниматься много структур, необходимо отслеживать статус всех видов информационного взаимодействия и всех мероприятий. К их числу относятся меры, принимаемые по предписанию CSIRT, или запросы на дальнейший обмен информацией, равно как и запросы на проведение технического анализа артефактов и обмен признаками несанкционированного доступа, информацией о других пострадавших и т. п. Такие действия, как правило, имеют место тогда, когда в целях осуществления действий, необходимых для смягчения последствий инцидента, CSIRT полагается на специальные знания и опыт, а также силы и средства, не находящиеся под ее непосредственным контролем. Однако подобное происходит и в более крупных организациях, где координацией мероприятий по смягчению и преодолению последствий занимается внутренняя CSIRT.

Предлагая услуги двусторонней или многосторонней координации, CSIRT участвует в обмене информацией, чтобы в рамках этих сил и средств предпринять соответствующие действия или помочь другим лицам выявить, предупредить или устранить существующую враждебную деятельность и помочь в прекращении инцидента в области информационной безопасности.

Результат: обеспечено информирование о текущем статусе всех мероприятий и статусе структур, участвующих в реагировании.

6.5.5 Функция: представление отчетов

Цель: обеспечение того, чтобы все вовлеченные подразделения компании были проинформированы о статусе текущих мероприятий, с тем чтобы решения относительно дальнейших шагов можно было принимать, по возможности, на основании наиболее полного понимания ситуации.

Описание: предоставление в сжатом виде фактической информации о статусе текущих мероприятий, которые требуется проводить или которые проводятся в рамках реагирования на

инцидент в области информационной безопасности. Для обеспечения действенной координации крайне необходимо предоставлять такую информацию своевременно, не дожидаясь запросов на нее, в контексте постоянной координации деятельности, требующейся для любого успешного реагирования.

Результат: внутренние заинтересованные стороны находятся в курсе всей текущей деятельности, уже проведенных и пока не завершенных мероприятий. Они получают также оценки предполагаемых последствий задержек, рекомендации и сведения о необходимых действиях, что позволяет понять общую эффективность выбранной стратегии реагирования и разработанного плана действий.

6.5.6 Функция: связь со средствами массовой информации

Цель: налаживание взаимодействия со средствами массовой информации (публичными), чтобы иметь возможность предоставлять достоверную и понятную фактическую информацию о происходящем, пресекая тем самым распространение слухов и недостоверных сведений.

Описание: очень часто контакты со средствами массовой информации не поддерживаются. Хотя CSIRT обычно пытаются избегать таких контактов, важно понимать, что средства массовой информации могут содействовать в подавлении некоторых видов систематических и широкомасштабных атак, приводящих к инцидентам в области информационной безопасности. Соответственно необходимо разъяснять, что является причиной инцидентов в области информационной безопасности, а также их последствия для пользователей и/или организаций. Иногда CSIRT может предпочесть предоставлять такую информацию в формате, уже готовом для публикации, однако это определенно требует специальных навыков, которыми не обладают большинство сотрудников CSIRT. В любом случае, если CSIRT поддерживает контакты со средствами массовой информации, ей следует позаботиться о том, чтобы максимально упростить технические детали и опустить всю конфиденциальную информацию.

Результат: подготовлена фактическая информация, дающая четкое общее представление о происходящем инциденте в области информационной безопасности, в том числе о мерах, которые должны принять потенциальные пострадавшие, или об избранной стратегии реагирования, направленной на преодоление последствий инцидента в области информационной безопасности.

6.6 Услуга: поддержка управления в кризисных ситуациях

Цель: обмен опытом и контактной информацией с другими специалистами по безопасности, CSIRT и сообществами CSIRT в целях смягчения последствий кризиса.

Описание: хотя в наши дни инциденты в области информационной безопасности лишь в редких случаях перерастают в кризис в масштабах организации или страны, такая возможность существует. Однако реагирование на кризис, как правило, ассоциируется с чрезвычайной ситуацией, угрожающей благополучию людей и общества в целом или, по крайней мере, существованию организации. Как принято в рамках управления в кризисных ситуациях, ответственность за реагирование на кризис принимает на себя высшее должностное лицо,

в результате чего в условиях чрезвычайной ситуации обычный порядок подчиненности изменяется.

Поскольку системы и сети могут стать одним из источников возникновения чрезвычайной ситуации или должны быть пригодны для реагирования на кризис, CSIRT, как правило, является важным ресурсом для управления такими ситуациями и может предоставлять не только ценный опыт, но и доступ к существующим услугам и сетям контактных лиц.

Результат: группа по управлению в кризисных ситуациях может использовать ресурсы CSIRT для решения проблем кибербезопасности в рамках текущего кризиса. При этом коммуникационные ресурсы CSIRT могут использоваться для того, чтобы обратиться к клиентам и внешним сторонам с просьбой о принятии конкретных мер содействия или о поддержке. Возможности группы можно использовать и для поддержания надежных связей с клиентами по ранее налаженным каналам и надежным сетям.

В рамках данной услуги предполагается осуществление следующих функций:

- информирование клиентов;
- представление отчетов о статусе информационной безопасности;
- информирование о решениях стратегического характера.

6.6.1 Функция: информирование клиентов

Цель: предоставление существующих коммуникационных ресурсов для помощи в реагировании на кризис.

Описание: в процессе реагирования на кризис необходимо рассылать и распространять информацию. Поскольку CSIRT создала соответствующие ресурсы для собственных целей, органы управления в кризисной ситуации, возможно, сочтут использование таких ресурсов целесообразным или необходимым.

Результат: клиенты получают имеющуюся информацию, а прочные доверительные отношения помогают убедить ее получателей в достоверности распространяемых данных.

6.6.2 Функция: представление отчетов о статусе информационной безопасности

Цель: обеспечение того, чтобы в распоряжении группы по управлению в кризисных ситуациях был полный обзор текущих инцидентов в области информационной безопасности и известных уязвимостей, воспринимаемых этой группой в качестве составной части своих общих приоритетов и стратегий.

Описание: данная функция предполагает предоставление в сжатом виде фактической информации о текущей ситуации в сфере кибербезопасности в клиентской структуре. Поскольку кризис может использоваться для инициирования новых атак либо происходящие в настоящее время атаки могут быть составной частью действий общего характера, определяющих этот кризис, группе по управлению в кризисных ситуациях очень важно располагать всей информацией о ситуации.

CSIRT может обеспечить такую информированность своих услуг и клиентов о ситуации. Это может происходить по запросу или предусматриваться стандартными механизмами действий в условиях кризиса. В любом случае предоставляемые отчеты должны быть своевременными и достоверными, поскольку регулирование кризиса, которое зависит от координации ресурсов для реагирования на наиболее существенные аспекты кризиса, может быть успешным лишь тогда, когда оно базируется на постоянном притоке информации.

Учитывая, что для реагирования на текущие инциденты в области информационной безопасности нужны ресурсы, необходимо принять решение либо о приостановке реагирования до тех пор, пока инцидент не завершится (и перераспределении имеющихся на данный момент ресурсов в другие сферы), либо о продолжении действий. Разумные решения могут быть приняты лишь там, где обеспечен максимально возможный уровень осведомленности о ситуации.

Результат: группа по управлению в кризисных ситуациях находится в курсе всей текущей деятельности, уже проведенных и пока еще не завершенных мероприятий. Она получает также оценки предполагаемых последствий задержек, рекомендации и сведения о необходимых действиях, что позволяет понять общую эффективность выбранной стратегии реагирования на происходящий кризис.

6.6.3 Функция: информирование о решениях стратегического характера

Цель: своевременное информирование других структур о последствиях кризиса для неурегулированных инцидентов в сфере информационной безопасности.

Описание: своевременное информирование других структур о последствиях кризиса для неурегулированных инцидентов в сфере информационной безопасности дает четкое представление о том, какого рода помощь CSIRT может оказать в течение кризиса, и помогает убедиться в том, что эти структуры понимают, чего следует ожидать. Это также гарантирует, что другие стороны прекратят поддержку CSIRT или взаимодействие с ней, если они сочтут, что масштаб кризиса возрастает.

Поскольку группа по управлению в кризисных ситуациях может принять решение о том, чтобы ввиду кризиса отложить реагирование на текущий инцидент в области информационной безопасности, такого рода решения необходимо доводить до сведения всех структур, получающих информацию и участвующих в этой деятельности. Это необходимо для того, чтобы избежать неправильных толкований и возникновения новых проблем, которые могут также повлечь за собой снижение доверия к CSIRT и/или организации, в рамках которой она работает.

Результат: информация о последствиях кризиса для деятельности CSIRT направляется клиентам и другим структурам, участвующим в реагировании на текущие инциденты в области информационной безопасности. Четко формулируются ожидания CSIRT от таких структур, что обеспечивает четкую передачу им потребностей CSIRT в информации.

7 Сфера обслуживания: управление уязвимостями

К сфере обслуживания по управлению уязвимостями относятся услуги, связанные с обнаружением, анализом и обработкой новых или ставших известными уязвимостей в информационных системах. К сфере обслуживания по управлению уязвимостями относятся также услуги по выявлению известных уязвимостей и реагированию на них, чтобы не допустить их использования. Соответственно эта сфера обслуживания включает услуги, связанные как с новыми, так и с уже известными уязвимостями.

Хотя иногда термин "управление уязвимостями" используется применительно к процессу, призванному предупредить возможность использования уже известных уязвимостей (например, "найди и исправь"), в настоящей концепции предоставления услуг CSIRT такие направления деятельности считаются функциями и подфункциями услуги реагирования на факторы уязвимости – одной из тех услуг, которые может предоставлять CSIRT. Для многих CSIRT такие функции реагирования на факторы уязвимости относятся к сфере ведения других структур, которые имеют возможность обнаруживать и устранять уязвимости систем безопасности.

В рамках данной сферы обслуживания предполагается осуществление следующих услуг:

- выявление/изучение уязвимостей;
- получение отчетов об уязвимостях;
- анализ уязвимостей;
- координация обмена информацией об уязвимостях;
- раскрытие информации об уязвимостях;
- реагирование на факторы уязвимости.

Многие CSIRT предоставляют не все эти услуги, а лишь те из них, которые входят в их сферу ответственности. Например, CSIRT может ограничиться такими услугами, как изучение новых факторов уязвимости, информация о которых есть в общедоступных источниках (выявление/изучение уязвимостей) или может быть получена от третьих сторон (получение отчетов об уязвимостях), а затем в случае необходимости выпустить бюллетень безопасности для своих клиентов (раскрытие информации об уязвимостях), не пытаясь при этом координировать усилия с поставщиками продукта или иными субъектами, ведущими поиск решений (координация обмена информацией об уязвимостях) или непосредственно участвовать в устранении уязвимости (реагирование на факторы уязвимости).

7.1 Услуга: выявление/изучение уязвимостей

Цель: обнаружение, изучение или поиск новых (ранее неизвестных) уязвимостей; уязвимости могут быть обнаружены теми, кто работает в сфере обслуживания по управлению уязвимостями, или в ходе других мероприятий, связанных с деятельностью CSIRT.

Описание: обнаружение новой уязвимости – это необходимый первый шаг, с которого начинается общий цикл управления уязвимостями. Эта услуга предполагает такие функции и мероприятия, которые CSIRT может активно осуществлять в рамках собственных изысканий или в рамках других услуг, направленных на обнаружение новой уязвимости. Функции и мероприятия, связанные с пассивным получением от кого-либо информации о новой уязвимости, будут описаны ниже в рамках услуги получения отчетов об уязвимостях. Иногда

CSIRT может обнаружить новую уязвимость в ходе другой деятельности, например анализа или изучения отчета об инциденте. К числу других возможностей получить сведения о новой уязвимости относятся использование общедоступных источников (например, веб-сайтов, списков рассылки[6]), других внешних источников (например, премиальных услуг, подписок) или же целенаправленные исследования, посвященные поиску уязвимостей (например, посредством нечеткого тестирования, обратного инжиниринга). Такие вновь полученные сведения, независимо от того, каким образом CSIRT обнаружила уязвимость или узнала о ней, необходимо оформлять документально и передавать организации для использования в процессе обработки уязвимостей.

Результат: эта услуга позволяет увеличить количество обнаруженных потенциальных уязвимостей, о которых непосредственно не сообщалось CSIRT.

В рамках данной услуги предполагается осуществление следующих функций:

- обнаружение уязвимости в ходе реагирования на инцидент;
- обнаружение информации об уязвимости в общедоступном источнике;
- исследование уязвимостей.

Эти функции могут относиться к услугам (или функциям), осуществляемым не CSIRT, а другими субъектами (например, исследователями, поставщиками, PSIRT или сторонними специалистами).

7.1.1 Функция: обнаружение уязвимости в ходе реагирования на инцидент

Цель: выявление уязвимости, которая была использована в рамках инцидента в области безопасности.

Описание: в ходе анализа инцидента в области безопасности возможно выявление информации, которая показывает, что уязвимость была использована злоумышленником. Инцидент мог быть обусловлен использованием известной уязвимости, которая ранее не была исправлена или уменьшена, или новой уязвимости (уязвимости нулевого дня).

Определенная часть такой информации об уязвимости может быть получена как результат осуществления одной из услуг в рамках сферы обслуживания по управлению инцидентами в сфере информационной безопасности, если уязвимость была использована в ходе инцидента. Эта информация может быть затем передана, в зависимости от целесообразности, в функцию сортировки уязвимостей или в службу анализа уязвимостей.

Результат: информация об уязвимости, которая, как предполагается, могла быть использована рамках инцидента в области безопасности, передана в сферу обслуживания по управлению уязвимостями.

[6] Получение новой информации об уязвимостях по электронной почте может рассматриваться – в зависимости от внутренних процедур, принятых в CSIRT, или степени распространения информации об уязвимости – как деятельность в рамках услуги выявления уязвимостей, функции обнаружения информации об уязвимости в общедоступном источнике, услуги получения отчетов об уязвимостях либо функции по приему отчета об уязвимости.

7.1.2 Функция: обнаружение информации об уязвимости в общедоступном источнике

Цель: получение информации о новой уязвимости из общедоступного источника или от третьего лица.

Описание: CSIRT может получать первоначальную информацию о новой уязвимости из различных источников, в которых сообщается об этой уязвимости. К числу источников могут относиться сообщения поставщиков, веб-сайты по проблемам безопасности, списки рассылки, базы данных об уязвимостях, конференции по проблемам безопасности, социальные сети и т. д. В рамках этой функции сведения о новых уязвимостях можно получать и из сторонних источников, которые, возможно, не являются полностью общедоступными, к числу которых относятся, например, платные подписки или премиальные услуги, предусматривающие распространение информации только среди ограниченной группы участников. Сотрудникам может быть поручено осуществление этой функции и сбор информации, с тем чтобы подготовить ее для последующего изучения и распространения. Аналогичную информацию об уязвимости можно получать и в рамках услуг сферы обслуживания осведомленности о ситуации.

Результат: выявлены новые уязвимости, информация о которых распространяется посредством общедоступных или иных внешних источников.

7.1.3 Функция: исследование уязвимостей

Цель: выявление новых уязвимостей или их поиск посредством целенаправленной деятельности или проведения исследований.

Описание: эта функция предполагает выявление новых уязвимостей путем проведения таких входящих в круг ведения CSIRT мероприятий, как тестирование систем или программного обеспечения с применением нечеткого тестирования (фаззинга) или обратного инжиниринга вредоносного программного обеспечения.

При осуществлении этой функции могут также использоваться материалы, полученные от услуги (услуг) в рамках сферы обслуживания управления инцидентами в сфере информационной безопасности или сферы обслуживания осведомленности о ситуации, которые инициируют применение данной функции для поиска предполагаемых уязвимостей.

Выявление новой уязвимости в ходе осуществления функции исследования уязвимостей может предоставить исходные данные для услуги по реагированию на инцидент, функции обнаружения уязвимостей (см. подфункции сканирование уязвимостей и тестирование на возможность проникновения).

Результат: в ходе исследований обнаружены новые уязвимости.

7.2 Услуга: получение отчетов об уязвимостях

Цель: получение и обработка информации об уязвимостях, переданной клиентами или третьими сторонами.

Описание: одним из основных источников информации об уязвимости могут послужить отчеты или вопросы, направленные клиентами CSIRT или иными третьими сторонами. CSIRT следует иметь в виду, что отчеты об уязвимостях могут поступать из разных источников, и разработать

механизм, процедуру и рекомендации по представлению отчетов об уязвимостях. К числу средств представления отчетов может относиться и форма для представления отчета об уязвимости на базе электронной почты или веб-сайта. Не все отчеты об уязвимостях от клиентов или третьих сторон представляются непосредственно CSIRT по установленным каналам.
В соответствующих рекомендациях необходимо привести указания по представлению отчетов, контактную информацию и сведения о порядке раскрытия информации.

Чтобы дать клиентам возможность более эффективно сообщать об уязвимостях, CSIRT необходимо создать один или несколько механизмов, а также разработать рекомендации или инструкции о порядке безопасного представления отчетов об уязвимостях. Для представления отчетов об уязвимостях можно использовать электронную почту, веб-сайт, специальную форму или портал для сообщения об уязвимости либо иные соответствующие каналы, позволяющие передавать отчеты защищенно и безопасно. Инструкции в отношении отчетов, если они не включены в сам бланк отчета об уязвимости, должны представляться в формате отдельного документа или размещаться на веб-странице и содержать перечень той информации, которую рекомендуется включать в отчет.

Результат: поступление отчетов об уязвимостях осуществляется на профессиональной и упорядоченной основе; производится также их первоначальная оценка и классификация.

В рамках данной услуги предполагается осуществление следующих функций:

- прием отчета об уязвимости;
- сортировка и обработка отчета об уязвимости.

7.2.1 Функция: прием отчета об уязвимости

Цель: получение или прием информации об уязвимости, представляемой клиентами или третьими сторонами.

Описание: чтобы прием отчетов об уязвимости был организован эффективно, необходимы механизмы и процедуры получения отчетов от клиентов, заинтересованных сторон и третьих лиц (лиц, обнаруживающих уязвимости, исследователей, поставщиков, PSIRT, других CSIRT или координаторов по проблемам уязвимостей и т. д.). Информация об уязвимости может касаться затронутых устройств, условий, необходимых для использования уязвимости, последствий (например, повышения привилегий, доступа к данным и т. д.), а также мер, принятых для решения, устранения и/или смягчения и закрытия проблемы уязвимости. Иногда прием информации об уязвимости может проводиться совместно с другой услугой, в первую очередь приемом отчетов об инцидентах в сфере информационной безопасности (например, если сведения об использовании уязвимости приводятся в отчете об инциденте).

Результат: обеспечивается должная обработка отчетов об уязвимостях, поступающих от клиентов или третьих лиц, включая инициирование их документального оформления или проверки.

В рамках данной функции предполагается осуществление следующих подфункций:

- регулярный мониторинг каналов связи и проверка работоспособности заявленных средств связи с CSIRT и возможности направлять по ним отчеты;

- направление лицу, представляющему отчет об уязвимости, первоначального подтверждения получения отчета, запрос дополнительной информации в случае необходимости и совместное определение желаемых результатов.

7.2.2 Функция: сортировка и обработка отчета об уязвимости

Цель: первоначальное изучение, классификация, приоритизация и обработка отчета об уязвимости.

Описание: отчеты об уязвимостях изучаются и сортируются в целях получения первоначального представления о соответствующей уязвимости и определения дальнейших действий (например, обработки данных об уязвимости для последующего анализа, запроса дополнительной информации у лица, представившего отчет, или в других источниках, принятия решения о том, что уязвимость не требует дальнейших действий). Степень подробности и качество информации, представленной в отчете об уязвимости, могут позволить или не позволить понять, действительно ли новая уязвимость существует.

В случае если нет оснований отклонять отчет об уязвимости, его следует передать в службу анализа уязвимостей для дальнейшего изучения, анализа и обработки. Если CSIRT не предоставляет услуг по анализу уязвимостей, то отчет следует безопасным образом передать для принятия дальнейших мер внешней группе, например затронутому поставщику (поставщикам), PSIRT или координатору по проблемам уязвимости.

Результат: выявлена информация, позволяющая определить порядок дальнейших действий.

В рамках данной услуги предполагается осуществление следующих подфункций:

- обработка отчетов и представленных данных, включая отдельные артефакты или материалы, для защиты целостности рабочей среды и недопущения применения подобных средств для успешных атак на CSIRT;
- повторное выражение признательности за отчет путем предоставления определенной информации о дальнейших мерах по итогам классификации и приоритизации;
- добавление новой информации об уже рассмотренной уязвимости к ранее полученным данным, чтобы обеспечить последовательный анализ и обработку.

7.3 Услуга: анализ уязвимостей

Цель: анализ подтвержденной уязвимости и получение представления о ней.

Описание: услуга анализа уязвимостей предусматривает осуществление функций, имеющих целью получение представления об уязвимости и ее возможных последствиях, выявление лежащих в ее основе проблемы или дефекта (основная причина), обеспечивающих возможность использования уязвимости, а также определение одной или нескольких стратегий устранения или смягчения, которые позволили бы пресечь или свести к минимуму использование уязвимости.

Работа по услуге анализа уязвимостей и ее функциям может продолжаться в параллельном режиме, тогда как работа по услуге координации обмена информацией об уязвимостях и ее

функциям ведется совместно с другими участниками в рамках скоординированного процесса раскрытия информации об уязвимости[7] (CVD).

Результат: углубление знаний о ключевых элементах уязвимости (например, ее описание, последствия, пути устранения).

В рамках данной услуги предполагается осуществление следующих функций:

- сортировка уязвимостей (подтверждение и классификация);
- анализ основных причин уязвимости;
- разработка методов устранения уязвимости.

7.3.1 Функция: сортировка уязвимостей (подтверждение и классификация)

Цель: классификация, приоритизация и первоначальная оценка уязвимости.

Описание: осуществление услуги по анализу уязвимостей начинается с обзора имеющейся информации, чтобы провести классификацию и приоритизацию этой уязвимости и оценить ее последствия для затронутых систем, относящихся к сфере ведения CSIRT. Если сведения об уязвимости были переданы в CSIRT клиентом или третьей стороной, некоторая часть этой работы может быть проведена в рамках осуществления функции сортировки и обработки отчета об уязвимости, связанной с услугой получения отчетов об уязвимостях.

Если предварительная сортировка еще не завершена, данные об уязвимости могут быть переданы соответствующему эксперту, который может предоставить техническое подтверждение того, что уязвимость имела определенные последствия для затронутых систем и что она относится к сфере ведения CSIRT (то есть может оказать воздействие на безопасность сетей или систем, что может повлечь за собой нарушение конфиденциальности, доступности или целостности информационных активов, которые, в соответствии с мандатом CSIRT, относятся к сфере ее ведения).

Результат: проведены классификация, приоритизация и обновление данных об уязвимости.

7.3.2 Функция: анализ основных причин уязвимости

Цель: получение представления о том, какой дефект разработки или реализации стал причиной возникновения уязвимости или создал возможность для ее появления.

Описание: цель анализа состоит в выявлении основной причины уязвимости путем определения обстоятельств, в которых уязвимость может существовать, а злоумышленник, соответственно, может ее использовать. В ходе этого анализа можно также попытаться понять, какие слабые места были использованы для того, чтобы инспирировать инцидент, и какие вредоносные навыки были применены для использования такого слабого места. Иногда, с учетом характера уязвимости, CSIRT может столкнуться с проблемами в попытке должным образом осуществить эту функцию. В некоторых случаях может оказаться, что такую функцию уже осуществило лицо,

[7] Соответствующую информацию о скоординированном процессе раскрытия информации об уязвимости (CVD) см. в разделах по сферам обслуживания координация обмена информацией об уязвимостях и информирование об уязвимостях.

обнаружившее уязвимость или сообщившее о ней. Во многих ситуациях наилучшим образом осуществить такую функцию может поставщик продукта или разработчик затронутого программного обеспечения или системы либо их соответствующая PSIRT. Может также оказаться, что уязвимость присутствует более чем в одном продукте, и в этом случае может понадобиться анализ нескольких затронутых компьютерных программ или систем, требующий координации усилий с разными поставщиками, PSIRT или заинтересованными сторонами.

Результат: полученное представление об уязвимости и о способах, которыми злоумышленник может ее использовать, применяется для определения методов преодоления или смягчения последствий, чтобы свести к минимуму риск стать объектом атаки или злонамеренного использования в будущем.

7.3.3 Функция: разработка методов устранения уязвимости

Цель: разработка мер, необходимых для исправления (устранения) соответствующей уязвимости или ограничения (сокращения) возможностей использовать последствия уязвимости.

Описание: в идеале задача этой функции – найти способы устранения или исправления уязвимости. Если поставщик не может своевременно предоставить средства для исправления или устранения неполадок, можно рекомендовать применение временной меры или обходного решения – так называемого смягчения, которое заключается в прекращении работы затронутого программного обеспечения или внесении изменений в конфигурацию, чтобы свести к минимуму потенциальное негативное воздействие уязвимости. Следует отметить, что на деле применение или использование методов устранения (исправления) или смягчения (обходное решение) относится к функциям отдельной услуги – в этой концепции она названа реагирование на факторы уязвимости.

Будучи составной частью услуги анализа уязвимостей, функция разработки методов устранения может предусматривать другие подфункции или мероприятия, например оценку возможностей изменения процедуры или архитектуры, изучение мер по смягчению силами третьей стороны или выявление новых уязвимостей, появляющихся на этапе устранения. Уязвимости, которые невозможно устранить или смягчить, следует документально оформлять как приемлемые риски.

В рамках этой функции информация или материалы нередко поступают от поставщика (поставщиков) затронутого продукта, иногда как часть первоначального отчета или сообщения, обработка которых проходила в рамках других услуг или функций.

Результат: разработан план внесения изменений (исправлений) в код программного обеспечения, применения обходного решения или совершенствования процедур, инфраструктуры и/или архитектуры, чтобы перекрыть то или иное направление атаки и не допустить использования уязвимости.

В рамках данной функции предполагается осуществление следующих подфункций:

- разработка мер устранения/исправления уязвимости;
- разработка мер смягчения уязвимости.

Как правило, эту функцию осуществляют другие структуры (например, поставщики продукта или PSIRT).

7.4 Услуга: координация обмена информацией об уязвимостях

Цель: обмен информацией и координация работы с участниками скоординированного процесса раскрытия информации об уязвимости (CVD).

Описание: работа с большинством уязвимостей предполагает уведомление различных сторон, которые могут совместными усилиями проводить анализ уязвимостей и исправлять их, в том числе лиц, обнаруживающих уязвимости/представляющих отчеты о них, затронутых поставщиков, разработчиков, PSRIT или других авторитетных специалистов (например, исследователей, CSIRT, координаторов, занимающихся проблемами уязвимости), а также сотрудничество с ними и координацию обмена соответствующей информацией.

Результат: налажен действенный и своевременный обмен информацией с участниками процедуры CVD, которые могут помочь с предоставлением информации, необходимой для устранения/смягчения уязвимости.

В рамках данной услуги предполагается осуществление следующих функций:

- уведомление/представление отчетов об уязвимостях;
- координация действий заинтересованных сторон, занимающихся проблемами уязвимости.

7.4.1 Функция: уведомление/представление отчетов об уязвимостях

Цель: инициация обмена информацией о вновь выявленной уязвимости с другими участниками процедуры CVD или предоставление им такой информации.

Описание: работа с большинством уязвимостей предполагает уведомление различных сторон, которые могут совместными усилиями проводить анализ уязвимостей и исправлять их, в том числе затронутых поставщиков, разработчиков, PSRIT или других авторитетных специалистов (например, исследователей, CSIRT, координаторов, занимающихся проблемами уязвимости), а также сотрудничество с ними и координацию обмена соответствующей информацией.

Результат: поставщики (или другие участники процедуры CVD) получают информацию об уязвимости и имеют возможность разрабатывать способы ее устранения или смягчения.

7.4.2 Функция: координация действий заинтересованных сторон, занимающихся проблемами уязвимости

Цель: координация работы различных заинтересованных сторон и участников скоординированного процесса раскрытия информации об уязвимости (CVD) и обмен информацией между ними по итогам их работы.

Описание: координировать обмен информацией между лицами, обнаруживающими уязвимости/представляющими отчеты о них, поставщиками, PSRIT и другими участниками скоординированного процесса раскрытия информации об уязвимости (CVD), содействуя тем самым проведению анализа и исправлению уязвимости, а также подготовке к раскрытию информации о ней. В рамках этой координации необходимо также прийти к договоренностям между участниками по вопросам о сроках и синхронизации раскрытия информации.

Результат: налажен более эффективный, оперативный и ответственный обмен информацией об уязвимости между участниками, которые имеют возможность разрабатывать способ устранения/смягчения уязвимости или информировать о нем.

В рамках данной функции предполагается осуществление следующей подфункции:

- подготовка публикации об уязвимости.

7.5 Услуга: раскрытие информации об уязвимостях

Цель: доведение информации об известных уязвимостях до сведения клиентов, чтобы они могли на основании этой информации принять меры к предупреждению, обнаружению, а также устранению/смягчению известных уязвимостей.

Описание: информирование клиентов об известных уязвимостях (потенциальных точках входа для нарушителей) с целью обеспечить обновление и мониторинг их систем на наличие эксплойтов. К числу методов раскрытия информации могут относиться обнародование информации различными путями (например, на веб-сайтах, по электронной почте, в социальных сетях), создание базы данных об уязвимостях или иные способы. Часто, хотя и не всегда, эта услуга предоставляется после услуги по координации обмена информацией об уязвимостях.

Результат: располагая информацией, клиенты могут избежать возможного использования ранее известных уязвимостей, а также обнаруживать и смягчать существующие уязвимости.

В рамках данной услуги предполагается осуществление следующих функций:

- разработка политики раскрытия информации об уязвимостях и обслуживание инфраструктуры;
- оповещение/передача данных/распространение информации об уязвимостях;
- обратная связь по итогам раскрытия информации об уязвимостях.

7.5.1 Функция: разработка политики раскрытия информации об уязвимостях и обслуживание инфраструктуры

Цель: разработка и осуществление политики, определяющей порядок обработки уязвимостей и информирования о них группами CSIRT, требования к этой работе, а также механизм (механизмы), применяемые для раскрытия информации об уязвимостях.

Описание: CSIRT, работающие с отчетами об уязвимостях, обязаны определить политику раскрытия информации об уязвимостях и ознакомить с ней своих клиентов, заинтересованные стороны и участников процедуры CVD, желательно путем ее размещения на веб-сайте CSIRT. Политика раскрытия информации об уязвимостях обеспечит прозрачность для заинтересованных сторон и поможет в разработке соответствующих стратегий раскрытия информации. Такая политика может предусматривать различные варианты: отказ от раскрытия, когда информация об уязвимостях не разглашается; ограниченное раскрытие, когда разглашается лишь часть информации; и полное раскрытие, когда раскрывается вся информация, в том числе, возможно, исследование для подтверждения механизма действия эксплойта. Политика раскрытия информации должна включать в себя такие компоненты, как сфера применения политики, ссылки на механизмы представления отчетов и рекомендации по

этому вопросу, а также предполагаемые временны́е рамки и механизмы информирования об уязвимостях.

Результат: повышение уровня доверия, углубление сотрудничества и ужесточение контроля за раскрытием информации, а также укрепление связей и усиление координации с участниками процедуры CVD.

7.5.2 Функция: оповещение/передача данных/распространение информации об уязвимостях

Цель: информирование клиентов (или общественности) о новой уязвимости, чтобы дать им возможность обнаруживать, устранять или смягчать уязвимость, а также не допустить ее использования в будущем.

Описание: информация об уязвимости доводится до сведения определенного круга клиентов. Для раскрытия информации могут быть использованы какие-либо или все механизмы, предусмотренные политикой раскрытия информации об уязвимостях. Механизмы распространения информации могут различаться в зависимости от потребностей или ожиданий целевой аудитории. Передача информации может проходить в форме выпуска уведомления или бюллетеня безопасности, рассылаемых по электронной почте или через текстовые сообщения, публикации на веб-сайте или в социальной сети, а также посредством других соответствующих форм и каналов связи. Раскрываемые материалы должны соответствовать определенному формату, включая в себя, как правило, такую информацию, как обзор или описание, уникальный идентификатор уязвимости, последствия, степень тяжести или оценку по CVSS, способ решения проблемы (устранение или смягчение), а также ссылки на соответствующие источники и материалы.

Результат: своевременное предоставление качественной и содержательной информации клиентам (или общественности) позволяет предупредить, обнаружить уязвимость, а также устранить/смягчить ее.

7.5.3 Функция: обратная связь по итогам раскрытия информации об уязвимостях

Цель: получение от клиентов вопросов и отчетов по поводу раскрытия информации и документа об уязвимостях и подготовка ответов на них.

Описание: после выявления новой уязвимости CSIRT могут рассчитывать на последующие контакты с некоторыми клиентами в форме вопросов относительно документа об уязвимости. Вопросы могут свидетельствовать, в частности, о необходимости пояснений относительно механизма раскрытия информации об уязвимостях, его пересмотра или внесения в него поправок. Клиенты могут просто поблагодарить за полученный документ об уязвимости, подтвердить факт его получения или же сообщить о проблеме или сложностях с применением предлагаемых мер устранения/смягчения. Если указывалось, что уязвимость уже была использована ранее, клиенты могут сообщать о новых инцидентах, последовавших в результате раскрытия информации об уязвимости. Такие отчеты следует обрабатывать в рамках функций услуги CSIRT, касающейся отчетов об инцидентах.

Результат: получены своевременные ответы на любые вопросы или запросы о помощи, поступившие после получения информации об уязвимости.

7.6 Услуга: реагирование на факторы уязвимости[8]

Цель: активный поиск информации об известных уязвимостях и принятие на ее основании мер для предупреждения, обнаружения и устранения/смягчения этих уязвимостей.

Описание: функции в рамках этой услуги призваны определить, присутствует ли обнаруженная уязвимость в системах клиентов, зачастую путем целенаправленного поиска таких уязвимостей. Услуга может предусматривать также принятие последующих мер по устранению или смягчению уязвимости с использованием стратегий установки обновлений или применения обходных решений.

Результат: на основании полученной информации были приняты меры к обнаружению уязвимости, устранению/смягчению обнаруженной уязвимости и недопущению использования уязвимости.

В рамках данной услуги предполагается осуществление следующих функций:

- обнаружение/сканирование уязвимостей;
- устранение уязвимостей.

Услуга по реагированию на факторы уязвимости и связанные с ней функции обычно осуществляются силами не CSIRT, а других специализированных групп, действующих в рамках организации. Кроме того, эту услугу, как правило, не предоставляет координационная CSIRT.

7.6.1 Функция: обнаружение/сканирование уязвимостей

Цель: ведение активного поиска известных уязвимостей в действующих системах.

Описание: цель данной функции заключается в обнаружении ранее не исправленных или не смягченных уязвимостей, прежде чем они будут использованы или окажут воздействие на сеть или устройства. Функция может быть инициирована в ответ на сообщение о новой уязвимости или осуществляться в рамках периодических проверок на присутствие известных уязвимостей. Чтобы обеспечить эффективность процесса обнаружения уязвимостей, полезно иметь реестр систем. Наличие такого реестра, в котором можно получить информацию о версии программного обеспечения, может позволить организации быстро оценить степень проникновения вновь обнаруженной уязвимости в ее инфраструктуру.

При осуществлении этой функции могут использоваться материалы, полученные в результате других услуг или функций, которые могут инициировать применение данной функции.

Результат: применение официальных процедур или инструментов выявления позволяет обнаруживать уязвимости.

[8] Хотя иногда эту функцию и подфункции по обнаружению уязвимостей относят к категории управления уязвимостями, в настоящей концепции предоставления услуг CSIRT они отнесены к услуге по реагированию на факторы уязвимости, которая является составной частью более широкой сферы обслуживания, называемой в концепции управлением уязвимостями.

В рамках данной функции предполагается осуществление следующих подфункций:

- сканирование/поиск уязвимостей;
- оценки уязвимости систем безопасности/тестирование на возможность проникновения.

Эта функция обычно осуществляется силами других структур (например, службами IT, SOC, сторонними специалистами, владельцами систем).

7.6.2 Функция: устранение уязвимостей

Цель: устранение или смягчение уязвимостей, чтобы не допустить их использования, обычно путем своевременной установки предоставленных поставщиком обновлений или иными методами.

Описание: задача мер по уменьшению уязвимости – устранить или ликвидировать уязвимость. В случае уязвимостей в программном обеспечении это обычно происходит путем применения и установки предоставленных поставщиком средств – обновлений или корректировок программного обеспечения. Если нет возможности получить или установить одобренные корректировки, для недопущения использования уязвимости можно применить альтернативную меру смягчения или обходное решение. Эта функция обычно осуществляется вслед за обнаружением уязвимости в рамках осуществления функции по обнаружению/сканированию/ поиску уязвимостей.

Результат: риск использования уязвимости устранен или ограничен.

В рамках данной функции предполагается осуществление следующих подфункций:

- устранение причин уязвимости (управление внесением корректировок);
- смягчение уязвимости.

Эта функция обычно осуществляется силами не CSIRT, а других структур (например, службой IT, SOC, владельцами систем).

8 Сфера обслуживания: осведомленность о ситуации

Осведомленность о ситуации предполагает способность выявлять, обрабатывать и понимать ключевые элементы событий, происходящих в рамках сферы ответственности CSIRT и вокруг нее и способных негативно отразиться на деятельности или миссии ее клиентов, а также информировать о таких событиях. Осведомленность о ситуации означает, в числе прочего, знание текущей ситуации и способность определить или предвидеть ее возможные изменения. К данной сфере обслуживания относятся функции сбора соответствующей информации из разных источников, ее интегрирования и своевременного распространения в целях оказания клиентам содействия в принятии более информированных решений. Для обеспечения осведомленности о ситуации некоторые организации предпочитают создавать отдельную группу, в других эти функции возлагаются на сотрудников CSIRT в силу авторитета этой группы, понимания ею контекста, наличия технических возможностей, доступа к активам, внешних связей и возложенной на нее миссии по предупреждению инцидентов. Обеспечение осведомленности о ситуации предусматривает не только реагирование на инциденты; эта услуга предоставляет другим услугам, таким как управление событиями в области информационной безопасности, управление инцидентами и передача знаний, возможность получать данные, проводить анализ и предпринимать действия. В рамках этой сферы обслуживания обеспечивается надлежащее интегрирование информации, исходящей из других сфер обслуживания, и ее своевременное доведение до сведения соответствующих клиентов.

В рамках этой сферы обслуживания выполняются следующие функции:

- получение данных;
- анализ и синтез;
- коммуникация.

8.1 Услуга: получение данных

Цель: собирать данные, позволяющие повысить осведомленность о происходящих внутренних и внешних событиях, способных повлиять на состояние безопасности клиентов.

Описание: запрашивать, собирать, определять и удовлетворять запросы клиентов на предоставление информации, необходимой для обеспечения осведомленности о важных для клиентов внутренних и внешних событиях. Эта услуга предполагает организацию сбора соответствующей информации, включая новости о текущих событиях, планирование будущих событий, составление отчетов и сообщений, фильтрование собранной информации, ее обработку для использования при анализе, прогнозировании и обнаружении инцидентов либо в иных целях (например, для разработки планов или отслеживания тенденций), ее сохранение для последующего использования, повышение ее доступности для поиска и т. п. Собранные данные используются для определения необходимых предупредительных мер и для помощи в принятии информированных решений в отношении управления инцидентами и мер по обеспечению доступности, целостности и безопасности информации. Не получив общего представления о важнейших элементах ситуации, другие функциональные подразделения имеют более

высокий риск составить неправильную картину в целом. Для разработки необходимой политики и процедур группы CSIRT могут применять технологии сбора и проверки информации.

Результат: данная услуга позволяет получить следующие результаты:

- набор требований к сбору информации, который определяет потребности в осведомленности о ситуации и увязывает эти требования с видами информации, которые необходимо собрать для удовлетворения этих потребностей;
- информация о нынешнем и предполагаемом будущем статусе ресурсов клиентов и проводимых ими мероприятий;
- информация о внешних событиях или тенденциях, дающая представление об обстановке и среде, в которой действуют клиенты, в том числе о новых технологиях, методах, практике, рисках и угрозах;
- информация, должным образом отформатированная и подготовленная для анализа и мероприятий по обнаружению.

В рамках данной функции предполагается осуществление следующих подфункций:

- разработка единой политики, ее уточнение и предоставление рекомендаций по ее реализации;
- привязка ресурсов к функциям, ролям, действиям и ключевым рискам;
- сбор данных;
- обработка и подготовка данных.

8.1.1 Функция: разработка единой политики, ее уточнение и предоставление рекомендаций по ее реализации

Цель: определить контекст, который должен учитываться клиентами и их ресурсами, чтобы понять, как должна функционировать инфраструктура.

Описание: сбор данных, разработка единой политики и ее уточнение определяют основы приемлемой повседневной деятельности. Конечным результатом является контекст, определяющий образ действий, которого клиенты и их инфраструктура, как предполагается, должны придерживаться в приемлемых условиях. Для CSIRT, действующих в рамках организаций, контекст включает понимание приемлемых для организации принципов политики, планов, нормального режима работы, допустимого риска и компромиссных решений. Это понимание и контекст создают основу, с которой могут сравниваться результаты наблюдений.

Результат: понимание приемлемых результатов наблюдений за происходящим в структуре клиента. При этом основное внимание уделяется изменениям и последствиям для инфраструктуры ресурсов.

8.1.2 Функция: привязка ресурсов к функциям, должностям, действиям и ключевым рискам

Цель: получить представление об имеющихся ресурсах, их принадлежности, исходных показателях и предполагаемых действиях, чтобы использовать эти данные для анализа, позволяющего выявить аномальные результаты наблюдения за ситуацией.

Описание: Сотрудникам CSIRT необходимо знать текущее состояние дел с обеспечением кибербезопасности клиента, а также точно представлять, что считается для него приемлемым уровнем безопасности. Для этого им, возможно, необходимо узнать:

- кто является законным пользователем внутренних и общедоступных систем и устройств;
- какие авторизованные устройства используются и в каких целях;
- какие процессы и приложения являются утвержденными, где допускается их использование и какие потребности клиента они удовлетворяют.

Эта информация помогает установить приоритетность ресурсов, потенциально подверженных риску, и определить условия для проведения мероприятий по управлению инцидентами. Чем более полной информацией будут располагать сотрудники CSIRT, тем проще им будет выявить проблемы в области безопасности и попытаться их решить. Для получения полной информации CSIRT, возможно, необходим будет доступ к применяемым стратегиям обеспечения безопасности, имеющимся средствам управления доступом, актуальным реестрам компьютерного оборудования и программного обеспечения, а также к подробным схемам сети.

Результат: осуществление этой функции позволяет составить следующие перечни:

- перечень основных функций и ресурсов, обеспечивающих их осуществление; некоторые ресурсы могут обеспечивать осуществление нескольких функций одновременно;
- перечень должностных лиц, осуществляющих каждую функцию, и эквивалентных им цифровых ролей в ресурсах;
- перечень обычно допустимых действий для каждого должностного лица;
- перечень основных рисков для ресурсов и для функций;

По мере изменения ситуации содержание этих перечней будет пересматриваться.

8.1.3 Функция: сбор данных

Цель: собирать информацию для услуги анализа и интерпретации и/или других услуг CSIRT.

Описание: мероприятия по сбору информации и данных не ограничиваются их получением в автоматическом режиме. Сбор данных подразумевает также выявление полезных источников, таких как информационная деятельность внешних структур, в том числе новостные сообщения от клиентуры других организаций, средств массовой информации, других CSIRT или организаций в сфере безопасности, внутренняя деятельность (например, организационные изменения), развитие технологий, события во внешней среде, события политического характера, тенденции в сфере злоумышленных действий, тенденции в обеспечении защиты, конференции, имеющиеся учебные материалы и т. д.

Функция сбора данных поддерживает деятельность в рамках других услуг, таких как управление событиями в области информационной безопасности, управление инцидентами в области информационной безопасности и передача знаний. В рамках этих услуг она способствует выполнению функций и действий, касающихся, например, анализа, прогнозирования, реагирования и уменьшения рисков. Вновь собранная информация может свидетельствовать о более высокой, чем раньше, вероятности злоумышленных действий в отношении клиента. События во внешней среде могут стать источником информации, свидетельствующей о наличии в данное время новых рисков для ресурсов или о необходимости более активных действий по обнаружению. В целом такая информация помогает получать актуальные данные, необходимые для принятия решений и реагирования на инциденты.

Результат: собраны данные и подготовлены наборы данных, характеризующие операционный контекст или среду деятельности и пригодные для использования в рамках других услуг и функций, в том числе аналитических, что позволяет представить клиентам картину текущей ситуации, идентифицировать оповещения или разработать план смягчения возросших рисков для ресурсов и вспомогательной инфраструктуры.

8.1.4 Функция: обработка и подготовка данных

Цель: создание набора достоверных, непротиворечивых и актуальных данных, поддерживающих действия CSIRT и отвечающих потребностям услуги анализа.

Описание: функция обработки и подготовки данных предусматривает преобразование, обработку, стандартизацию и проверку набора данных. Источники данных о кибербезопасности необходимо проверять на надежность, что часто бывает обусловлено большим количеством ложноположительных результатов. Кроме того, соответствующие данные нередко поступают в разных форматах, и для проведения полного анализа необходимо вновь полученные данные объединить с полученными прежде. Иногда в ходе подготовки данных возникает необходимость анализировать или обрабатывать некоторые виды данных (например, статьи). Например, может оказаться необходимым извлечь из статьи соответствующую информацию по безопасности (имена, даты, места, информацию по техническим вопросам, сведения о слабых местах, названия систем) и сопоставить их с внутренними данными с точки зрения возможных последствий.

Некоторые методы проведения анализа требуют хранения данных в одном формате или наличия одного и того же количества записей в файле. Подготовка данных может проходить в несколько этапов. Дополнение данных (известное также как обогащение данных) проводится путем добавления к данному фрагменту данных связанной с ними информации из других внутренних и внешних источников. Например, группы могут собирать такую информацию об адресах Интернет-протоколов (IP-адресах), как идентификаторы автономных систем, страновые коды или данные геолокации. Там, где речь идет об информации о внутренних ресурсах, группы могут дополнять свои реестры данных о ресурсах сведениями об имени ответственного за ресурс, его должности, выданных ему разрешениях в отношении других ресурсов, реальном местонахождении его работы в течение продолжительного времени и т. д.

Результат: имеются в наличии данные, которые могут быть использованы в рамках других услуг или функций.

8.2 Услуга: анализ и синтез

Цель: понимание момента, когда реальная ситуация не соответствует ожиданиям (например, когда конкретные активы могут подвергнуться воздействию опасного события).

Описание: процесс применения текущих и ранее полученных данных и методов анализа для определения ситуации, которая может затронуть активы клиента и его средства обеспечения безопасности, нередко осуществляемый в форме поиска ответа на вопрос или тестирования на основе опыта. Анализ может выявить момент, когда события перестают соответствовать обычному ожидаемому поведению, или раскрыть информацию об обстоятельствах, характере или причинах событий или моделей поведения. Анализ позволяет предусмотреть последствия для текущей ситуации и ситуации в будущем. Например, система может записать, что идентификационные данные пользователя были успешно введены в систему, однако она не показывает, были ли действия совершены законным пользователем. Для того чтобы группа получила более точную картину происходящего, позволяющую определить правомерность события, в анализ следует включать сведения из новых источников (например, опроса пользователя). Для анализа и интерпретации собранных данных и их воздействия на клиентов могут использоваться самые разные методы.

Результат: составлен набор выводов о возможных прошлых, нынешних и/или вероятных будущих событиях, касающихся клиента. Сюда же могут быть включены рекомендации относительно тех или иных решений, которые необходимо принять клиентам. Результаты анализа следует дополнить фактическими данными, такими как результаты наблюдений, полученные с датчиков и из других источников, и результаты их интерпретации, проведенной аналитиками с использованием различных методов. Анализ предусматривает также принятие решения о том, кому именно из клиентов следует сообщить о результатах и что именно им следует сообщить.

В рамках данной услуги предполагается выполнение следующих функций:

- прогнозирование и выводы;
- обнаружение событий (путем оповещения и/или поиска);
- воздействие на ситуацию.

8.2.1 Функция: прогнозирование и выводы

Цель: анализ информации, полученной на этапе сбора данных, в целях получения картины текущей ситуации или прогнозирования развития событий в будущем.

Описание: процесс формулирования выводов относительно текущей ситуации и прогнозирования возможной ситуации в ближайшем будущем на основании статуса собранных данных и динамики их изменения. Иногда на основании этих данных можно оперативно сделать вывод о наличии проблемы безопасности.

Результат: обновление картины текущей ситуации вместе с накоплением знаний о том, когда изменится ситуация и как она может измениться.

8.2.2 Функция: обнаружение событий (путем оповещения и/или поиска)

Цель: представление клиентам детального описания и подтверждения текущей ситуации.

Описание: систематический и часто целенаправленный поиск аномальной деятельности в сети и вне ее на основании информации из внешних и внутренних источников и выявленных тенденций. Оказание помощи клиентам в проведении анализа данных, полученных с датчиков и из других источников, на основании которых они могут сделать выводы о среде и ситуации, в которой они находятся. Например, если датчик обнаружения вирусов посылает оповещение о наличии подозрительного файла, группа может проанализировать конфигурацию системы, конфигурацию датчика, файл, в отношении которого было послано оповещение, действия пользователя на тот момент и, более того, сделать вывод о степени серьезности наблюдаемой проблемы. Важное содействие в осуществлении этой функции может оказать сфера обслуживания по управлению инцидентами в области информационной безопасности. Данные наблюдения от датчиков, применяемых для обнаружения инцидентов, могут совместно использоваться многими подразделениями по предоставлению услуг.

Сотрудникам CSIRT необходимо также составить картину текущей ситуации на основании конкретных данных об угрозах. Иногда подобные действия называют поиском угроз. Обычно поиск угроз предполагает либо подготовку среды к обнаружению конкретной угрожающей деятельности, либо поиск такой деятельности, которая, возможно, уже осуществляется.

Результат: обновление картины текущей ситуации на основании выявленных в сфере деятельности клиента событий.

8.2.3 Функция: содействие принятию решений по вопросам управления инцидентами в области информационной безопасности

Цель: получение новых аналитических материалов, которые могут помочь уменьшить ущерб при инциденте, снизить риск в будущем или выявить вновь возникшее слабое место.

Описание: анализ конкретных фактических данных позволяет получить аналитические материалы, способствующие урегулированию инцидента. Иногда CSIRT могут ориентировать свой ситуационный анализ на получение конкретного желаемого результата, например урегулирования инцидента. Некоторые меры реагирования на инцидент могут по-разному воздействовать на картину текущей ситуации, и те, кто отвечает за принятие таких мер, могут просить о проведении анализа возможных вариантов (например, на предмет последствий, затрат, риска неудачи). Потребности клиентов в сфере принятия решений могут меняться по мере изменения картины текущей ситуации, и в помощь им сотрудники CSIRT могут инициировать проведение новых анализов. Эта деятельность имеет отношение к сфере обслуживания по управлению инцидентами в области информационной безопасности. Содействие в осуществлении функций управления инцидентами оказывает сфера обслуживания осведомленности о ситуации, а сама ситуация может изменяться вследствие мер, принимаемых в рамках сферы обслуживания по управлению инцидентами.

Результат: на основании вновь полученных данных наблюдения повысился уровень осведомленности о ситуации как основа для осуществления функций по управлению инцидентами. В результате принятия мер по управлению инцидентами обновлена картина текущей ситуации.

8.2.4 Функция: воздействие на ситуацию

Цель: определение ожидаемого потенциального воздействия данного или возможного результата наблюдений на ситуацию.

Описание: данная функция определяет, какое воздействие прогнозы или предположения могут оказать на текущую ситуацию или на ситуацию в ближайшем будущем. К числу таких воздействий может относиться увеличение или снижение тех или иных рисков, например потери данных, простоя системы, или последствий для конфиденциальности/наличия/целостности данных.

Результат: проведен анализ вероятного воздействия предположений или прогнозов на ситуацию.

8.3 Услуга: коммуникация

Цель: уведомление клиентов или иных членов сообщества по проблемам безопасности об изменении ситуационных рисков.

Описание: знания, полученные благодаря осведомленности о ситуации, необходимо довести до сведения клиентов. Это позволит им прореагировать на полученные данные и принять меры к повышению уровня защиты, например снижая риски для третьих лиц путем совершенствования систем безопасности некоторых поставщиков, входящих в группу повышенного риска.

Результат: клиенты своевременно получают точную, имеющую практическую ценность информацию и таким образом могут лучше понять прежнюю ситуацию и внести положительные изменения в текущую ситуацию, а также поправить дела в будущем.

В рамках данной услуги предполагается осуществление следующих функций:

- внутренние и внешние коммуникации;
- представление отчетов и рекомендаций;
- осуществление;
- распространение информации/интегрирование информации/обмен информацией;
- управление обменом информацией.

8.3.1 Функция: внутренние и внешние коммуникации

Цель: информирование клиентов (и другие стороны) о текущей ситуации и ее возможных изменениях.

Описание: Полученные результаты анализа и интерпретации могут быть использованы для совершенствования процесса принятия решений с использованием для этого процедур

внутренних и внешних коммуникаций. Конкретные порции информации доводятся до сведения тех, кому она необходима. Коммуникация включает и способ доставки контента, и сам контент. Сотрудники CSIRT могут предоставлять новую информацию и объяснять, как она изменит ситуацию. Например, они могут сообщить клиентам, какие последствия для них может иметь новый метод действий злоумышленников, выявленный в ходе инцидента. Также может сообщаться информация о тенденциях, например о наиболее полезных источниках обогащенных данных и о том, каким образом клиент может использовать эти данные для повышения уровня своей осведомленности о ситуации.

Результат: клиенты лучше информированы и готовы принимать меры и решения, которые повысят их уровень безопасности или улучшат их ситуацию.

8.3.2 Функция: представление отчетов и рекомендаций

Цель: доведение результатов, артефактов или выводов, содержащих важную информацию, которая была выявлена или получена в ходе анализа, до сведения заинтересованных сторон понятными для них способами и в удобных для них форматах.

Описание: в отчетах и рекомендациях необходимо четко показать, какой выбор есть у клиентов и какие действия им предстоит предпринять, а также дать анализ предполагаемых последствий каждого варианта и каждого действия. В информации о выводах необходимо привести перечень фактических данных в обоснование анализа и рекомендаций (если рекомендации даются). Аудитории следует четко разъяснить, какими методами были получены выводы, чтобы они могли вынести собственное суждение в отношении представленных претензий. Сотрудники CSIRT могут составлять отчеты по поводу отдельного события, серии событий, тенденций, особенностей, возможных событий и т. п., чтобы помочь своим клиентам разобраться в ситуации.

Результат: повышена способность своевременно предоставлять точные и полные отчеты о ситуации, фактические данные в обоснование выводов и/или рекомендации относительно возможных действий и их последствий для клиентов.

8.3.3 Функция: осуществление

Цель: использовать коммуникации для повышения готовности среды, в которой действуют клиенты, к изменениям ситуации и реагированию на такие изменения.

Описание: иногда сотрудники CSIRT могут также вносить рекомендуемые изменения в компоненты инфраструктуры безопасности, например изменяя правила для брандмауэра на конкретной системе-ловушке по результатам ситуационного анализа.

Результат: клиенты принимают меры или вносят изменения в инфраструктуру на основании полученных сообщений, содержащих данные анализов, прогнозы и/или рекомендации.

8.3.4 Функция: распространение информации/интегрирование информации/ обмен информацией

Цель: сбор, стандартизация и подготовка информации, а впоследствии обмен ею с и клиентами и другими лицами.

Описание: настоящая функция может включать в себя следующие подфункции:

- использование результатов предоставления услуги анализа для внутренних и внешних процессов разработки планов и принятия решений;
- определение надлежащих получателей информации;
- обеспечение доступности результатов анализа;
- обеспечение успешной передачи сведений;
- отслеживание хода обмена информацией и предоставление соответствующих отчетов;
- направление соответствующей информации в услугу передачи знаний для дальнейшего использования и распространения.

Результат: результаты анализа в рамках услуги осведомленности о ситуации используются (как самой организацией, так и ее клиентами) в качестве исходных данных для принятия решений по ключевым направлениям деятельности, включая поиск угроз, анализ и урегулирование инцидентов. Распространение результатов осуществляется в рамках мер по обработке или обнаружению инцидентов. На основании информации и данных, полученных в рамках услуги осведомленности о ситуации, в сфере обслуживания по передаче знаний могут быть подготовлены примеры наиболее эффективной практики, отчеты, а также материалы для обучения и повышения осведомленности.

8.3.5 Функция: управление обменом информацией

Цель: обеспечение успешного и удобного процесса передачи информации.

Описание: настоящая функция может включать в себя следующие подфункции:

- предоставление информации другим группам;
- подготовка отформатированной информации к передаче;
- отслеживание процесса передачи и его результатов.

Результат: есть уверенность, что была передана нужная информация и что она была получена партнерами, клиентами и другими участниками сообщества. Представлены отчеты о ходе обмена информацией.

8.3.6 Функция: обратная связь

Цель: повышение качества, своевременности, точности и актуальности данных, получаемых из внутренних и внешних источников.

Описание: эта функция предусматривает обеспечение обратной связи по поводу информации, предоставленной, полученной и использованной клиентами, другими поставщиками услуг или иными заинтересованными сторонами. Была ли полученная информация точной, применимой, своевременной, стратегической, новой/ранее не известной и т. д.? Была ли она полезна для

проведения расследования? Позволила ли она найти новые подходы? Речь здесь может идти и о предоставлении другой CSIRT (выступающей в качестве внешнего источника) информации о пользе или изменении подписей, выводах по итогам применения ловушек, показателях компрометации, предостережениях, сведениях об угрозах, мерах по смягчению и т. д. Эта работа может проводиться силами сферы обслуживания по передаче знаний. В этом случае результаты должны быть доведены до сферы обслуживания осведомленности о ситуации.

Результат: данные наблюдений и обратной связи доводятся до сведения внутренних и внешних источников в целях повышения точности, своевременности, качества и полезности полученной информации.

9 Сфера обслуживания: передача знаний

В силу специфики своих услуг CSIRT имеют уникальную возможность собирать соответствующие данные, проводить детальный анализ и выявлять угрозы, тенденции и риски, равно как и разрабатывать оптимальные на данный момент практические методы, помогающие организациям обнаруживать инциденты в области безопасности, предупреждать их и реагировать на них. Передача таких знаний клиентам является ключевым условием повышения кибербезопасности в целом.

В рамках данной сферы обслуживания предусматривается предоставление следующих услуг:

- повышение осведомленности;
- профессиональная подготовка и обучение;
- практические занятия;
- консультирование по техническим вопросам и вопросам политики.

9.1 Услуга: повышение осведомленности

Цель: повышение общей способности клиентов обеспечивать свою безопасность и помогать им обнаруживать, предупреждать инциденты и устранять их последствия; обеспечение повышения уровня подготовки и осведомленности клиентов.

Описание: эта услуга предполагает принятие в сотрудничестве с клиентами, специалистами и доверенными партнерами мер по повышению общего уровня понимания угроз и мер, которые могут быть приняты для предупреждения или смягчения рисков, обусловленных этими угрозами.

Результат: клиенты в необходимой степени осведомлены о:

- событиях, действиях и тенденциях, которые могут негативно отразиться на их способности действовать оперативно и безопасно;
- мерах, которые необходимо принимать для обнаружения, предупреждения и смягчения угроз и злонамеренных действий;
- передовом опыте обеспечения безопасности и операционной деятельности.

В рамках данной услуги предполагается осуществление следующих функций:

- проведение исследований и обобщение информации;
- разработка материалов для составления отчетов и повышения осведомленности;
- распространение информации;
- информационно-разъяснительная работа.

9.1.1 Функция: проведение исследований и обобщение информации

Цель: обобщение, сопоставление и приоритизация информации, которая может быть доведена до сведения клиентов в целях повышения эффективности принимаемых ими мер безопасности, а также предупреждения и смягчения рисков.

Описание: эта функция предполагает проведение исследований и обобщение данных, необходимых для подготовки информационных материалов и отчетов, в том числе полученных в рамках осуществления других услуг/функций, прежде всего в таких сферах обслуживания, как управление событиями в сфере безопасности, управление инцидентами в сфере безопасности и осведомленность о ситуации.

Результат: информация о соответствующих тенденциях, происходящих в данный момент инцидентах и передовом опыте обобщена и может быть использована для подготовки отчетов и информационных материалов для разных аудиторий.

9.1.2 Функция: разработка материалов для составления отчетов и повышения осведомленности

Цель: использование обобщенной информации и результатов соответствующих исследований для подготовки материалов на различных носителях, предназначенных для разных аудиторий и имеющих целью оптимальное донесение до них соответствующего контента.

Описание: эта функция предполагает разработку материалов для разных аудиторий (технического персонала, руководителей, конечных пользователей и т. д.) и в разных форматах, например в виде презентаций, коротких видеофильмов, мультфильмов, буклетов, материалов технического анализа, отчетов о тенденциях и годовых отчетов.

Результат: разработаны отвечающие потребностям клиентов отчеты CSIRT и информационные материалы необходимого качества с использованием разнообразных и эффективных методов и платформ доставки.

9.1.3 Функция: распространение информации

Цель: распространение информации по проблемам безопасности в целях повышения уровня осведомленности и качества практических мер по обеспечению безопасности.

Описание: эта функция предполагает осуществление процесса распространения информации, который может помочь CSIRT наилучшим образом доставлять подготовленные ею отчеты и информационные материалы ее клиентам с учетом особенностей разных аудиторий и содержания этой информации.

Результат: создана система распространения информации, позволяющая клиентам CSIRT получать своевременный доступ к актуальной информации с использованием различных методов, например подкастов, блогов, публикаций и видео в социальных сетях, пресс-релизов, объявлений, кампаний, открытых докладов и т. д.

9.1.4 Функция: информационно-разъяснительная работа

Цель: установление и поддерживание отношений со специалистами или организациями, которые могут помочь CSIRT в осуществлении ее миссии или участвовать в этой работе.

Описание: эта функция предполагает создание партнерств, укрепление сотрудничества и привлечение ключевых заинтересованных сторон, как входящих, так и не входящих в число

клиентов, в целях распространения информации и наиболее эффективного практического опыта; оказания помощи клиентам и внешним заинтересованным сторонам в ознакомлении с услугами, которые может предоставлять CSIRT, и выгодами их получения; содействия CSIRT в более глубоком изучении потребностей клиентов; а также в целях создания условий для осуществления миссии CSIRT. Такие действия могут предусматривать обеспечение функциональной совместимости или укрепление сотрудничества между организациями или в их рамках.

Результат: ведется активная и последовательная информационно-разъяснительная работа, включающая встречи с ключевыми заинтересованными сторонами, участие в отраслевых совещаниях, выступления на конференциях, организацию конференций и т. п.

9.2 Услуга: профессиональная подготовка и обучение

Цель: обеспечение профессиональной подготовки и обучения клиентов CSIRT (в том числе, возможно, специалистов по организационной работе и сотрудников CSIRT) по темам, связанным с кибербезопасностью, обеспечением информационной безопасности и управлением инцидентами.

Описание: программа профессиональной подготовки и обучения может помочь CSIRT установить связи со своей клиентурой и повысить общую эффективность мер по обеспечению кибербезопасности, в том числе способности предотвращать будущие инциденты. Такая программа может:

- помочь в поддержании осведомленности пользователей;
- помочь клиентам разобраться в меняющейся ситуации и угрозах;
- содействовать обмену информацией между CSIRT и ее клиентами;
- обучать клиентов применению инструментов, процессов и процедур, связанных с обеспечением безопасности и управлением инцидентами.

Этого можно добиться за счет разного рода действий, включая документирование требуемых знаний, навыков и способностей (ЗНС), разработку образовательных и учебных материалов, предоставление контента, наставничество, а также профессиональный рост и развитие навыков. Эти виды деятельности в комплексе будут содействовать наращиванию потенциала клиентуры и самой группы.

Результат: создана целостная программа профессиональной подготовки и обучения, позволяющая клиентам CSIRT приобретать необходимые знания:

- о методах обнаружения угроз, их предупреждения и реагирования на них;
- об инструментах и практических методах защиты важнейших активов;
- о процедурах управления инцидентами и способах получения помощи.

В рамках данной услуги предполагается осуществление следующих функций:

- сбор информации о потребностях в отношении знаний, навыков и способностей;
- разработка образовательных и учебных материалов;

- предоставление контента;
- наставничество;
- повышение квалификации сотрудников CSIRT.

9.2.1 Функция: сбор информации о потребностях в отношении знаний, навыков и способностей

Цель: должная оценка, определение и документальное оформление потребностей клиентов в отношении обязательных ЗНС, подготовка соответствующих учебных и образовательных материалов и повышение уровня навыков клиентов.

Описание: эта функция предполагает сбор информации о потребностях в отношении знаний, навыков и способностей (ЗНС), а также компетенции клиента в целях определения того, какое обучение и профессиональную подготовку необходимо ему предоставить.

Результат: определены и документально оформлены потребности клиентов в отношении ЗНС, с тем чтобы использовать эти данные при разработке соответствующих образовательных и учебных материалов.

9.2.2 Функция: разработка образовательных и учебных материалов

Цель: разработка, исходя из потребностей клиентов в отношении ЗНС, образовательных, методических и учебных материалов, соответствующих методам передачи контента, которые признаны оптимальными с точки зрения работы с разными аудиториями или передачи конкретных знаний.

Описание: эта функция предполагает разработку или приобретение образовательных и учебных материалов, таких как презентации, лекции, демонстрации, модели, видео, книги, брошюры и т. д.

Результат: созданы образовательные и учебные материалы CSIRT соответствующего качества, которые удовлетворяют потребностям клиентов и предусматривают использование разнообразных и эффективных методов и платформ представления материалов.

9.2.3 Функция: предоставление контента

Цель: разработка официальной процедуры предоставления контента, которая может помочь CSIRT наиболее эффективным образом предоставлять контент своим клиентам с учетом особенностей разных аудиторий и разных видов контента.

Описание: эта функция предполагает передачу знаний и контента "учащимся". Это может быть осуществлено разными методами, такими как обучение с помощью компьютерных технологий/онлайновое обучение, обучение с инструктором, виртуальное обучение, конференции, презентации, лабораторные занятия, занятия в форме соревнования, обучение по книгам, веб-трансляция видеоматериалов и т. п.

Результат: разработана система предоставления контента, призванная помочь клиентам получить технические и коммуникативные навыки с применением альтернативных методов,

в том числе книг, брошюр, веб-трансляции видеоматериалов, презентаций, практических лабораторных занятий, занятий в форме соревнований, обучения с помощью компьютерных технологий/онлайнового обучения, очного обучения и т. д. В итоге клиенты имеют возможность освоить предоставленный контент.

9.2.4 Функция: наставничество

Цель: разработка программы привлечения опытных сотрудников к обучению персонала CSIRT, клиентов или доверенных внешних партнеров на основе установившихся отношений.

Описание: программа наставничества может обеспечить как формальные, так и неформальные механизмы, в рамках которых наставник делится с обучаемым знаниями, способами приобретения навыков, наблюдениями, а также жизненным и профессиональным опытом вне рамок официальных взаимоотношений подчинения и структуры группы. В рамках этой деятельности могут быть организованы посещения объектов, ротация (обмен), наблюдение за наставником на его рабочем месте и обсуждение мотивации тех или иных решений и действий.

Результат: в коллективе CSIRT снизился уровень текучки кадров, повысилась лояльность, степень доверия и общая способность принимать обоснованные решения. Возросли способности и потенциал клиентов и сотрудников CSIRT, в том числе в сфере выстраивания доверительных отношений.

9.2.5 Функция: повышение квалификации сотрудников CSIRT

Цель: оказание помощи сотрудникам в успешном и корректном планировании их карьеры и карьерном росте.

Описание: определив необходимый набор навыков, CSIRT использует повышение профессиональной квалификации для обеспечения непрерывности процесса получения новых знаний, навыков и способностей, связанных с профессиональной сферой обеспечения безопасности, специфическими служебными обязанностями, а также общей средой деятельности группы. Для этого могут быть организованы посещение конференций, прохождение углубленной профессиональной подготовки, перекрестное обучение и т. п.

Результат: группа укомплектована квалифицированными и подготовленными сотрудниками, обладающими необходимыми техническими и коммуникативными навыками и пониманием процессов, которые соответствуют их должностным обязанностям и требованиям, предъявляемым к ним на рабочих местах. Сотрудники CSIRT готовы к выполнению повседневных задач по оказанию содействия группе и ее клиентам.

9.3 Услуга: практические занятия

Цель: проведение практических занятий по оценке и повышению эффективности и результативности осуществления услуг и функций в сфере кибербезопасности.

Описание: организация предлагает клиентам услуги, предназначенные для содействия разработке, проведению и оценке практических занятий по вопросам кибербезопасности,

имеющих целью обучение и/или оценку потенциала, в том числе в области обмена данными, как отдельных клиентов, так и сообщества заинтересованных сторон в целом. Целями таких практических занятий могут быть:

- тестирование политики и процедур – оценить, разработаны ли политика и процедуры, достаточные для эффективного обнаружения инцидентов, реагирования на них и смягчения их последствий. Как правило, такие занятия носят аудиторный/теоретический характер;
- тестирование на оперативную готовность – оценить, сформирована ли у организации способность к управлению инцидентами, то есть способность своевременно и эффективно обнаруживать инциденты, реагировать на них и смягчать их последствия, а также проверить правильность расстановки кадров, актуальность содержания инструкций и корректность выполнения процедур.

Эта услуга направлена на удовлетворение потребностей как организации, так и ее клиентов. В частности, практические занятия по моделированию событий/инцидентов в области кибербезопасности могут использоваться для решения одной или нескольких задач:

- наглядность – продемонстрировать услуги и функции в области кибербезопасности, а также уязвимости, угрозы и риски в целях повышения уровня осведомленности.
- обучение – обучить сотрудников применению новых инструментов, методов и процедур:
  - на уровне практических занятий – предоставить сотрудникам возможность применить инструменты, методы и процедуры, которыми они должны владеть. Практические занятия необходимы для восстановления легко утрачиваемых навыков, а также для повышения и поддержания эффективности работы;
  - на уровне оценки – анализировать и понимать уровень эффективности и результативности услуг и функций в области кибербезопасности, а также уровень подготовки персонала;
  - на уровне проверки – определять возможность обеспечить определенный уровень эффективности и/или результативности услуг и функций в области кибербезопасности.

Результат: повысился уровень эффективности и результативности услуг и функций в области кибербезопасности, определены пути его дальнейшего повышения.

В зависимости от конкретной цели (целей) практического занятия возможны также ознакомление внутренних или внешних заинтересованных сторон с проблемами кибербезопасности, обучение сотрудников, а также оценка и/или проверка эффективности и результативности инструментов, услуг и функций. Существует также возможность накопления опыта для повышения в дальнейшем качества практических занятий и подготовки отчета для руководства или других заинтересованных сторон.

В рамках данной услуги предполагается осуществление следующих функций:

- анализ требований;

- определение формата и создание среды;
- разработка сценария;
- проведение практического занятия;
- обзор результатов практического занятия.

9.3.1 Функция: анализ требований

Цель: обеспечение эффективности практического занятия путем концентрации внимания на конкретных проблемах, которые рассматриваются в его рамках.

Описание: определить учебные задачи и сферу охвата практического задания. Составить перечень конкретных услуг, умений и тем, рассматриваемых в ходе практического занятия. Убедиться, что практическое занятие предусматривает мероприятия и темы, относящиеся к тем навыкам, приобретение которых участниками обязательно или желательно, а также разделы, по которым должно проводиться тестирование.

Результат: подготовлено описание цели практического занятия, а также тех учебных задач, которые должны быть решены в ходе его проведения.

9.3.2 Функция: определение формата и создание среды

Цель: определение и перечисление внутренних и внешних ресурсов и инфраструктуры, необходимых для проведения практического занятия.

Описание: определить формат и платформу, которые позволяли бы решить поставленные задачи и получить планируемые результаты практического занятия.

Результат: определены тип практического занятия (аудиторное занятие, практическая работа, моделирование и т. д.), а также внутренние и внешние ресурсы, необходимые для его проведения.

9.3.3 Функция: разработка сценария

Цель: предоставление целевой аудитории возможности повысить эффективность и результативность услуг и функций, а также уровень навыков, знаний и умений путем работы с смоделированными событиями/инцидентами в области кибербезопасности, включая аспекты связи.

Описание: разработать сценарии практических занятий для помощи заинтересованным сторонам в решении стоящих перед ними задач. Участникам практического занятия и проводящим его лицам следует также предоставить инструкции и руководящие указания; в эти инструкции необходимо включить информацию о рекомендуемых действиях для участников занятия с подробным описанием некоторых/всех этапов сценария.

Результат: разработан основной сценарий и формализованные задания разных видов, а также задачи и обязанности лиц, проводящих занятие.

9.3.4 Функция: проведение практического занятия

Цель: проведение тренировочного/практического занятия, позволяющего персоналу CSIRT повысить степень своей уверенности в правильности плана работы CSIRT, действующей в рамках данной организации, а также в своей способности реализовать его.

Описание: эта функция предполагает проведение тестирования уровня подготовленности учащихся из числа клиентов для определения их способности применять на практике знания, полученные в процессе профессиональной подготовки, и выполнять должностные обязанности или функции. Тестирование может проводиться в реальной или виртуальной среде в форме моделирования, в полевых условиях, в рамках аудиторного занятия в форме деловой игры или на основе сочетания этих методов при условии планомерной постановки задач. Кроме того, это поможет установить, какого уровня подготовки достигла группа, а также есть ли возможности для улучшения ее работы, и если да, то в каких сферах.

Результат: проведена оценка уровня подготовки CSIRT и ее готовности к действиям, показавшая, что ЗНС, ключевые процедуры и меры осуществления в комплексе обеспечивают успешное выполнение работы или требуют адаптации/совершенствования.

9.3.5 Функция: обзор результатов практического занятия

Цель: проведение на материалах фактических наблюдений официального объективного анализа практического занятия.

Описание: подготовить отчет о проведенном занятии, включив в него описание полученных в ходе практического занятия уроков или выводов/примеров наиболее эффективных видов практики, и довести результаты анализа до сведения заинтересованных сторон/руководства.

Результат: подготовлена документация, в которой подробно освещаются степень успешности практического занятия и возможные пути повышения его качества, а также содержатся выводы общего характера и рекомендуемые меры по расширению возможностей организации в области управления инцидентами, совершенствованию процессов, связанных с деятельностью коллектива CSIRT, и укреплению потенциала, в том числе в области обмена данными, как отдельных клиентов, так и сообщества заинтересованных сторон в целом.

9.4 Услуга: консультирование по техническим вопросам и вопросам политики

Цель: обеспечение учета в политике и процедурах клиентов необходимых мер по управлению инцидентами и, в конечном счете, предоставление клиентам возможности более эффективно управлять рисками и угрозами, равно как и повысить эффективность деятельности CSIRT.

Описание: содействовать клиентам CSIRT и основным заинтересованным сторонам, как входящим, так и не входящим в число клиентов, в проведении мероприятий по управлению рисками и обеспечению непрерывной деятельности, предоставляя им по мере необходимости технические рекомендации, помогая клиентам в разработке и осуществлении политики, а также побуждая их оказывать более эффективное содействие CSIRT. Принципы политики важны также с точки зрения официального признания услуг, которые предоставляет CSIRT.

Результат: клиенты имеют возможность принимать решения по организационным вопросам на основании наиболее эффективного практического опыта по обеспечению операционной безопасности, в том числе по обеспечению непрерывной деятельности и преодолению последствий чрезвычайных ситуаций, а также осознают необходимость участия групп по управлению инцидентами, выступающих в качестве доверенных консультантов, в принятии решений относительно деятельности компании, когда это целесообразно.

В рамках данной услуги предполагается осуществление следующих функций:

- содействие управлению рисками;
- содействие разработке планов по обеспечению непрерывной деятельности и преодолению последствий чрезвычайных ситуаций;
- поддержка политики;
- консультирование по техническим вопросам.

9.4.1 Функция: содействие управлению рисками

Цель: совершенствование выявления возможностей и угроз, улучшение механизмов контроля, повышение эффективности процесса предотвращения потерь и управления инцидентами в сочетании с обеспечением информационной безопасности и выполнением других соответствующих функций.

Описание: содействовать проведению мероприятий по оценке рисков или соблюдению нормативных требований. Это может предполагать проведение самой оценки или содействие в анализе ее результатов.

Результат: клиенты имеют возможность выявлять риски и угрозы и выбирать соответствующие варианты управления рисками, в том числе необходимые и эффективные стратегии управления инцидентами, контроля безопасности или смягчения угроз.

9.4.2 Функция: содействие разработке планов по обеспечению непрерывной деятельности и преодолению последствий чрезвычайных ситуаций

Цель: выполнение функции доверенного консультанта по вопросам обеспечения непрерывной деятельности и преодоления последствий чрезвычайных ситуаций путем предоставления объективных, основанных на фактах рекомендаций с учетом ситуации, в которой эти рекомендации могут быть применены, а также любых применимых ограничений в отношении ресурсов.

Описание: содействовать клиентам в проведении мероприятий по повышению устойчивости организации, разработанных с учетом выявленных рисков.

Результат: клиенты имеют возможность должным образом осуществлять планы обеспечения непрерывной деятельности и преодоления последствий чрезвычайных ситуаций, включающие стратегии управления инцидентами и согласующиеся с такими стратегиями.

9.4.3 Функция: поддержка политики

Цель: выполнение функции доверенного консультанта по вопросам разработки и осуществления политики путем предоставления объективных, основанных на фактах рекомендаций с учетом ситуации, в которой эти рекомендации могут быть применены, а также любых применимых ограничений в отношении ресурсов.

Описание: эта функция оказывает содействие клиентам в разработке, реализации, институционализации и обеспечении соблюдения политики, предоставляя им возможность инициировать и поддерживать мероприятия в области управления инцидентами. В случае внутренних CSIRT это обычно предполагает оказание содействия в осуществлении политики в области информационной безопасности и других направлений операционной политики. В случае координационных и национальных CSIRT могут осуществляться также меры поддержки государственной политики и вновь принятого законодательства.

Результат: клиенты имеют возможность разрабатывать эффективную политику, институционализировать политику и обеспечивать осуществление эффективных стратегий управления инцидентами.

9.4.4 Функция: консультирование по техническим вопросам

Цель: проведение консультаций по техническим вопросам, призванных помочь клиентам повысить эффективность управления рисками и угрозами и применять наиболее эффективный практический опыт операционной деятельности и обеспечения безопасности, а также принимать действенные меры реагирования на инциденты.

Описание: в рамках этой функции осуществляется поддержка клиентов и предоставление им рекомендаций по совершенствованию инфраструктуры, инструментов и услуг, имеющих отношение к сфере кибербезопасности, в целях совершенствования мер безопасности и управления инцидентами в целом.

Консультирование может проводиться по следующим вопросам:

- меры обеспечения безопасности при приобретении, проверке соответствия нормативным требованиям, обслуживании и обновлении;
- внутренние и внешние проверки инфраструктуры и инструментов, имеющих отношение к сфере кибербезопасности;
- требования к разработке безопасного программного обеспечения и безопасному кодированию.

Результат: клиентам предоставляется поддержка в разработке, приобретении, управлении, эксплуатации и обслуживании их инфраструктуры, систем и инструментов, а также помощь в наращивании функциональных возможностей, потенциала и зрелости мер по управлению инцидентами.

ПРИЛОЖЕНИЕ 1. Выражение признательности

Следующие представители сообществ CSIRT, работая на добровольных началах, внесли существенный вклад в подготовку настоящей версии концепции предоставления услуг CSIRT. Их фамилии приводятся в алфавитном порядке, без указания титулов и званий, но с указанием организации, которую они представляют, должности и страны.

- Вилюс Бенетис, NRD CIRT (Литва)
- Оливье Калеф (координатор сферы обслуживания), openCSIRT Foundation (Франция)
- Кристина Ойперс (координатор сферы обслуживания), CERT.br (Бразилия)
- Анджела Хорнман, CERT/CC, SEI, CMU (США)
- Аллен Хаусхолдер, CERT/CC, SEI, CMU (США)
- Клаус-Петер Коссаковски (редактор), Гамбургский университет прикладных наук (Германия)
- Арт Мэнион, CERT/CC, SEI, CMU (США)
- Аманда Малленс (сокоординатор сферы обслуживания), CISCO (США)
- Сэмюэл Перл (координатор сферы обслуживания), CERT/CC, SEI, CMU (США)
- Даниэль Рётлисбергер (координатор сферы обслуживания), Swisscom (Швейцария)
- Сигитас Рокас, NRD CIRT (Литва)
- Мэри Росселл, Intel (США)
- Робин М. Руфл (сокоординатор сферы обслуживания), CERT/CC, SEI, CMU (США)
- Дезире Захер, Finanz Informatik (Германия)
- Красимир Т. Цветанов, Fastly (США)
- Марк Зайчек (сокоординатор сферы обслуживания), CERT/CC, SEI, CMU (США)

ПРИЛОЖЕНИЕ 2. Термины и определения

В настоящем разделе даются определения некоторых терминов, используемых в концепции предоставления услуг CSIRT.

Действие – описание способа осуществления какого-либо процесса на различных уровнях деятельности группы.

Бюллетень безопасности[9] – сообщение или бюллетень, содержащие информацию, рекомендации или предупреждения относительно уязвимости продукта.

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

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.

Общеизвестные уязвимости и незащищенность[10] **(CVE)** – перечень известных уязвимостей с указанием идентификационного номера, описанием и по меньшей мере одной ссылкой на публичный источник. Используется в качестве стандартного идентификатора изучаемых уязвимостей.

Система оценки общеизвестных уязвимостей[11] **(CVSS)** – количественная оценка, отражающая степень серьезности уязвимости.

Перечень общеизвестных слабых мест[12] **(CWE)** – официальный перечень категорий слабых мест в программном обеспечении, применяемый для описания слабых мест в архитектуре, проектировании или кодах программного обеспечения; выступает в качестве стандартного количественного показателя для инструментальных средств по защите программного обеспечения, работающих с такими слабыми местами, а также в качестве общего базового стандарта при выявлении слабых мест, смягчении их воздействия и предупреждении их возникновения.

Клиентура – определенная группа физических лиц и/или организаций, имеющих доступ к конкретному набору услуг, которые предоставляет CSIRT.

Источник контекстуальных данных – источник данных, представляющий в контексте конкретные сведения, например об идентичности, ресурсе или событии в области информационной безопасности. Примерами могут служить базы данных о пользователях, перечни ресурсов, службы блокирования IP-адресов или информация об угрозах.

9 ISO/IEC 29147:2014, Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.1.
10 https://cve.mitre.org/
11 https://www.first.org/cvss/
12 https://cwe.mitre.org/about/index.html

Скоординированный процесс раскрытия информации об уязвимости – термин применяется в отношении процедуры раскрытия информации, предусматривающей меры координации. Источник: ISO/IEC 29147:2018, Terms and definitions.

Координатор[13] – дополнительный участник, который может оказывать помощь поставщикам и лицам, обнаруживающим уязвимости, в обработке и раскрытии информации об уязвимости.

Модель обнаружения – конкретная ситуация, выявляемая в рамках сферы обслуживания по управлению событиями в сфере информационной безопасности. Термин возник в сфере разработки программного обеспечения, однако сегодня широко используется специалистами по выявлению уязвимостей.

Эмбарго – приостановка публикации сведений об уязвимости до тех пор, пока затронутые поставщики не смогут выпустить обновления для систем безопасности, принять компенсационные меры или предложить обходные варианты в целях защиты клиентов.

Лицо, обнаруживающее уязвимости[14], – физическое лицо или организация, выявляющие потенциальную уязвимость продукта или онлайновой услуги. Следует отметить, что к числу таких лиц могут относиться исследователи, журналисты, компании, занимающиеся проблемами безопасности, хакеры, пользователи, государственные органы или координаторы.

Функция – действие или комплекс действий для достижения цели в рамках той или иной услуги, также может быть определена как набор соответствующих мер[15]; выполнять **функцию** – выполнять конкретное действие, работу, операцию[16].

Событие в сфере информационной безопасности – наблюдаемое событие в IT-среде, связанное с безопасностью, например вход в систему пользователя или IDS-предупреждение. События в сфере информационной безопасности, как правило, оставляют определенные следы, например запись с результатами аудита или запись в файле регистрации, которые могут быть собраны и проанализированы в рамках сферы обслуживания по управлению событиями в сфере информационной безопасности.

Инцидент в сфере информационной безопасности[17] – любое неблагоприятное событие в сфере информационной безопасности (или комплекс событий в сфере информационной безопасности), свидетельствующее о нарушении какого-либо аспекта информационной безопасности пользователя, системы, организации и/или сети. Разные организации могут по-разному определять инциденты в сфере информационной безопасности, но, как правило, к их числу относят:

- потерю конфиденциальности информации;
- нарушение целостности информации;

[13] ISO/IEC 30111:2013, Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.1.
[14] ISO/IEC 29147:2014, Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.3.
[15] Источник: https://www.merriam-webster.com/dictionary/function
[16] Источник: https://www.dictionary.com/browse/function
[17] На основании RFC2350 вместо понятия "безопасность ИТ" использовано понятие "информационная безопасность", https://tools.ietf.org/html/rfc2350.0.

- отказ в обслуживании;
- использование услуги, систем или информации в неправомерных целях;
- повреждение систем.

Инцидентом в сфере информационной безопасности можно считать атаку, даже если благодаря должным мерам защиты она оказалась неудачной.

Ключевой показатель деятельности[18] **(KPI)** – измеряемый показатель эффективности компании в достижении ключевых целей хозяйственной деятельности. Организации применяют KPI на разных уровнях для оценки успешности достижения своих целевых показателей.

Зрелость – показатель, демонстрирующий, 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. Возможности организации определяются охватом и качеством установленных принципов политики и документации, а также способностью выполнять установленные процедуры.

Открытый исходный код – разработки, которые лицензируются таким образом, что это позволяет их свободно распространять и вносить в них изменения в том случае, если их исходный код является общедоступным, распространяется бесплатно, без ограничений для любых лиц, групп или сфер деятельности и является технологически нейтральным. Программное обеспечение с открытыми исходными кодами часто поддерживается сообществом лиц или структурами, которые совместно его создают и поддерживают.

Продукт[19] – система, произведенная или разработанная для продажи или бесплатного распространения.

Устранение[20] **(или исправление)** – изменения, вносимые в продукт или онлайновую услугу в целях устранения или уменьшения уязвимости. Устранение уязвимости, как правило, происходит путем замены двоичного файла, изменения конфигурации или корректировки и перекомпиляции исходного кода. Устранение уязвимости описывается различными понятиями, включая корректировку, исправление, обновление, оперативное исправление и повышение статуса. Меры по уменьшению уязвимости также называют обходными вариантами и контрмерами.

Ответственное раскрытие информации – термин, применяемый в отношении процедуры или модели, в рамках которой раскрытие информации об уязвимости происходит лишь спустя некоторое время, необходимое для устранения уязвимости (исправления или корректировки). Этот термин не всегда означает то же самое, что и термин "скоординированный процесс раскрытия информации об уязвимости".

[18] https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator
[19] ISO/IEC 29147:2014, Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.5.
[20] ISO/IEC 29147:2014, Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.6.

Риск[21] – "влияние неопределенности на цели". В этом определении к числу неопределенностей относятся события (которые могут произойти либо не произойти), а также неопределенности, вызванные неоднозначностью информации или ее отсутствием.

Принятие риска[22] – стратегия реагирования на риск, согласно которой группа, работающая над проектом, принимает решение признать факт наличия риска и не предпринимать никаких действий до тех пор, пока риск не реализуется.

Реестр рисков[23] – документ, в котором зафиксированы результаты анализа рисков и планирования реагирования на риски.

Услуга – комплекс узнаваемых, связанных между собой действий, направленных на достижение конкретного результата. Такие результаты могут быть ожидаемы клиентами или заинтересованной стороной той или иной структуры или востребованы ими или от их имени.

Соглашение об уровне обслуживания (SLA) – договор между поставщиком услуг (внутренним или внешним) и конечным пользователем, определяющий уровень обслуживания, который, как ожидается, будет обеспечивать поставщик услуг.

Заинтересованные стороны[24] – физические лица или группы, определяющие или модифицирующие сферы обслуживания или услуги и обеспечивающие следование соответствующей стратегии информирования об услуге, а также группы, могущие извлечь выгоду из предоставляемых услуг.

Задачи – перечень действий, которые должны быть осуществлены для выполнения конкретной функции.

Поставщик[25] – лицо или организация, разработавшие продукт или услугу либо отвечающие за их сопровождение.

Уязвимость[26] – слабое место в программном обеспечении, компьютерном оборудовании или онлайновой услуге, которое может быть объектом эксплуатации.

[21] ISO 31000:2009/ ISO Guide 73:2002, Risk management– rinciples and guidelines – Terms/Definitions 2.1.
[22] The Project Management Body of Knowledge (PMBOK) Guide and Standards.
[23] The Project Management Body of Knowledge (PMBOK) Guide and Standards.
[24] Architecture Content Framework.
[25] ISO/IEC 30111:2013, Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.7.
[26] ISO/IEC 30111:2013, Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.8.

ПРИЛОЖЕНИЕ 3. Вспомогательные материалы

Alberts, David S., et.al. Understanding information age warfare. In *DOD Command and Control Research Program Publication Series*. ADA395859. Booz Allen & Hamilton, McLean, VA. 2001.
https://apps.dtic.mil/docs/citations/ADA395859

Barford P., et al. (2010) Cyber SA: Situational Awareness for Cyber Defense. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, 2010. Boston, MA. ISBN 978-1-4419-0140-8_1
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_1

Boyd, John R. Destruction and Creation. Goal Systems International. September 3, 1976.
http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

Cartwright, James E. Joint Concept of Operations for Global Information Grid NetOps. *United States Strategic Command*. PDF August 10, 2005. Homeland Security Digital Library. August 10, 2005.
https://www.hsdl.org/?view&did=685398

Committee on National Security Systems Instruction CNSSI 4009. *Committee on National Security Systems Website.* June 23, 2019 [accessed].
https://www.cnss.gov/cnss/

Cybersecurity Situation Awareness. *The MITRE Corporation Website.* June 25, 2019 [accessed].
https://www.mitre.org/capabilities/cybersecurity/situation-awareness

Endsley, Mica R. Toward a theory of situation awareness in dynamic systems. *Human factors* Volume 37. Number 1. March 1995 Pages 32-64.
https://journals.sagepub.com/doi/10.1518/001872095779049543

FIRST *Product Security Incident Response Team (PSIRT) Services Framework*, Version 1.0, 2018. North Carolina: First.org, 2018.
https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0

FIRST Vulnerability Reporting and Data eXchange SIG (VRDX-SIG). 2013-2015. North Carolina: First.org, 2015.
https://www.first.org/global/sigs/vrdx/

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.0, 2017. North Carolina: First.org, 2017.
https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

Hawk, Robert. Situational Awareness in Cyber Security. [blog post]. *Hawk's Posts: Security Essentials from Robert Hawk.* June 11, 2015.
https://www.alienvault.com/blogs/security-essentials/situational-awareness-in-cyber-security

Householder, Allen D.; Wassermann, Garret; Manion, Art; King, Christopher. *The CERT® Guide to Coordinated Vulnerability Disclosure*. CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. 2017.
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Householder, Alan. Vulnerability Discovery for Emerging Networked Systems [blog post]. *Vulnerability discovery techniques*. November 20, 2014.
https://insights.sei.cmu.edu/cert/2014/11/-vulnerability-discovery-for-emerging-networked-systems.html

International Organization for Standardization. *Information technology – Security techniques – Vulnerability disclosure.* Second Edition. ISO/IEC 29147:2018. Geneva, Switzerland: ISO: IEC. 2018.
https://www.iso.org/standard/72311.html

International Organization for Standardization. *Information technology – Security techniques – Vulnerability handling processes*. First Edition. ISO/IEC 30111:2013. Geneva, Switzerland: ISO: IEC. 2013.
https://www.iso.org/standard/53231.html

Jajodia, Sushil, et al., (Eds.). *Cyber Situational Awareness: Issues and Research*. Part of the Advances in Information Security book series (ADIS, volume 46). 2010. ISBN 978-1-4419-0140-8
https://link.springer.com/book/10.1007/978-1-4419-0140-8

Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001. ISBN: 9783831100590.

Kossakowski; Klaus-Peter & Stikvoort, Don. *A Trusted CSIRT Introducer in Europe*. Amersfoort, Netherlands: M&I/Stelvio, February, 2000.
http://www.ti.terena.nl/process/ti-v2.pdf

Manion, Art & Householder, Alan. *Vulnerability Analysis.* CERT Coordination Center (CERT/CC). May 30, 2019.
https://vuls.cert.org/

McGuinness, B. &, Foy, L. A subjective measure of SA: The crew awareness rating scale (cars). In Kaber, D.B.; Endsley, M.R.; p. 286-291. *Proceedings of the First Human Performance, situation awareness and automation conference; user-centered design for the new millennium*. Savannah, Georgia, October 2000.

Salerno, John; Hinman, Michael & Boulware, Douglas. Situation awareness model applied to multiple domains. In *Proceedings of the Defense and Security Conference*, Orlando, FL, March 2005.
https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5813/0000/A-situation-awareness-model-applied-to-multiple-domains/10.1117/12.603735.full?SSO=1

Stone, Steve. Data to Decisions for Cyberspace Operations*. The MITRE Corporation Website*. January 2016.
https://www.mitre.org/publications/technical-papers/data-to-decisions-for-cyberspace-operations

Tadda G.P., Salerno J.S. (2010) Overview of Cyber Situation Awareness. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, Boston, MA. 2010.
ISBN 978-1-4419-0140-8
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_2

West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. CMU/SEI-98-HB-001. Software Engineering Institute, Carnegie Mellon University. 1998.
http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

ПРИЛОЖЕНИЕ 4. Обзор всех услуг, предоставляемых CSIRT, и связанных с ними функций

СФЕРА ОБСЛУЖИВАНИЯ
Управление событиями в сфере информационной безопасности

Мониторинг и обнаружение
- Управление журналами регистрации и датчиками
- Управление моделями обнаружения
- Управление контекстуальными данными

Анализ событий
- Корреляция
- Классификация

СФЕРА ОБСЛУЖИВАНИЯ
Управление инцидентами в сфере информационной безопасности

Получение отчетов об инцидентах в сфере информационной безопасности
- Прием отчетов об инцидентах в сфере информационной безопасности
- Сортировка и обработка отчетов об инцидентах в сфере информационной безопасности
- Работа с отчетами об инцидентах в сфере информационной безопасности

Анализ инцидентов в сфере информационной безопасности
- Сортировка инцидентов в сфере информационной безопасности (приоритизация и категоризация)
- Сбор информации
- Координация подробного анализа
- Анализ основных причин инцидента в области информационной безопасности
- Сопоставление инцидентов

Анализ артефактов и данных экспертиз
- Анализ мультимедийной информации и поверхности носителя информации
- Обратный инжиниринг
- Анализ в ходе выполнения и/или динамический анализ
- Сравнительный анализ

Смягчение и преодоление последствий
- Разработка плана реагирования
- Меры индивидуального характера и локализация
- Восстановление системы
- Содействие другим структурам, занимающимся проблемами информационной безопасности

Координация реагирования на инциденты в сфере информационной безопасности
- Связь
- Рассылка уведомлений
- Рассылка актуальной информации
- Координация деятельности
- Представление отчетов
- Связь со средствами массовой информации

Поддержка управления в кризисных ситуациях
- Информирование клиентов

СФЕРА ОБСЛУЖИВАНИЯ
Управление уязвимостями

Выявление/изучение уязвимостей
- Обнаружение уязвимости в ходе реагирования на инцидент
- Обнаружение информации об уязвимости в общедоступном источнике
- Исследование уязвимостей

Получение отчетов об уязвимостях
- Прием отчета об уязвимости
- Сортировка и обработка отчета об уязвимости

Анализ уязвимостей
- Сортировка уязвимостей (подтверждение и классификация)
- Анализ основных причин уязвимости
- Разработка методов устранения уязвимости

Координация обмена информацией об уязвимостях
- Уведомление/представление отчетов об уязвимостях
- Координация действий заинтересованных сторон, занимающихся проблемами уязвимости

Раскрытие информации об уязвимостях
- Разработка политики раскрытия информации об уязвимостях и обслуживание инфраструктуры
- Оповещение/передача данных/распространение информации об уязвимостях
- Обратная связь по итогам раскрытия информации об уязвимостях

Реагирование на факторы уязвимости
- Обнаружение/сканирование уязвимостей
- Устранение уязвимостей

СФЕРА ОБСЛУЖИВАНИЯ
Осведомленность о ситуации

Получение данных
- Разработка единой политики, ее уточнение и предоставление рекомендаций по ее реализации
- Привязка ресурсов к функциям, должностям, действиям и ключевым рискам
- Сбор данных
- Обработка и подготовка данных

Анализ и синтез
- Прогнозирование и выводы
- Обнаружение событий (путем оповещения и/или поиска)
- Воздействие на ситуацию

Коммуникация
- Внутренние и внешние коммуникации
- Представление отчетов и рекомендаций
- Осуществление

СФЕРА ОБСЛУЖИВАНИЯ
Передача знаний

Повышение осведомленности
- Проведение исследований и обобщение информации
- Разработка материалов для составления отчетов и повышения осведомленности
- Распространение информации
- Информационно-разъяснительная работа

Профессиональная подготовка и обучение
- Сбор информации о потребностях в отношении знаний, навыков и способностей
- Разработка образовательных и учебных материалов
- Предоставление контента
- Наставничество
- Повышение квалификации сотрудников CSIRT

Практические занятия
- Анализ требований
- Определение формата и создание среды
- Разработка сценария
- Проведение практического занятия
- Обзор результатов практического занятия

Консультирование по техническим вопросам и вопросам политики
- Содействие управлению рисками
- Содействие разработке планов по обеспечению непрерывной деятельности и преодолению последствий чрезвычайных ситуаций
- Поддержка политики
- Консультирование по техническим вопросам

	• Представление отчетов о статусе информационной безопасности • Информирование о решениях стратегического характера			