Весна 2020 года

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

Версия 1.1

Уведомление. В настоящем документе приводится описание методов 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, причиненный в результате использования этой информации или в связи с ее использованием.

Содержание

Концепция предоставления услуг PSIRT

Цель

Концепции предоставления услуг – это документы высокого уровня, содержащие подробное описание возможных услуг, которые могут предоставляться группами реагирования на инциденты в сфере компьютерной безопасности (CSIRT) и группами реагирования на инциденты в сфере безопасности продукции (PSIRT). Разработчиками этих документов являются признанные специалисты из экспертного сообщества FIRST. FIRST стремится использовать материалы, получаемые от всех секторов, включая группы CSIRT с полномочиями общенационального уровня, CSIRT частного сектора, PSIRT, а также другие заинтересованные стороны. Предполагалось, что эти документы будут служить основой для разработки новых учебных материалов. Однако сегодня они используются гораздо шире, например, для определения исходного каталога услуг, предоставляемых новыми группами.

В ходе разработки концепции предоставления услуг CSIRT стало очевидно, что PSIRT предоставляют услуги совсем иного рода и, как правило, работают совсем в других условиях. Поэтому было принято решение подготовить отдельный документ по PSIRT. Поскольку эти два документа имеют много общего, в дальнейшем они будут увязаны друг с другом. Руководство разработкой концепций осуществляет Консультативный совет по вопросам образования.

Концепции создавались для помощи организациям в формировании, поддержании и наращивании потенциала их CSIRT или PSIRT. Концепции, которые носят рекомендательный характер, содержат сведения о различных моделях, возможностях, услугах и результатах. Соответственно группы вправе использовать собственные модели и создавать возможности, отвечающие уникальным потребностям их заинтересованных сторон. Концепции направлены на оказание содействия группам реагирования на инциденты в сфере безопасности (SIRT) путем определения основных обязанностей, предоставления рекомендаций по вопросам создания потенциала для выполнения этих обязанностей и предложения способов, которыми группы могли бы обеспечить дополнительные преимущества организациям, в рамках которых они работают, и информировать их об этих преимуществах.

Введение

Группа реагирования на инциденты в сфере безопасности продукции (PSIRT) – это действующее в рамках организации подразделение, главной задачей которого является выявление, оценка и устранение рисков, связанных с уязвимостями защиты ее продукции, в том числе предложений, решений, компонентов и/или услуг, которые организация производит и/или продает.

Должным образом организованная PSIRT не является независимой структурой, которая не связана с разработкой продукции, производимой организацией. Напротив, такая группа представляет собой составную часть более широкой программы организации по безопасному проектированию. Это подразделение обеспечивает включение мер по обеспечению безопасности в цикл безопасной разработки (SDL) продукции.

Реагирование на инциденты в сфере безопасности продукции нередко ассоциируется с этапом обслуживания, поскольку информация о большинстве уязвимостей защиты продукции поступает в виде сообщений о несоответствии требованиям к качеству продукции после ее выхода на рынок. Вместе с тем PSIRT может сыграть определенную роль и раньше – при сборе информации о потребностях на этапах создания архитектуры, проектирования, планирования и моделирования риска. Деятельность PSIRT может быть полезной и в плане представления рекомендаций по выявленным в организации проблемам безопасности и надзора за их устранением.

Структура концепции предоставления услуг PSIRT

СФЕРЫ ОБСЛУЖИВАНИЯ – УСЛУГИ – ФУНКЦИИ – ПОДФУНКЦИИ

СФЕРЫ ОБСЛУЖИВАНИЯ

Сферы обслуживания объединяют услуги, имеющие общую характеристику. Они помогают упорядочить услуги путем их распределения по категориям верхнего уровня, что обеспечивает их более четкое понимание. Спецификация для каждой сферы обслуживания включает в себя описательную часть – текст общего характера с описанием сферы обслуживания, а также перечень услуг в рамках данной сферы.

УСЛУГИ

Услуга – это комплекс распознаваемых, связанных между собой действий, направленных на достижение того или иного результата и проводимых от имени или в интересах клиентуры группы реагирования на инциденты.
Определение услуги дается по следующей схеме:

- описательная часть с описанием характера услуги;

- раздел "Цель и результат", в котором описываются предназначение и измеримые результаты услуги.

ФУНКЦИИ

Функция – это действие или набор действий, направленных на достижение цели той или иной услуги. Любая функция может использоваться совместно и применяться в рамках нескольких услуг.

Определение функции дается по следующей схеме:

- описательная часть с описанием функции;
- раздел "Цель и результат", в котором описываются предназначение и измеримые результаты услуги;
- перечень подфункций, которые могут выполняться в составе той или иной функции.

ПОДФУНКЦИЯ

Подфункция – это действие или набор действий, направленных на достижение цели той или иной функции. Любая подфункция может использоваться совместно и применяться в рамках нескольких функций.

Чем PSIRT отличается от CSIRT

Главным признаком, отличающим PSIRT какой-либо организации от других групп реагирования на инциденты в сфере безопасности, действующих в рамках той же организации, например CSIRT, является ориентация на продукты. В центре внимания ведомственной CSIRT обычно находится безопасность компьютерных систем и/или сетей, образующих инфраструктуру этой организации.

Хотя между ведомственной CSIRT и PSIRT существуют важные различия, необходимо учитывать, что между этими двумя группами имеется синергическая связь. Важно иметь в виду, что PSIRT работает не в отрыве от других подразделений организации, и в настоящем документе мы будем выделять области сотрудничества и взаимодействия, которые следует развивать.

Организационная структура PSIRT

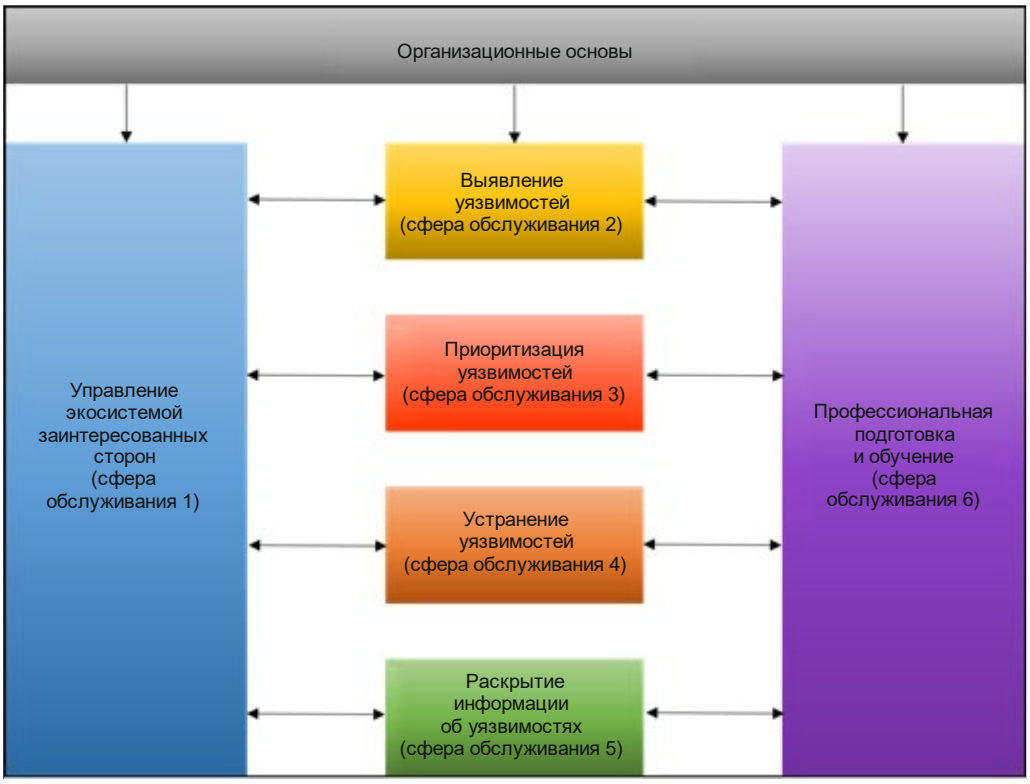


Рисунок 1. Организационная структура

PSIRT могут быть столь же уникальными и разнообразными, как и продукты, которые они помогают защищать. Организации, действующие в одном и том же секторе или в одной и той же отрасли, могут иметь разные финансово-хозяйственные характеристики, модели операционной деятельности, ассортимент продукции, организационные структуры и стратегии разработки продуктов. Поэтому не существует единой стандартной стратегии реагирования на инциденты в сфере безопасности продукции или единой структуры группы, обязательных для всех организаций. Тем не менее большинство компаний используют три модели PSIRT – распределенную, централизованную и гибридную.

Распределенная модель

Распределенная модель предполагает наличие небольшой основной PSIRT, члены которой совместно с представителями групп разработчиков продуктов занимаются устранением уязвимостей защиты в продуктах. В рамках этой модели небольшой операционный отдел PSIRT выполняет несколько основных обязанностей:

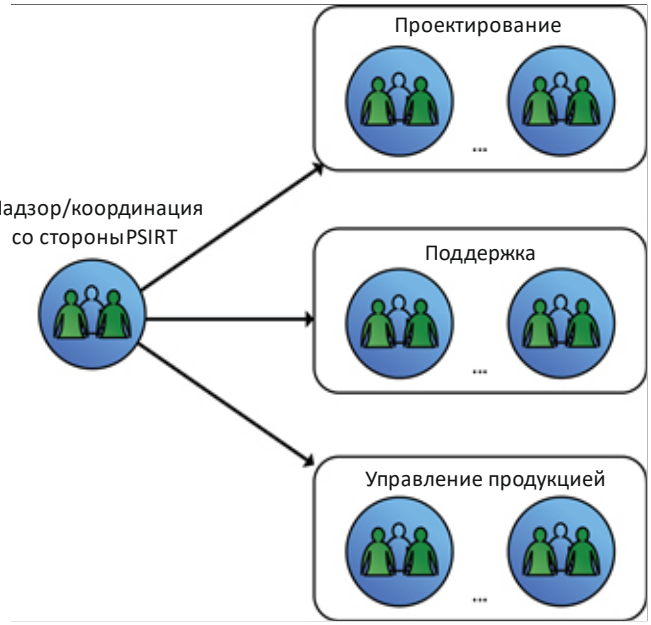


Рисунок 2. Распределенная модель

- разработка политики, процессов, процедур и рекомендаций по приоритизации, анализу, устранению уязвимостей защиты и распространению информации об исправлениях, мерах по уменьшению влияния или иной рекомендательной информации об устранении этих уязвимостей;
- создание в организации структуры (многоуровневой), в состав которой входят представители, ответственные за проектирование безопасности продукции;
- обеспечение руководства и консультирования по вопросам устранения уязвимостей защиты продуктов и потенциального риска для предприятия;
- выполнение функций центра сбора данных об уязвимостях защиты в тех случаях, когда наличие единого центра контроля способствует экономии за счет масштабов;
- информирование ответственного за разработку продукта/менеджера по продукту и инженера по безопасности о новых уязвимостях защиты, содействие в разработке планов устранения уязвимостей, а также подготовку/публикацию сообщений об исправлениях или мерах по уменьшению влияния, в том числе об управлении инцидентами.

Распределенная модель может быть выгодна для организации с большим и разнообразным ассортиментом продукции, поскольку затраты на выполнение функций PSIRT распределяются по всей организации. Эта модель позволяет также масштабировать работу PSIRT за счет привлечения квалифицированных специалистов из групп по проектированию продуктов.

Недостатком распределенной модели PSIRT является то, что лица, отвечающие за приоритизацию и устранение уязвимостей защиты, не контролируются напрямую операционным отделом PSIRT и не отчитываются перед ним.

Централизованная модель

При использовании централизованной модели в штате PSIRT числится больше сотрудников, которые привлекаются из различных подразделений и отчитываются перед одним или несколькими руководителями высшего звена, отвечающими за безопасность производимой организацией продукции. Эта модель может иметь примерно следующую структуру.

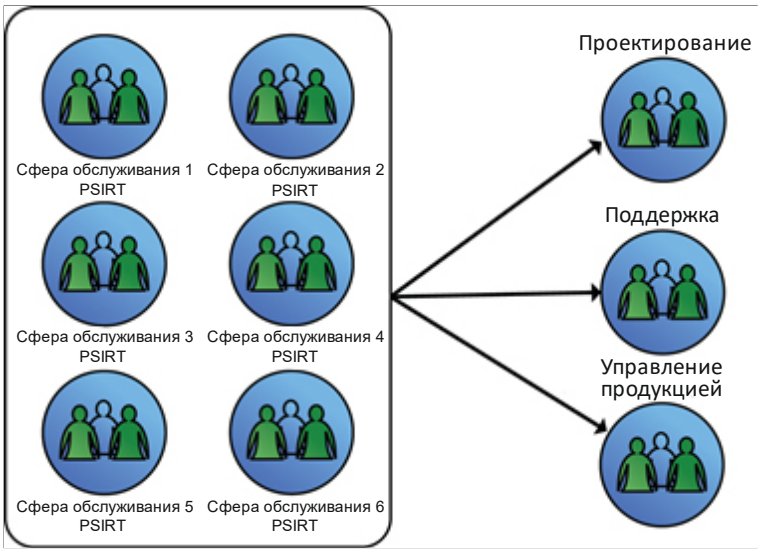


Рисунок 3. Централизованная модель

- *Отдел PSIRT по управлению программами*: разрабатывает политику, процессы, процедуры и рекомендации по приоритизации, анализу, устранению уязвимостей защиты и распространению информации об исправлениях, меры по смягчению последствий или иной рекомендательной информации об устранении этих уязвимостей. Осуществляет руководство деятельностью PSIRT в целом и системой отслеживания ошибок, а также является представителем PSIRT в рамках организации.
- *Отдел PSIRT по сбору и приоритизации информации по безопасности:* осуществляет мониторинг различных внешних источников уязвимостей защиты, проводит оценку первоначального воздействия уязвимостей защиты на ассортимент выпускаемой организацией продукции.

- *Отдел PSIRT по устранению инцидентов и распространению информации:* передает исправления программного кода, обеспечивающие устранение уязвимостей защиты, непосредственно в группы по проектированию продуктов.

Эта модель успешно применяется в небольших организациях и/или в организациях с однородным ассортиментом продукции. Модель предполагает сосредоточение в одном подразделении организации специалистов, обладающих высокой квалификацией и большим опытом в сфере безопасности. Недостатком этой модели являются расходы на содержание централизованной специализированной группы, которую нельзя масштабировать в случае расширения или диверсификации ассортимента продукции.

Гибридная модель

- Гибридная модель – это вариант, сочетающий характеристики как распределенной, так и централизованной модели. Организация может захотеть применить некоторые свойства и особенности обеих этих моделей, создав гибрид, учитывающий следующие факторы:
- корпоративную структуру и размер организации;
- размер и разнообразие ассортимента продукции;
- стратегию разработки продуктов.

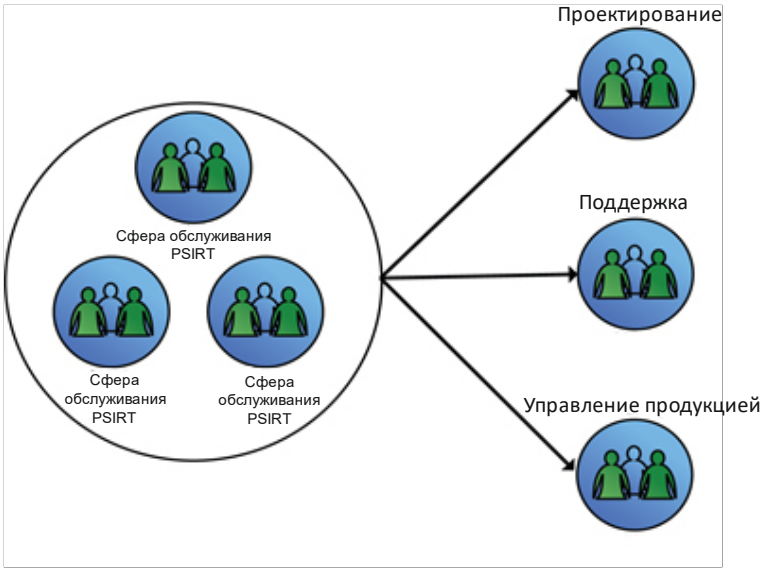


Рисунок 4. Гибридная модель

Прочие соображения

Для PSIRT важно обладать достаточной самостоятельностью, чтобы занимать независимую и объективную позицию в отношении уязвимостей защиты продукции,

производимой организацией. Соответственно разрабатывая стратегию и структуру PSIRT, организации следует рассмотреть вопрос об оптимальных путях интеграции группы в организацию и о структуре ее отчетности. Важно, чтобы PSIRT была подотчетна должностному лицу компании, которое подтверждало бы ее полномочия.

По мере роста PSIRT и повышения уровня ее зрелости, равно как и по мере изменения стоящих перед ней задач, состав и структура отчетности группы могут меняться. Движущей силой изменений и развития PSIRT являются ее ключевые заинтересованные стороны, а также, к сожалению, последствия серьезной уязвимости для широкого спектра базы заинтересованных сторон организации. Круг таких заинтересованных сторон часто зависит от той модели, которой придерживается организация, а также от ее размеров.

Заинтересованные стороны

Учет нужд и потребностей заинтересованных сторон играет важнейшую роль при определении стратегии и структуры PSIRT. Модель, по которой организация создает PSIRT, может стать фактором, определяющим, кто именно является заинтересованной стороной и каким влиянием обладают эти стороны. Большое значение имеет поддержание на постоянной основе конструктивных взаимоотношений. Об экосистеме заинтересованных сторон и о работе с ними подробнее рассказывается в разделе Сфера обслуживания 1. Управление экосистемой заинтересованных сторон.

Еще одно обстоятельство, которое необходимо принимать во внимание, создавая группу реагирования на инциденты в сфере безопасности продукции и разрабатывая ее стратегию, – это факторы влияния. Это не то же самое, что заинтересованные стороны, поскольку, говоря о заинтересованных сторонах, мы имеем в виду отдельных людей или группы людей, в то время как факторы влияния – это отраслевые и правительственные стандарты, законы, нормативные акты и тенденции. Эти факторы влияния могут предъявлять более жесткие требования к формированию, стратегиям, политике и функциональным характеристикам PSIRT, нежели заинтересованные стороны.

Чем занимается PSIRT?

Применяемая модель определяет сферу охвата и оперативную деятельность PSIRT, но это не всегда те изменения в действиях, которые организации необходимо предпринять для устранения уязвимостей защиты ее продукции. Модель уточняет круг возможностей, действий и ответственности, непосредственно относимых к сфере ведения PSIRT, а не распределенных по всей структуре организации.

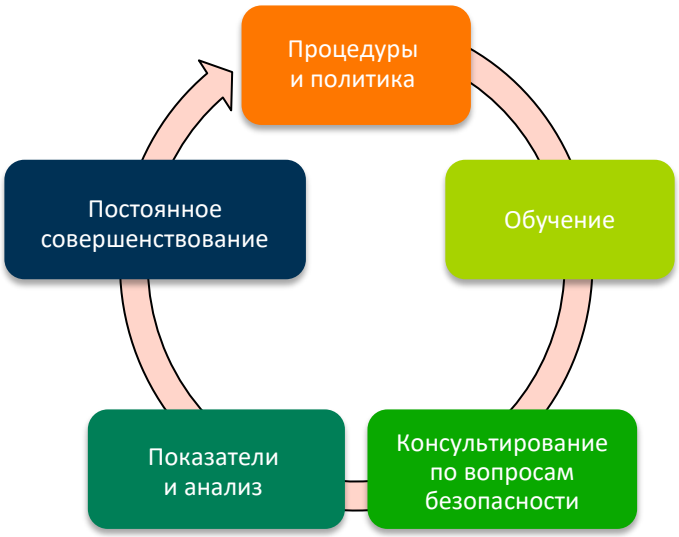


Рисунок 5. Основные направления деятельности PSIRT

Постоянная разработка процедур и политики

PSIRT определяет политику организации в сфере обеспечения безопасности продукции. Требования со стороны PSIRT определяются и диктуются потребностями бизнеса, а не наоборот. Прежде чем приступать к осуществлению разработанной PSIRT политики, ее необходимо обсудить с руководством организации и получить его поддержку для повышения ее значимости. Утвержденная политика должна дополняться четкими процедурами, следование которым обеспечит соблюдение организацией принципов этой политики.

Обучение заинтересованных сторон

Наряду с разработкой политики и процедур PSIRT следует создать системы организации работы и управления, которые упростили бы осуществление и соблюдение мер, необходимых для устранения уязвимостей защиты продукции. Это поможет организации утвердить обеспечение безопасности продукции в качестве составной части своей повседневной хозяйственной деятельности.

Самая грубая ошибка, которую можно допустить, приступая к организации работы и осуществлению политики и процедур PSIRT, – это рассматривать их как отдельную зону ответственности или отдельное требование. Поэтому чрезвычайно важно обучить всех сотрудников организации основам обеспечения безопасности продукции и проинформировать их о той роли, которую они могут в этом сыграть. Необходимо, чтобы все без исключения сотрудники организации были включены в этот процесс и обеспечены

условиями и возможностями для выполнения требований, предусмотренных политикой PSIRT.

Значение количественных показателей

Крайне важно оценивать степень успешности работы группы реагирования на инциденты в сфере безопасности продукции. Отчеты о количественных показателях не определяют требования, но содействуют осуществлению программы, помогают определить потребность в ресурсах и могут помочь с выявлением областей, где есть потребность в совершенствовании процедур или инструментов. Разработка и отслеживание количественных показателей может также способствовать развитию PSIRT за счет выявления проблем или узких мест в процессе развертывания и внедрения PSIRT. Подробнее о количественных показателях, отслеживание которых может оказаться полезным, см. в разделах Услуга 1.7. Показатели для заинтересованных сторон и Услуга 5.4. Показатели уязвимости.

Определения

В настоящем документе мы даем определения некоторым используемым здесь терминам. Необходимо отметить, что термины "сферы обслуживания", "услуги" и "функции" указывают на то, что делается на том или ином уровне деятельности группы, в то время как задачи и действия указывают на то, как это делается на том или ином уровне ее деятельности. Информация по задачам и действиям публикуется в приложении и может/будет обновляться чаще.

– **Бюллетень безопасности**[1] – сообщение или бюллетень, содержащие информацию, рекомендации или предупреждения относительно уязвимости продукта.

– **Пороги ошибок** – критерии, определяющие типы ошибок, которые классифицируются как уязвимости защиты. Ошибки, соответствующие этим критериям, обрабатываются как уязвимости в рамках стандартных операционных процедур PSIRT.

– **Координатор**[2] – дополнительный участник, который может оказывать помощь поставщикам и лицам, обнаруживающим уязвимости, в обработке и раскрытии информации об уязвимости.

– **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**[3] – 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.

– **Открытый исходный код** – относится к разработкам, 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

[1] ISO/IEC 29147:2014, Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.1.

[2] ISO/IEC 30111:2013, Information technology – Security techniques–Vulnerability handling processes – Terms/Definitions 3.1.

[3] ISO/IEC 29147:2014, Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.3.

поддерживается сообществом лиц или структурами, которые совместно его создают и поддерживают.

– **Партнеры** – производители оригинального оборудования (OEM), поставщики, производители изделий собственной разработки (ODM).

– **Продукт**[4] – система, произведенная либо разработанная для продажи или бесплатного распространения.

– **Проверка качества для завершения этапа тестирования** – комплекс критериев, которые должны быть соблюдены для перехода на следующий этап разработки или выпуска продукта.

– **Устранение**[5] **(или исправление)** – изменения, вносимые в продукт или онлайновую услугу в целях устранения или уменьшения влияния уязвимости. Устранение уязвимости, как правило, происходит путем замены двоичного файла, изменения конфигурации или корректировки и перекомпилирования исходного кода. Устранение уязвимости описывается различными терминами, в частности такими, как заплатка, исправление, обновление, оперативная корректировка и модернизация. Меры по уменьшению влияния уязвимости также называются обходными приемами или контрмерами.

– **Риск**[6] – "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**[7] – стратегия реагирования на риск, согласно которой группа по проекту принимает решение признать факт наличия риска и не предпринимать никаких действий до тех пор, пока риск не реализуется.

– **Реестр рисков**[8] – документ, в котором зафиксированы результаты анализа рисков и планирования реагирования на риски.

– **Цикл обеспечения безопасности на этапах разработки (SDL) –** процесс разработки, помогающий разработчикам создавать более защищенные продукты и выполнять требования к соблюдению безопасности, снижая при этом затраты на разработку.

---

[4] ISO/IEC 29147:2014, Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.5/.

[5] ISO/IEC 29147:2014, Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.6/.

[6] ISO 31000:2009/ISO Guide 73:2002, Risk management – Principles and guidelines – Terms/ Definitions 2.1/.

[7] The Project Management Body of Knowledge (PMBOK) Guide and Standards.

[8] The Project Management Body of Knowledge (PMBOK) Guide and Standards.

– **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**[9] – применительно к PSIRT заинтересованные стороны – это группы, создающие или модифицирующие продукт или компоненты продукта, обеспечивающие следование соответствующей стратегии информирования о продукте, а также могущие извлечь выгоду из обеспечения безопасности продукции. Короче, заинтересованные стороны PSIRT либо вносят вклад в обеспечение безопасности продукции или реагирование на инциденты, либо извлекают из этого выгоду.

– **Третье лицо** – любой поставщик верхнего уровня или производитель, осуществляющий поставки комплектующих для продукта или решения/услуги.

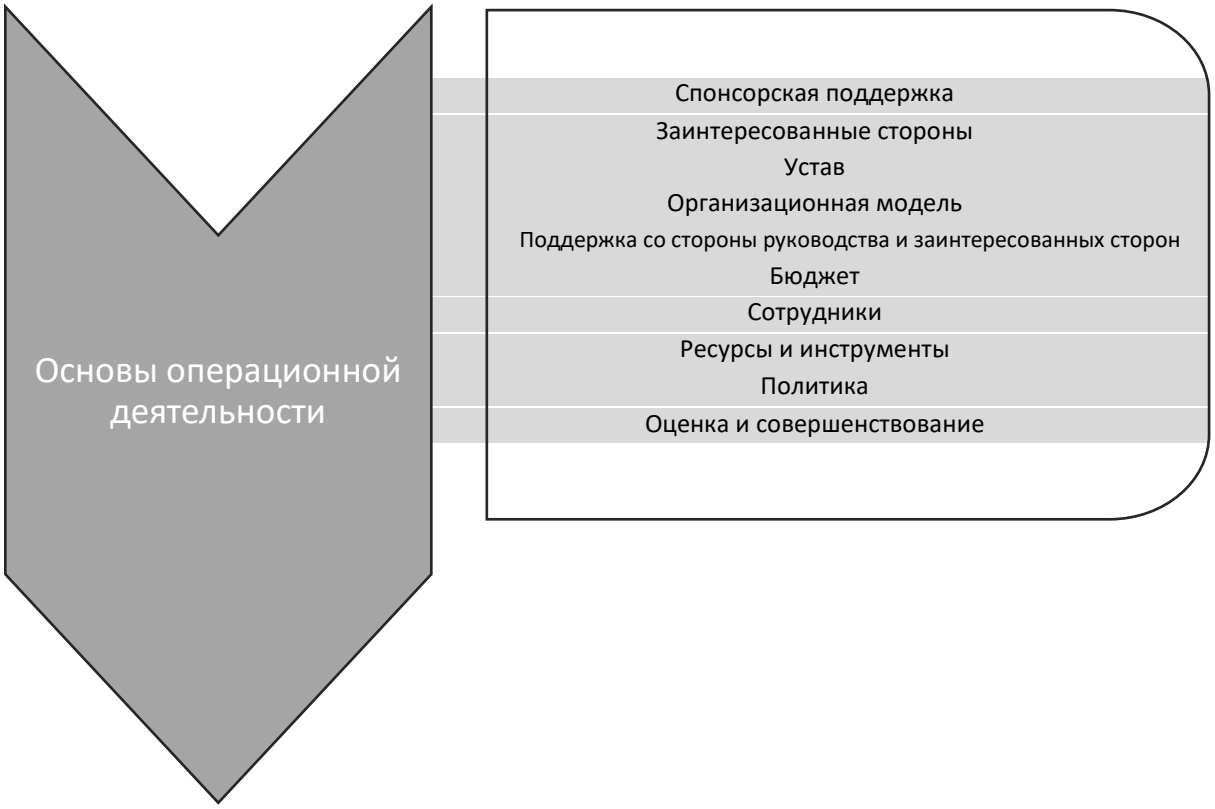
– **Поставщик**[10] – лицо или организация, разработавшие продукт или услугу либо отвечающие за их обслуживание.

– **Уязвимость**[11] – слабое место в программном обеспечении, компьютерном оборудовании или онлайновой услуге, которое может быть объектом эксплуатации.

[9] Architecture Content Framework.

[10] ISO/IEC 30111:2013, Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.7/.

[11] ISO/IEC 30111:2013, Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.8.



В этом разделе дается определение и описание основных компонентов, необходимых организации для планирования, создания и обеспечения эффективной работы PSIRT.

***Цель**: предоставить организации возможность планировать и внедрять основные компоненты для создания и обеспечения функционирования PSIRT.*

***Результат**: меры по выявлению, планированию и внедрению основных оперативных компонентов PSIRT помогают организации в создании собственной PSIRT, что позволит подготовить PSIRT к выполнению ею своей миссии и обеспечит стабильную способность компании предоставлять свои продукты и услуги определенным заинтересованным сторонам.*

I. Стратегия

A. Поддержка со стороны руководства

Заручитесь поддержкой со стороны руководства организации и лиц, принимающих ключевые решения.

***Цель**: информировать руководство организации и заручиться поддержкой (участием) со стороны ее руководителей (например, должностных лиц высшего звена, совета директоров) или других лиц, принимающих решения, чтобы создать возможности для эффективной работы PSIRT.*

***Результат**: стабильное финансирование и поддержка без зависимости от обеспечения желаемых показателей деятельности компании.*

Чтобы заручиться поддержкой со стороны руководства, организации необходимо вести информационно-разъяснительную работу с представителями руководства, предоставляя им планы и другую сопутствующую информацию, которая помогала бы им понять цель, значение, потенциальные риски уязвимостей для безопасности и выгоды, которые приносит деятельность PSIRT (см. ниже разделы "Устав PSIRT" и "Бюджет").

Дополнительную информацию см. в разделе Услуга 1.1. Взаимодействие с внутренними заинтересованными сторонами.

B. Заинтересованная сторона

Определите заинтересованные стороны и взаимоотношения, которые ваша PSIRT будет поддерживать с этими группами.

***Цель**: понять, кого PSIRT будет обслуживать и с кем она будет взаимодействовать.*

***Результат**: четко определенный список заинтересованных сторон.*

В этот список следует включить внешние заинтересованные стороны, например клиентов организации, сторонних специалистов по исследованию проблем в области безопасности, CSIRT и другие PSIRT, а также внутренние заинтересованные стороны, например разработчиков программного обеспечения, инженеров, специалистов по поддержке клиентов, юристов, а также специалистов по связям с общественностью/корпорациями/средствами массовой информации.

Дополнительную информацию см. в разделе Сфера обслуживания 1. Управление экосистемой заинтересованных сторон (Услуга 1.1. Взаимодействие с внутренними заинтересованными сторонами, Услуга 1.2. Взаимодействие с сообществом лиц, обнаруживающих уязвимости, Услуга 1.3. Взаимодействие с сообществами и организациями и Услуга 1.4. Работа с заинтересованными сторонами нижнего уровня).

C. Устав PSIRT

Разработайте устав или иной документ (например, стратегический план, план осуществления или документ о концепции деятельности).

***Цель**: определить, описать и оформить документально основные программные элементы деятельности PSIRT.*

***Результат**: документ с описанием причин создания/основания PSIRT и желательных результатов ее деятельности.*

В уставе PSIRT/плане ее работы следует описать:

- миссию PSIRT (должна поддерживать миссию организации и согласовываться с ней);
- цель и распределение ролей и обязанностей;
- продукты и услуги (например, сбор сообщений об уязвимостях, разработка исправлений или корректировок, распространение уведомлений об исправлениях).

D. Организационная модель

Определите и документально оформите организационную структуру и модель, которые будет использовать PSIRT.

***Цель**: определить, описать и оформить документально организационную модель, в соответствии с которой будет работать PSIRT.*

***Результат**: создание четко определенной структуры группы с документально оформленным распределением ролей и обязанностей.*

В документально оформленной организационной модели должна быть описана структура внутренней отчетности PSIRT и определен орган, которому подчиняется PSIRT. Описание некоторых наиболее распространенных организационных моделей (например, распределенной модели, централизованной модели, гибридной модели) см. в разделе "Организационная структура PSIRT". Дополнительную информацию см. в разделе Услуга 1.5. Координация деятельности по информированию об инцидентах в рамках организации.

E. Поддержка со стороны руководства и заинтересованных сторон

Заручитесь поддержкой и участием со стороны руководства и внутренних заинтересованных сторон.

***Цель**: информировать руководство других подразделений организации и внутренние заинтересованные стороны и получать с их стороны поддержку и участие, что обеспечит возможность эффективной работы PSIRT.*

***Результат**: чтобы заручиться постоянной поддержкой заинтересованных сторон, им предоставляется информация об основных показателях хозяйственной деятельности.*

Дополнительную информацию см. в разделе Услуга 1.1. Взаимодействие с внутренними заинтересованными сторонами.

II. Тактика

A. Бюджет

Определите стоимость ресурсов, необходимых для работы PSIRT, и получите соответствующий объем финансовых средств для их финансирования.

***Цель**: определить, описать и оформить документально организационную модель, в соответствии с которой PSIRT будет работать и финансироваться.*

***Результат**: документально оформленные операционные затраты, расходы и модель финансирования PSIRT.*

В бюджете следует предусмотреть расходы на персонал PSIRT (заработную плату, льготы и другие расходы, связанные с обязательствами), оборудование и другие капитальные затраты (например, на системы/устройства информационных технологий, приобретение лицензий на компьютерные программы), а также смету на обучение (включая командировки).

B. Персонал

Определите объем кадровых ресурсов, необходимый для обеспечения предоставления услуг PSIRT, и привлеките квалифицированных сотрудников.

***Цель**: определить, описать и оформить документально организационную модель, в соответствии с которой PSIRT будет укомплектована кадрами.*

***Результат**: документально оформленные потребности PSIRT в кадрах.*

При этом следует определить должностное положение, а также роль и обязанности каждого сотрудника PSIRT, а также компетенции (знания, навыки и умения [ЗНУ]), которыми они должны обладать, равно как и любые иные требования применительно к их должности (например, уровень образования, опыт, свидетельства о повышении квалификации). Соответствующие позиции или должности могут замещать штатные сотрудники, поставщики, подрядчики или представители этих категорий в каком-либо сочетании.

В рамках штатного расписания (или в отдельном документе) следует определить и спланировать требования к прохождению подготовки, в том числе общей подготовки для всех сотрудников PSIRT и подготовки сотрудников в соответствии с выполняемыми ими ролями (например, первоначальное ознакомительное обучение/кураторство, непрерывная подготовка, обучение и повышение уровня информированности, специальная подготовка в целях повышения профессиональной квалификации).

Дополнительную информацию см. в разделе Услуга 6.1. Профессиональная подготовка сотрудников PSIRT.

C. Ресурсы и инструменты

Определите и приобретите иные необходимые ресурсы и инструменты.

***Цель**: определить и приобрести ресурсы, оборудование и инструменты, необходимые для работы PSIRT.*

***Результат**: осознанные и документально оформленные потребности PSIRT в наборе инструментов и ресурсах.*

К числу таких ресурсов и инструментов относятся:

- инфраструктура, например рабочие помещения (офисное пространство);
- инструменты/технологии/оборудование (компьютерное оборудование, программное обеспечение) (см., например, раздел Услуга 3.3. Воспроизведение уязвимостей);
- система/методы отчетности об уязвимостях (например, веб-сайт, электронная почта, телефон) (см. раздел Услуга 2.1. Прием сообщений об уязвимостях);
- защищенная связь (например, PGP/шифрование) (см. раздел Функция 1.5.2. Организация безопасной связи);
- база данных об уязвимостях/система отслеживания уязвимостей (например, см. разделы Функция 1.5.3. Обновление системы отслеживания дефектов безопасности и Функция 3.2.1. База данных лиц, обнаруживающих уязвимости).

III. Операционная деятельность

A. Политика и процедуры

Оформите документально политику, процессы и процедуры, касающиеся деятельности PSIRT.

***Цель**: определить, описать и документально оформить политику и процедуры, в соответствии с которыми PSIRT будет работать.*

***Результат**: у PSIRT будет официальная политика, описывающая полномочия PSIRT, систему управления ею и направления ее деятельность. Будут также документально оформлены процедуры/указания, описывающие порядок исполнения возложенных на группу обязанностей.*

Документально оформленные политика и процедуры обеспечивают их общее понимание всеми сотрудниками PSIRT, согласованность и воспроизводимость предоставляемых PSIRT продуктов и услуг, а также служат в качестве учебных материалов для новых сотрудников PSIRT.

B. Оценка и усовершенствование

Определите показатели для оценки эффективности и/или результативности деятельности в целях выявления областей, нуждающихся в усовершенствовании.

***Цель**: оценить на основании качественных или количественных показателей, насколько успешно работает PSIRT, и выявить области, возможно, нуждающиеся в усовершенствовании.*

***Результат**: PSIRT сможет измерять эффективность своей деятельности и определять области, которые желательно усовершенствовать.*

PSIRT следует постоянно и/или периодически оценивать на основании качественных или количественных показателей эффективность своей деятельности (предоставление своих продуктов и услуг) и выявлять любые ее области, возможно, нуждающиеся в усовершенствовании.

Показатели и методы оценки могут быть как неформальными (например, путем сбора отзывов от заинтересованных сторон), так и формальными, а сама оценка может проводиться по мере необходимости (например, при документальном оформлении накопленного опыта (см. раздел Функция 1.1.3. Процедура анализа инцидентов)) или по заранее определенному графику.

Информация, содержащаяся в настоящей концепции оказания услуг PSIRT, может стать одним из источников критериев или возможностей для оценки работы PSIRT.

Сфера обслуживания 1

В данной сфере обслуживания описываются услуги и функции, которые PSIRT может выполнять для того, чтобы надлежащим образом взаимодействовать с внутренними и внешними заинтересованными сторонами. Услуги в рамках этой сферы обслуживания предоставляются на всем протяжении инцидента или жизненного цикла процесса развития PSIRT. Задача данной сферы обслуживания – обеспечить необходимое информирование всех заинтересованных сторон PSIRT и их участие в процессе реагирования на инциденты.

Прежде чем официально приступить к предоставлению таких услуг, PSIRT должна определить заинтересованные стороны, имеющие непосредственное отношение к ее деятельности. К числу таких заинтересованных сторон относятся предприниматели и руководители компании, группы разработчиков внутри компании, внешние поставщики или разработчики компонентов и даже клиентура организации. Для упрощения процесса коммуникации весьма полезно составить таблицу с указанием связей заинтересованных сторон с конкретными продуктами/версиями. Прежде чем налаживать коммуникации с такими заинтересованными сторонами, имеет смысл узнать их точку зрения и выяснить, какими способами и методами они хотят осуществлять взаимодействие (через сетевой портал, личные сообщения по электронной почте, чаты в интернете, систему обработки обращений и т. д.). Для целей настоящего документа заинтересованные стороны разделены на несколько групп (в вашей конкретной ситуации ваша компания может

выделить и другие их группы): лица, обнаружившие уязвимость, коллеги/партнеры, подразделения компании и потребители вашей продукции.

> ***Цель**: определить процедуры и механизмы обмена информацией с отобранными заинтересованными сторонами, с которыми PSIRT может и должна взаимодействовать.*
> ***Результат**: успешное взаимодействие с экосистемой заинтересованных сторон PSIRT обеспечит своевременное поступление сообщений о выявленных уязвимостях, а также удовлетворенность заинтересованных сторон/партнеров в случаях, когда информация об уязвимостях безопасности в обязательном порядке доводится до сведения заинтересованных сторон организации.*

Услуга 1.1 Взаимодействие с внутренними заинтересованными сторонами

Рисунок 6. Взаимодействие с внутренними заинтересованными сторонами

Определите процедуры взаимодействия с внутренними заинтересованными сторонами, чтобы в случае инцидента обеспечить их информирование и получение помощи с их стороны. Успешное взаимодействие с внутренними заинтересованными сторонами позволяет повысить эффективность связей и мер реагирования за счет четкого

информирования о роли и месте PSIRT в организации и обеспечения внутренних связей между группами разработчиков продукта и аналитиками по вопросам безопасности.

***Цель**: закрепить полномочия и задачи PSIRT в отношении внутренних заинтересованных сторон для содействия эффективной координации усилий по устранению уязвимостей и обеспечению безопасности продукции.*

***Результат**: активное взаимодействие с внутренними сторонами упрощает всю деятельность PSIRT и получение желаемых результатов. Например, если дефекты выявляются сотрудниками компании, это ослабляет незамедлительно оказываемое давление в виде внешних эмбарго или внимания со стороны средств массовой информации, позволяя решать проблему в плановом порядке, выгодном для организации, ее клиентов и сообщества в целом, и сводит к минимуму риск обнародования информации о неисправленных уязвимостях.*

Функция 1.1.1 Взаимодействие с внутренними заинтересованными сторонами

Поддерживайте активный диалог с подразделениями, занимающимися разработкой, тестированием, упаковкой и техническим сопровождением предлагаемой организацией продукции. К числу внутренних заинтересованных сторон относятся не только инженеры, но и специалисты по тестированию/обеспечению качества, проверке технических характеристик выпускаемых изделий, поддержке клиентов, сбыту и маркетингу, а также другие технические специалисты в данной области.

***Цель**: обеспечить присутствие PSIRT на внутренних платформах рассылки сообщений/информации для уведомления заинтересованных лиц в организации о существовании, процедурах и функциях PSIRT.*

***Результат**: PSIRT имеет официально оформленный список внутренних заинтересованных лиц и понимает их функции и обязанности.*

Подфункция 1.1.1.1 Взаимодействие с предпринимателями и руководителями корпорации/компании

Чтобы деятельность PSIRT была эффективной, группа должна понимать текущее положение дел в компании и уметь реагировать на него. Взаимодействие с предпринимателями и руководством компании может быть полезно для PSIRT в разных отношениях. Поддержка со стороны руководства помогает легитимизировать деятельность PSIRT в рамках компании. PSIRT получает возможность доводить информацию до сведения руководства, помогая принимать взвешенные бизнес-решения. Кроме того, это дает возможность руководству компании уведомлять об изменениях политического и

организационного характера, которые могут повлечь за собой изменение миссии PSIRT.

Подфункция 1.1.1.2 Взаимодействие со службами по связям с общественностью, юридическим вопросам и корпоративным коммуникациям

Взаимодействие с подразделениями, занимающимися внутренними коммуникациями и юридическими вопросами, позволяет обеспечивать соответствие PSIRT принятым на данный момент стандартам брендирования и передачи информации, а также нормативно-правовым положениям, которые обязана соблюдать организация (например, защита персональных данных, области, находящиеся в ведении федерального правительства). Каждая из таких заинтересованных сторон имеет уникальный доступ к важным для PSIRT заинтересованным сторонам, и чтобы обеспечить эффективное сотрудничество всех сторон, необходимо налаживать каналы связи до наступления серьезных событий или инцидентов.

Подфункция 1.1.1.3 Взаимодействие со службами по отдельным видам деятельности

Взаимодействие с заинтересованными сторонами из числа разработчиков обеспечивает надлежащее документальное оформление, приоритизацию и решение проблем. Например, инженерам из группы PSIRT или ее уполномоченным представителям необходимо координировать меры по устранению уязвимостей с группой разработчиков программного обеспечения, ответственных за дефектный код. В случае инцидента такие партнерские связи помогают также быстро передавать информацию и эффективно и оперативно решать проблему. В данном случае к числу заинтересованных лиц относятся менеджеры по программам или продуктам, группы надзора за SDL, руководители проектов, специалисты по разработке продуктов и другие лица с аналогичным кругом деловых обязанностей.

Подфункция 1.1.1.4 Взаимодействие с группами разработок/инженерных решений

Инженерам из группы PSIRT необходимо координировать меры по устранению уязвимостей с группами по разработке компьютерных программ, ответственными за дефектный код. Взаимодействие с заинтересованными сторонами из числа разработчиков обеспечивает надлежащее документальное оформление, приоритизацию и решение проблем. В случае инцидента такие партнерские связи помогают также быстро передавать информацию и эффективно и оперативно решать проблему.

Подфункция 1.1.1.5 Взаимодействие со службами по работе с клиентами – отделами продаж и службами поддержки

Инженерам из группы PSIRT необходимо предоставлять разъяснения и информацию отделам по поддержке клиентов, чтобы в случае возникновения проблем и их обнародования эти структуры могли ответить на вопросы клиентов и помочь в удовлетворении их требований. К службам поддержки могут относиться сотрудники, непосредственно контактирующие с клиентами (то есть справочная служба), сотрудники служб первоочередной поддержки (например, специалисты по технической поддержке, менеджеры-консультанты по работе с заинтересованными сторонами и т. д.), сотрудники внутренних/внешних отделов продаж или сотрудники, работающие на местах (продавцы-консультанты, специалисты по продажам и т. д.).

Подфункция 1.1.1.6 Участие в деятельности внутренних рабочих групп

В организациях с более сложной структурой инженеры из группы PSIRT могут выстраивать и укреплять связи с внутренними заинтересованными сторонами, участвуя в различных внутренних мероприятиях или в деятельности рабочих групп. Это помогает PSIRT закреплять/накапливать технический опыт и создавать каналы общения и связей для будущей работы.

Функция 1.1.2 Внутренний цикл обеспечения безопасности на этапе разработки продукции

Поддержание и обеспечение соблюдения цикла обеспечения безопасности на этапе разработки продукции является ключевым условием для формирования у заинтересованных сторон доверия к продукции организации. Если организация не способна продемонстрировать многократное применение стандартов безопасности в течение жизненного цикла продукта, заинтересованные стороны могут утратить доверие к продукции организации, предъявить к организации более жесткие требования (возложить на нее обязанность доказывания, установить право на проведение проверок и т. д.), что в конечном итоге может привести к потере доходов и утрате доверия со стороны заинтересованных сторон. ***Цель**: организации, придерживающиеся рекомендуемых стандартов обеспечения безопасности на протяжении всего цикла разработки продукта, снизят затраты на устранение дефектов безопасности в своей продукции за счет выявления таких дефектов на более ранних стадиях разработки продуктов. Все участники такого цикла разработки будут иметь четкое представление об ожиданиях относительно функций безопасности, функциональных*

возможностей и требований к предлагаемым продуктам, а также понимать свои задачи и зоны ответственности в рамках этого цикла.

***Результат**: PSIRT располагает четкой информацией о выпуске продукта и способна представить показатели и данные в отношении своевременности доставки. Работая в рамках зрелых организаций PSIRT может собирать данные о наиболее часто встречающихся слабых местах в ранее выпускавшихся продуктах, что позволяет избежать подобных ошибок в будущем.*

Подфункция 1.1.2.1 Участие в деятельности в рамках SDL

SDL – это критически важный управленческий процесс, с помощью которого организация может стабильно и регулярно предлагать новые продукты, соответствующие общепринятым стандартам. Участие PSIRT в разработке и поддержании SDL организации помогает гарантировать применение надлежащих методов обеспечения безопасности и проведение соответствующих проверок.

Подфункция 1.1.2.2 Участие в управлении SDL

SDL – это критически важный управленческий процесс, с помощью которого организация может стабильно и регулярно предлагать новые продукты, соответствующие общепринятым стандартам. Участие PSIRT в управлении SDL организации и внедрении его принципов помогает гарантировать применение надлежащих методов обеспечения безопасности и проведение соответствующих проверок, а также документальное оформление исключений и их надлежащий анализ.

Функция 1.1.3 Процедура анализа инцидентов

В случае обнаружения уязвимостей в предлагаемых организацией продуктах PSIRT требует изучения возникших проблем, какими бы ошибками – в кодах, процессах или в действиях сотрудников – они ни были вызваны, чтобы затем довести результаты до сведения участвующих заинтересованных сторон и руководства организации. Некоторые особенно серьезные или получившие наибольшую огласку уязвимости безопасности могут потребовать более глубокого анализа реакции компании и принятых ею мер по исправлению ошибок. Анализ инцидента проводится на совещании с участием всех внутренних заинтересованных сторон, занимавшихся устранением уязвимости и информированием общественности, при этом документально фиксируется, что было сделано хорошо, что можно было сделать лучше и какие изменения будут произведены в случае возникновения подобных событий в будущем.

***Цель**: дать четкий и основанный на фактических данных отчет о событиях, имевших место в ходе реагирования на уязвимость, в том числе об инцидентах, связанных с безопасностью, представив точки зрения всех принимавших участие сторон/групп. В особо сложных ситуациях PSIRT может содействовать организации в принятии мер по устранению уязвимости, имеющей важные последствия и вызвавшей широкий резонанс, или возглавить такую работу.*

***Результат**: PSIRT предоставляет данные о мерах, принятых организацией для устранения уязвимостей в программном обеспечении. Эти данные включаются в категорию "извлеченные уроки", которые будут использоваться как основа для улучшений при возникновении событий в будущем.*

Подфункция 1.1.3.1 Введение процедуры анализа дефектов безопасности продукции

Введение последовательной процедуры анализа инцидента по его завершении помогает постоянно совершенствовать продукцию на основе извлеченных уроков.

Подфункция 1.1.3.2 Анализ сроков проведения процедур и выпуска обновлений

Выявление сильных и слабых мест.

Подфункция 1.1.3.3 Анализ резонансных инцидентов

Обобщение извлеченных организацией уроков, практики реагирования на резонансные инциденты и их анализа и, при необходимости, предоставление полученных данных бизнес-сообществу и другим заинтересованным сторонам.

Услуга 1.2 Взаимодействие с сообществом лиц, обнаруживающих уязвимости

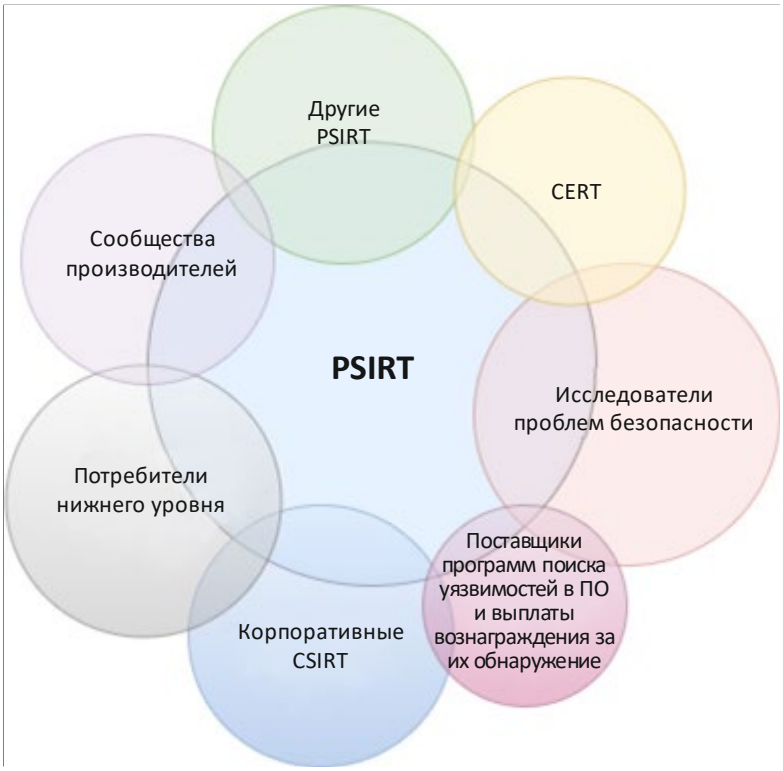


Рисунок 7. Примеры внешних заинтересованных сторон PSIRT

Услуги по обеспечению взаимодействия с исследовательским сообществом как заинтересованной стороной. Лица, обнаруживающие уязвимости, могут заниматься их поиском по разным причинам и с разными целями; в числе таких лиц могут быть научные работники, профессиональные разработчики, специалисты по выявлению проблем безопасности или любители. Некоторые из них могут изучать атаки или дефекты с точки зрения теории, рассчитывая на публикации и научные достижения, тогда как другие, возможно, являются специалистами по выявлению проблем безопасности, преследующими финансовые и карьерные цели. Среди таких лиц могут быть и любители или энтузиасты, занимающиеся поиском уязвимостей в свободное время, возможно чтобы заслужить почет и уважение в среде единомышленников. Взаимодействие с лицами, обнаруживающими уязвимости, представляет собой упреждающий подход к реагированию на инциденты в сфере безопасности продукции.

> ***Цель**: позиционировать действующую в организации PSIRT как активного члена исследовательского сообщества и обеспечивать ситуативную осведомленность об угрозах, способных повлиять на безопасность продукции, производимой организацией. Неприязненные или враждебные отношения с лицами, обнаруживающими уязвимости, могут привести к тому, что*

организация не будет заблаговременно уведомлена о результатах исследований, что неблагоприятно скажется на ее возможностях реагировать на уязвимости защиты и, соответственно, негативно скажется на отношении заинтересованных сторон к организации.

***Результат**: успешное взаимодействие с сообществами укрепит репутацию организации и ее позиции на рынке как лидера в области обеспечения безопасности продукции. Помимо этого, успешное взаимодействие с лицами, обнаруживающими уязвимости, позволит своевременно получать доступ к результатам исследований и/или сведениям об уязвимостях защиты, что поможет организации подготовиться к реагированию на возможное обнародование таких сведений.*

Функция 1.2.1 Взаимодействие с лицами, обнаруживающими уязвимости

Осуществление мер, направленных на поддержание активного диалога со специалистами по поиску уязвимостей, обладающими профессиональным опытом в сфере безопасности продукции компании и имеющими доступ к различным каналам. PSIRT может принимать самые разные меры по налаживанию более тесного взаимодействия с сообществами специалистов по поиску уязвимостей в продукции компании. Например, высококвалифицированным специалистам этого профиля можно предлагать заключение индивидуальных договоров, приглашать их на конференции и другие мероприятия и даже спонсировать их научные изыскания.

***Цель**: расширять присутствие в социальных сетях. Вести мониторинг социальных сетей и других популярных сайтов/форумов, разыскивая признаки того, что специалисты по поиску уязвимостей или заинтересованные стороны, возможно, обнаружили какую-либо проблему. Рассмотреть возможность регулярного посещения конференций по проблемам безопасности, на которых можно лично встречаться со специалистами по поиску уязвимостей.*

***Результат**: благодаря четко определенным каналам связи PSIRT сможет чаще и быстрее получать предварительные уведомления от обнаруживающих уязвимости лиц, с которыми удалось наладить тесное взаимодействие.*

Функция 1.2.2 Взаимодействие с другими PSIRT

Налаживание взаимосвязей с аналогичными PSIRT может помочь в обмене информацией и, потенциально, в обеспечении взаимопомощи и/или координации действий в случае инцидента. Сотрудничество с аналогичными организациями может способствовать получению данных, крайне необходимых для устранения уязвимостей, а также приобретению организацией знаний и опыта в результате

проведения двумя такими группами консультаций по проблемам. PSIRT необходимо создавать каналы связи (как обычные, так и защищенные) с ключевыми аналогичными организациями. Установление и укрепление связей с аналогичными отраслевыми структурами имеет решающее значение для обмена информацией и координации усилий по решению проблем, важных для обеих организаций.

Цель: *создать каналы связи между вашей организацией и другими PSIRT для обмена данными об уязвимостях, оперативной информацией об угрозах и передовым опытом.*

Результат*: создание сообщества аналогичных PSIRT имеет большое значение для реагирования на уязвимости в цепочке поставок программного обеспечения. В этом случае можно рассчитывать на более оперативное реагирование.*

Подфункция 1.2.2.1 Документальное оформление и определение аналогичных PSIRT

Сбор контактных данных и налаживание взаимодействия с перспективой на будущее. PSIRT необходимо работать и взаимодействовать с более широким кругом PSIRT, чтобы обмениваться передовым опытом и результатами анализа извлеченных уроков. В случае возникновения уязвимостей их устранение часто осуществляется совместными усилиями нескольких групп, что позволяет PSIRT наращивать свой потенциал за счет получения информации и/или помощи от таких внешних партнеров.

Подфункция 1.2.2.2 Определение процедуры скоординированного раскрытия информации

PSIRT необходимо тщательно документировать условия обмена информацией об уязвимостях и соответствующие соглашения. PSIRT следует соблюдать требования относительно эмбарго, выдвинутые лицом, обнаружившим уязвимость, и/или сообщившей о ней организацией (и рассчитывать на такое же соблюдение эмбарго с их стороны).

Подфункция 1.2.2.3 Определение процедур обмена информацией по вопросам безопасности

PSIRT необходимо определить методы безопасного обмена информацией об уязвимостях и другой конфиденциальной информацией со сторонами, договорившимися о скоординированном раскрытии информации. К числу таких методов могут относиться применение внеполосного режима, средств

неэлектронной связи, электронной почты/порталов с шифрованием или закрытых списков рассылки.

Подфункция 1.2.2.4 Участие в деятельности отраслевых специальных групп по интересам и рабочих групп

Сотрудничество с коллегами по проблемам, представляющим интерес для отрасли, помогает поддерживать и укреплять контакты, а совместное решение проблем повышает уровень профессионализма в отрасли.

Функция 1.2.3 Взаимодействие с координаторами (CSIRT и другими организациями, занимающимися вопросами координации)

Сотрудничество с правительственными CSIRT помогает укреплять доверие к обмену информацией, а самой PSIRT – заручиться доверием и уважением со стороны важных для нее партнеров. К числу таких организаций или сообществ, имеющих соответствующие интересы, относятся, помимо прочего, FIRST, MITRE, Организация по развитию открытых стандартов для информационного общества (OASIS), Отраслевой консорциум по укреплению безопасности интернета (ICASI), Международная организация по стандартизации (ИСО). Группы-участницы можно выбирать по странам, компаниям, регионам или отраслям.

***Цель**: организации нередко становятся мишенями для злоумышленников, которые используют ранее неизвестные уязвимости для проникновения в сети этих организаций. Налаживание связей с CSIRT способствует укреплению доверия и установлению контактов, что позволяет заранее получать сообщения о возможных уязвимостях.*

***Результат**: хорошие отношения с CSIRT и другими организациями, занимающимися вопросами координации, позволяют оперативно получать сведения об уязвимостях. В этом случае также можно рассчитывать на более быстрое принятие ответных мер.*

Подфункция 1.2.3.1 Взаимодействие с сообществами и партнерами

PSIRT следует выяснить, на каких площадках ведут диалог внешние группы, представляющие для нее интерес, и попытаться войти в число участников подобных форумов.

Функция 1.2.4 Взаимодействие с исследователями, занимающимися проблемами безопасности

Исследованиями в сфере безопасности могут заниматься самые разные люди, в том числе научные работники, любители и специалисты-практики по этим вопросам. Эти лица, как правило, первыми в отрасли обнаруживают уязвимости.

Специалисты по исследованию, пытаются вступить в контакт с лицом, ответственным за разработку продукта, однако по ряду причин им не всегда удается это сделать. PSIRT становится в этом случае пассивным получателем сообщений от таких лиц или групп и вынуждена работать в заданных извне временных рамках. Именно поэтому в интересах PSIRT применять упреждающий подход к работе с лицами, проводящими исследования в сферах, которые имеют отношение к продуктам, которыми занимается PSIRT, и налаживать с ними позитивные связи, чтобы получать больше сведений о выявленных проблемах.

Подфункция 1.2.4.1 Взаимодействие с поставщиками систем безопасности

Крупные коммерческие компании – поставщики систем безопасности работают с заинтересованными сторонами в случаях нарушения безопасности и часто располагают данными судебной экспертизы, к которым PSIRT обычно доступа не имеют. Налаживание связей с такими поставщиками помогает в формировании взаимного доверия и уважения и, в идеале, может помочь PSIRT получить доступ к критически важным данным об угрозах, которые в ином случае группа получить бы не могла.

Подфункция 1.2.4.2 Документальное оформление отношений с соответствующими поставщиками систем безопасности

Знакомство и должным образом организованное взаимодействие с поставщиками систем безопасности может ускорить коммуникации и принятие мер, связанных с информированием об уязвимостях и их устранением, поскольку такие поставщики будут сообщать PSIRT о возникающих проблемах. Прежде чем вступать в отношения с поставщиками программ поиска ошибок в программном обеспечении и выплаты вознаграждения за их обнаружение, такие отношения следует тщательно проверить и задокументировать, чтобы все стороны понимали, как они должны себя вести, к каким ресурсам они могут получить доступ, каким образом происходит обмен данными и с кем именно.

Подфункция 1.2.4.3 Документальное оформление методов взаимодействия с поставщиками систем безопасности

PSIRT следует выяснить, на каких площадках ведут диалог внешние группы, представляющие для нее интерес, и попытаться войти в число участников подобных форумов.

Функция 1.2.5 Взаимодействие с поставщиками программ поиска ошибок в программном обеспечении и выплаты вознаграждения за их обнаружение

Налаживание контактов с поставщиками таких программ в целях повышения эффективности коммуникаций и обмена данными по проблемам управления уязвимостями.

***Цель**: если ваша организация регулярно получает сведения об уязвимостях от поставщиков/посредников, выплачивающих вознаграждение лицам, обнаружившим ошибки в программном обеспечении, рассмотрите возможность налаживания прямых связей с такими организациями, которые часто заключают соглашения об уровне обслуживания (SLA) в отношении подлежащих устранению уязвимостей.*

***Результат**: прямые взаимосвязи с поставщиками программ поиска ошибок в программном обеспечении и выплаты вознаграждения за их обнаружение помогут наладить конструктивный диалог, в ходе которого их можно проинформировать о выпуске исправлений для систем безопасности. Такие взаимосвязи помогут не только заключить SLA на приемлемых условиях, но и снизить – к взаимной выгоде всех заинтересованных сторон – риск появления уязвимостей нулевого дня.*

Подфункция 1.2.5.1 Документирование и определение соответствующих программ поиска ошибок в программном обеспечении и выплаты вознаграждения за их обнаружение

Определите поставщиков программ поиска ошибок в программном обеспечении, которые могли бы работать с предлагаемыми компанией продуктами, и задокументируйте отношения с ними.

Подфункция 1.2.5.2 Взаимодействие с поставщиками программ поиска ошибок в программном обеспечении и выплаты вознаграждения за их обнаружение

Определить каналы для налаживания активного диалога с поставщиками таких программ.

Функция 1.2.6 Учет потребностей CSIRT

CSIRT – это особая категория заинтересованных сторон нижнего уровня, которые занимаются исключительно вопросами обеспечения безопасности. Хотя обычно взаимодействовать с такими группами можно в рамках стандартной практики взаимодействия с заинтересованными сторонами и работы с клиентами, PSIRT необходимо понимать особые потребности и подходы этих ориентированных на обеспечение безопасности групп, учитывая, что они будут контактировать с PSIRT и получать от нее информацию. К числу таких потребностей относятся форматы и сроки раскрытия информации (см. раздел Услуга 5.3. Раскрытие информации), а также каналы связи по конкретным запросам.

Услуга 1.3 Взаимодействие с сообществами и организациями

Дополнительного внимания требуют к себе две группы заинтересованных сторон, с которыми PSIRT предстоит взаимодействовать. Участие сообществ, именуемых иногда сообществами нижнего уровня и верхнего уровня, крайне важно, поскольку это позволяет повысить эффективность совместных мер по устранению уязвимостей или взаимопомощи в рамках сотрудничества аналогичных групп. Термин "структура верхнего уровня" применяется в отношении групп или физических лиц, поставляющих вашей организации компоненты или проекты для ваших продуктов. Термин "структура нижнего уровня" относится к физическим лицам, группам и организациям, которые в своих разработках используют производимую вашей организацией продукцию. Взаимодействие со структурами нижнего уровня рассматривается в разделе Услуга 1.4. Работа с заинтересованными сторонами нижнего уровня.

Активно работающее сообщество верхнего уровня может содействовать внедрению инноваций в производство продукции, а также помочь в решении сложных задач по устранению уязвимостей, зачастую восполняя нехватку важных знаний по этим вопросам у сотрудников организации. Аналогичным образом поддержание профессиональных отношений с сотрудниками и подразделениями других организаций может помочь PSIRT расширить свои возможности за счет ознакомления с их подходами, опытом и знаниями. Для этого необходимо в порядке собственной инициативы наладить взаимодействия с сообществом специалистов по безопасности в качестве заинтересованной стороны, а также установить связи с партнерами и аналогичными PSIRT.

***Цель**: PSIRT необходимо создать и поддерживать активную экосистему, включающую партнеров и аналогичные структуры. Подобные объединения могут быть полезны для выработки подхода к поиску и устранению дефектов с учетом многих мнений, а также для организации обмена примерами передовой практики между разными группами в целях расширения общего опыта устранения уязвимостей.*

***Результат**: хорошие взаимоотношения и активная экосистема с участием партнеров и аналогичных организаций будут способствовать обмену оперативной информацией о выявленных угрозах и передовым опытом. PSIRT, пользующейся хорошей репутацией в сообществе специалистов в области безопасности, может быть проще изыскивать ресурсы и заручиться помощью в сложных ситуациях.*

Функция 1.3.1 Определение сообществ и партнеров верхнего уровня и взаимодействие с ними

В продукцию организации часто включаются коды или компоненты, созданные сторонними производителями. Создатели подобных материалов нередко именуются третьими сторонами, поставщиками или поставщиками верхнего уровня, производителями оригинального оборудования (OEM) или просто партнерами. Полезно выявить таких партнеров в вашей экосистеме и определить, каким образом организация будет поддерживать контакты и взаимодействовать с ними в случае выявления уязвимостей в коде, созданном третьей стороной.

***Цель**: наладить дружеские рабочие отношения с лицами или группами, которые поставляют вам компоненты, или с группами, которым поставляет компоненты ваша организация. Понимание того, кто и каким образом должен поддерживать контакты с такими группами, позволит PSIRT постоянно находиться в курсе возникающих проблем, а также знать, кого нужно ставить в известность в случае выявления дефектных компонентов, поставляемых организацией.*

***Результат**: PSIRT имеет более четкое представление о том, от кого и откуда поступают компоненты. Это позволяет быстрее получать информацию и устранять дефекты в случае их выявления в компонентах.*

Подфункция 1.3.1.1 Определение сообществ и партнеров верхнего уровня и документальное оформление отношений с ними

Сообщества и партнеры верхнего уровня предоставляют коды и/или знания и опыт, используемые в продуктах, предлагаемых организацией. Очень важно знать таких поставщиков и работать с ними, поскольку в случае поступления информации об уязвимостях защиты и участия PSIRT в работе по их устранению это может обеспечить быстрое и эффективное взаимодействие. В идеале такие взаимоотношения должны быть оформлены в договорах, подпадающих под действие соглашений о неразглашении информации и других мер защиты организации.

Подфункция 1.3.1.2 Взаимодействие с сообществами и партнерами

Сообщества и партнеры верхнего уровня могут использовать разные методы и инструменты для разработки своего программного обеспечения/продуктов и информирования о них. PSIRT необходимо понимать, каким образом следует взаимодействовать с такими внешними группами, и убедиться в том, что у них имеются соответствующие контакты/методы, которые позволяют осуществлять сотрудничества по вопросам безопасности, касающимся этих внешних сторон.

Подфункция 1.3.1.3 Участие в деятельности сообществ верхнего уровня

Участие в деятельности сообществ и партнеров верхнего уровня помогает установить доверие между группами и расширить возможности таких внешних групп за счет знаний и опыта, которыми, возможно, располагает организация.

Подфункция 1.3.1.4 Участие в мероприятиях, организуемых сообществами и отраслью

Конференции и профессиональные форумы дают PSIRT великолепную возможность вступать в контакт с заинтересованными сторонами и партнерами, напрямую получать важную для организации информацию, а также сформировать благоприятное к себе отношение и хорошую репутацию в глазах внешних партнеров, что в дальнейшем может оказаться полезным для координации усилий и совместной работы.

Подфункция 1.3.1.5 Взаимодействие с группами по безопасности в рамках сообщества

Для PSIRT крайне важно понимать, с какими именно группами по безопасности, имеющимися в компаниях верхнего уровня – поставщиками программного обеспечения/компьютерного оборудования/услуг (PSIRT, CSIRT, инженерами в области безопасности) следует поддерживать контакты и каким образом. Установление каналов связи и взаимопонимание между PSIRT и этими группами помогает эффективно взаимодействовать в кризисных ситуациях или при устранении уязвимостей.

Функция 1.3.2 Определение сообществ и партнеров нижнего уровня и взаимодействие с ними

Понятие "структура нижнего уровня" имеет много смысловых оттенков, но это не означает, что PSIRT может игнорировать эти чрезвычайно важные группы заинтересованных сторон. Выражение "нижний уровень" относится к любому продукту, организации или физическому лицу, которые получают и используют в своих собственных целях продукты или предложения, поставляемые организацией, в рамках которой работает PSIRT. Чаще всего это клиенты или

потребители предлагаемых товаров и услуг, однако так бывает не всегда. Иногда другая компания может использовать или лицензировать продукты, производимые организацией, в рамках которой работает PSIRT, и перепродавать их как свой товар через это третье лицо, или же, как это обычно бывает с программным обеспечением с открытым исходным кодом, одна группа производит и поддерживает программное обеспечение, а широкий круг сторон, именуемых также сторонами "ниже источника", пользуется этим ресурсом.

Подфункция 1.3.2.1 Определение сообществ, потребителей и партнеров нижнего уровня и документальное оформление отношений с ними

Сообщества и партнеры нижнего уровня являются потребителями кодов и/или знаний и опыта, которые задействованы в продуктах, производимых организацией. В идеале подобные отношения должны быть документально оформлены в договорах, подпадающих под действие соглашений о неразглашении информации и других мер защиты организации.

Подфункция 1.3.2.2 Взаимодействие с сообществами нижнего уровня

Сообщества и партнеры нижнего уровня могут использовать разные методы и инструменты для разработки своего программного обеспечения/продуктов и информирования о них. PSIRT необходимо понимать, каким образом следует взаимодействовать с такими внешними группами, и убедиться в том, что у них имеются соответствующие контакты/методы, которые позволяют осуществлять сотрудничество по вопросам безопасности, касающимся этих внешних сторон.

Услуга 1.4 Работа с заинтересованными сторонами нижнего уровня

Чтобы успешно задействовать круг ваших заинтересованных сторон в этом качестве, PSIRT должны разработать процедуры и методы взаимодействия с сообществом заинтересованных сторон по вопросам реагирования на инциденты в сфере безопасности продукции. Крайне важно добиться того, чтобы заинтересованные в продукции организации стороны были удовлетворены ею, поскольку от них зависят текущие и будущие возможности организации получать доходы.

***Цель**: PSIRT необходимо создавать и поддерживать каналы связи с кругом заинтересованных сторон организации, чтобы информировать их об уязвимостях защиты продукции или о мерах реагирования на инциденты в сфере безопасности.*

***Результат**: хорошие взаимоотношения с вашими заинтересованными сторонами не только будут способствовать поддержанию (а в некоторых случаях и увеличению) доходов, но также предоставят заинтересованным*

сторонам возможность высказать свое мнение о вашей продукции, развивая у них чувство вовлеченности и причастности к принятию решений.

Функция 1.4.1 Взаимодействие с заинтересованными сторонами нижнего уровня

Сторонам, заинтересованным в вашей продукции и услугах, необходимо предоставить каналы для обмена информацией и мнениями, а также для получения сведений о том, как организация устраняет уязвимости защиты продукции. Упреждающее взаимодействие с заинтересованными сторонами организации способствует получению позитивного опыта отношений с брендом и поддержанию/укреплению лояльности заинтересованных сторон.

***Цель**: разработать для заинтересованных сторон организации, относящихся к нижнему уровню, каналы поддержания связи с PSIRT и получения помощи в решении проблем в области безопасности. Отсутствие надлежащей реакции на запросы и требования заинтересованных сторон может негативно отразиться на репутации бренда и повлечь за собой негативные публичные комментарии, отказ от возобновления контрактов или потерю новых возможностей для бизнеса.*

***Результат**: заинтересованные стороны нижнего уровня должны получать оперативные и четкие разъяснения относительно дефектов безопасности. Это будет способствовать укреплению доверия к продукции и повышению лояльности к бренду. Формируйте с помощью PSIRT общий позитивный опыт отношений с компанией и закрепите у заинтересованных сторон представление о профессионализме PSIRT. В общем плане стремитесь улучшить отношение к бренду в целом.*

Подфункция 1.4.1.1 Разработка четкой политики в отношении жизненного цикла и поддержки продукции

Организации следует четко и публично заявить, на что заинтересованным сторонам следует рассчитывать с точки зрения исправления уязвимостей защиты и сроков поддержки продукции. Дополнительную информацию см. в разделе Сфера обслуживания 4.

Подфункция 1.4.1.2 Взаимодействие с заинтересованными сторонами

У сторон, заинтересованных в продукции и услугах организации, будут возникать вопросы, потребность в помощи или устранении дефектов защиты, о которых они сообщают. PSIRT следует активно реагировать на запросы заинтересованных сторон, предоставлять ясную и точную информацию относительно таких уязвимостей и обеспечивать уменьшение риска до тех пор, пока заинтересованной стороне не будет предоставлено решение проблемы.

Услуга 1.5 Координация деятельности по информированию об инцидентах в рамках организации

Инциденты в сфере безопасности затрагивают многие группы внутри организации, иногда включая продукцию. PSIRT играет ключевую роль в координации мер по устранению уязвимости защиты продукции, а также выполняет функции центра по уведомлению уполномоченных внутренних заинтересованных сторон об инцидентах.

***Цель**: обеспечить всех участников бизнес-процесса информацией о мерах реагирования на уязвимости защиты продукции, с тем чтобы участники могли принимать обоснованные решения в отношении дальнейших действий. Средства связи могут быть самыми разными (электронная почта, традиционная почта, RSS-каналы, социальные сети и т. д.), но в конечном итоге все они должны предоставлять ясную, своевременную, точную информацию об уязвимостях безопасности продукции и инцидентах, имеющих значение для заинтересованных сторон.*

***Результат**: внутренние заинтересованные стороны будут осведомлены о масштабах и последствиях угроз для продукции и услуг, предлагаемых организацией. Информировать заинтересованные стороны необходимо для того, чтобы они могли в дальнейшем, после устранения уязвимостей безопасности продукции и появления средств смягчения последствий этих уязвимостей, принимать соответствующие решения.*

Функция 1.5.1 Предоставление каналов/средств связи

Для обеспечения эффективного взаимодействия с заинтересованными сторонами PSIRT должна предоставить широкий выбор каналов связи. Различные заинтересованные стороны могут иметь свои предпочтения в выборе средств связи. При разработке и выпуске средств связи PSIRT должна учитывать интересы как можно более широкой пользовательской аудитории. PSIRT также должна быть оснащена необходимым оборудованием для принятия сообщений об уязвимостях безопасности продукции, комментариев и вопросов из различных источников.

***Цель**: предоставить заинтересованным сторонам каналы для связи с PSIRT.*

***Результат**: при помощи этих каналов связи – электронной почты, веб-чатов, веб-форм и т. д. – внутренние заинтересованные стороны получают возможность поддерживать связь и обмениваться информацией с PSIRT.*

Подфункция 1.5.1.1 Предоставление четко определенных каналов связи

Заинтересованные стороны должны знать, по каким каналам они могут задавать вопросы, проверять статус ошибок и сообщать PSIRT о возникших

проблемах. Если заинтересованные стороны сталкиваются с последствиями уязвимости безопасности продукции или обнаруживают такую уязвимость, у них должна быть возможность без труда создать и отправить PSIRT сообщение об этой проблеме.

Подфункция 1.5.1.2 Предоставление каналов для внутренней связи

Для привлечения внутренних заинтересованных сторон PSIRT должна обеспечить каналы связи, по которым будет распространяться информация о положении дел с устранением уязвимостей безопасности продукции. Внутренние заинтересованные стороны должны иметь возможность без труда связываться с PSIRT, для того чтобы узнать о статусе своих запросов.

Подфункция 1.5.1.3 Предоставление каналов для внешней связи

Для привлечения внешних заинтересованных сторон PSIRT должна обеспечить каналы связи, по которым будет распространяться информация о положении дел с устранением уязвимостей безопасности продукции. Каналы внешней связи должны пройти проверку/отбор для подтверждения их технической применимости и надлежащей маршрутизации к внутренним подразделениям.

Функция 1.5.2 Организация безопасной связи

Зачастую PSIRT приходится обрабатывать информацию, считающуюся конфиденциальной (то есть вопросы, находящиеся под эмбарго). PSIRT должна иметь возможность организовывать безопасную и надежную связь с лицами, обнаруживающими уязвимости, другими организациями или с соответствующими внутренними подразделениями. Соблюдение соглашений о неразглашении информации и поддержание связи только по частным каналам способствует укреплению доверия со стороны лиц, обнаруживающих уязвимости. Защита конфиденциальной информации об уязвимости безопасности продукции от сторон, не имеющих права на доступ к ней, также позволяет надлежащим образом и эффективно урегулировать данные вопросы в соответствии с условиями эмбарго. Безопасные каналы связи также могут обеспечить защиту персональных данных лиц, обнаруживающих уязвимости и не желающих быть идентифицированными. Необходимо разработать соответствующую политику хранения информации, которая предусматривала бы надлежащее уничтожение данных после окончания их использования.

***Цель**: предоставить сторонам каналы для приватного обмена информацией по вопросам уязвимости безопасности продукции. Такие каналы обеспечивают защиту конфиденциальности информации по этим вопросам, а также защиту*

конфиденциальности персональных данных лиц, обнаруживающих уязвимости, до тех пор, когда эта информация сможет быть публично раскрыта.

***Результат**: стороны, принимающие участие в решении вопросов безопасности, получают возможность приватно обмениваться информацией с другими сторонами, которые нуждаются в информации по этому вопросу. Лица, обнаруживающие уязвимости, с большей вероятностью будут и далее предоставлять организации сведения об уязвимости, если они будут уверены в том, что организация обеспечивает защиту их персональных данных.*

Подфункция 1.5.2.1 Предоставление безопасных каналов связи

PSIRT должна обеспечить лицам, обнаруживающим уязвимости, и партнерам, занимающимся устранением уязвимостей, оказывающим воздействие на предлагаемые организацией продукты и услуги, доступ к закрытым и защищенным каналам для обмена информацией.

Функция 1.5.3 Обновление системы отслеживания дефектов безопасности

PSIRT должна иметь доступ к системе (системам) регистрации всех дефектов продукции и быть способна создавать и использовать систему отслеживания уязвимостей безопасности и обмена информацией по этим вопросам.

***Цель**: надлежащая система регистрации и отслеживания дефектов безопасности позволяет организации предоставлять информацию о времени и месте устранения уязвимостей. Система отслеживания дефектов также позволяет осуществлять связь между PSIRT, лицами, обнаруживающими уязвимости, и инженерами, принимающими активное участие в решении проблемы.*

***Результат**: при помощи системы надлежащего отслеживания уязвимостей безопасности продукции все стороны, нуждающиеся в доступе к информации о данной уязвимости, могут отслеживать историю ее возникновения и ход работы по ее устранению, а также оставлять комментарии.*

Подфункция 1.5.3.1 Предоставление возможности отслеживания дефектов безопасности продукции

Внешним и внутренним сторонам (если это применимо) необходимо предоставить доступ к системам отслеживания дефектов безопасности и (в соответствии с принципом наименьших привилегий) для обновления и отслеживания хода работ по устранению таких дефектов. Внешние лица, обнаруживающие уязвимости, должны получать сведения о статусе своих сообщений, представленных PSIRT.

Подфункция 1.5.3.2 Разработка и публикация процедуры отслеживания дефектов безопасности

PSIRT должна обеспечить лицам, обнаруживающим уязвимости, и партнерам, которые занимаются устранением уязвимостей, оказывающих воздействие на предлагаемые организацией продукты и услуги, доступ к закрытым и безопасным каналам для обмена информацией.

Функция 1.5.4 Распространение и публикация информации

После решения возникшей проблемы PSIRT должна распространить информацию о характере уязвимости безопасности, используя в качестве критерия систему оценки общеизвестных уязвимостей (CVSS), о степени ее опасности и ее последствиях, о потенциальных рисках эксплуатации уязвимости, а также о способах решения возникшей проблемы или смягчения ее последствий. Один из часто используемых способов широкого/публичного распространения информации об уязвимости – это внесение этой уязвимости в общий перечень общеизвестных уязвимостей и незащищенности (CVE). Таким образом можно создать уникальную справку об этой проблеме, присвоив ей идентификационный номер, создав ее описание и сделав по крайней мере одну публичную ссылку на нее.

***Цель**: распространение подробной информации о выявленных и устраненных уязвимостях безопасности продукции. Заинтересованные стороны должны иметь возможность получить поддержку или доступ к альтернативным средствам сдерживания рисков, пока не будут приняты официальные исправления.*

***Результат**: заинтересованные стороны будут получать информацию о проблемах в области безопасности, о возможном воздействии этих проблем и о способах их исправления. Заинтересованные стороны, получающие своевременную информацию и обновления, с большей вероятностью будут положительно относиться к организации и либо продолжат пользоваться ее услугами и продукцией, либо расширят их использование в будущем.*

Подфункция 1.5.4.1 Предоставление нескольких разных каналов связи

Разные заинтересованные стороны предпочитают использовать разные способы взаимодействия/связи в случае публичного раскрытия информации об уязвимостях защиты продукции. PSIRT должна использовать не только традиционную систему информирования в виде рекомендаций, но и другие способы, обеспечивающие максимальную вовлеченность заинтересованных сторон и их осведомленность об уязвимости безопасности. После устранения

уязвимостей PSIRT должна распространять информацию об исправлении ошибки, используя для этого самые разные методы.

Подфункция 1.5.4.2 Предоставление заинтересованным сторонам возможности оставлять отзывы

Отзывы способствуют повышению эффективности процедур и реагирования в будущем. С помощью отзывов PSIRT может определить, в каких областях она действует эффективно, а в каких областях ей следует принимать меры по дальнейшему развитию и усовершенствованию своей деятельности.

Услуга 1.6 Выражение благодарности и признательности лицам, обнаруживающим уязвимости

Выражение признательности лицам, обнаруживающим уязвимости, а также выражение им благодарности за сотрудничество с PSIRT в деле устранения дефектов способствует повышению доверия к ним и к их организации (если это применимо) в сообществе.

***Цель**: лица, обнаруживающие уязвимости, получают признание за участие в раскрытии информации об уязвимостях продукции. Благодаря словам признательности эти лица получают возможность укрепить свою репутацию, создать свое профессиональное портфолио и продемонстрировать свою ценность для организации.*

***Результат**: опыт положительного сотрудничества с лицами, обнаруживающими уязвимости, способствует укреплению защиты продукции. Признательность, выражаемая этим лицам, важна для внутренних сотрудников, поскольку помогает им укрепить свою репутацию и продемонстрировать свой опыт и знания.*

Функция 1.6.1 Выражение признательности

Выражение признательности лицу (лицам), ответственному(ым) за выявление уязвимостей защиты продукции, – это важнейший компонент рабочего процесса по выявлению уязвимостей. Простые слова благодарности способствуют укреплению доверия и уважения в сообщества и свидетельствуют о внимании, которое организация уделяет вопросам безопасности.

***Цель**: лица, обнаруживающие уязвимости, получают признание за свой ответственный подход к раскрытию информации об уязвимостях защиты продукции. Благодаря таким словам признательности эти лица получают возможность укрепить свою репутацию и создать свое профессиональное портфолио.*

***Результат**: опыт положительного сотрудничества с лицами, обнаруживающими уязвимости, способствует укреплению защиты продукции. Признательность, выражаемая лицам, обнаруживающим уязвимости, важна для них, поскольку помогает им укрепить свою репутацию и побуждает их продолжать в дальнейшем присылать PSIRT сообщения о выявляемых уязвимостях.*

Подфункция 1.6.1.1 Выражение признательности

В распоряжении PSIRT имеется наиболее эффективный и недорогой способ вознаградить обнаружившее уязвимость лицо за его усилия и участие в выявлении уязвимости безопасности продукции, – это письменно выразить свою признательность. Выражение признательности лицу (лицам), обнаруживающему(им) уязвимости, как правило, включается в бюллетени по безопасности, примечания к выпускам программного обеспечения и тексты CVE. PSIRT должна будет определить, каким образом информация о лице, обнаружившем уязвимость, будет распространяться внутри организации.

Функция 1.6.2 Вознаграждение лиц, обнаруживающих уязвимости

В целях обеспечения положительных результатов для заинтересованных сторон и стимулирования дальнейшего распространения информации о научных изысканиях PSIRT может принять решение о разработке программы вознаграждения или поощрения подобного сотрудничества, с тем чтобы способствовать его продолжению и развитию в будущем.

***Цель**: вознаградить лицо (лиц), сообщающее о дефектах безопасности продукции и услуг организации. Вознаграждение может принимать различные формы – от электронных/письменных посланий с выражением благодарности до подарков от организации, денежных вознаграждений или других материальных премий/поощрений. PSIRT должна обеспечить прозрачность выдачи подобных вознаграждений и правил их вручения.*

***Результат**: данная практика направлена на обеспечение положительного отношения к организации PSIRT и поощрение продолжения сотрудничества по вопросам безопасности в будущем.*

Подфункция 1.6.2.1 Создание программы вознаграждения лиц, обнаруживающих уязвимости

PSIRT может финансировать программу вознаграждения, предназначенную для поощрения положительного настроя лиц, обнаруживающих уязвимости. Вознаграждения могут принимать вид денежных премий, корпоративных подарков или любых других материальных поощрений, которые могут иметь

ценность для лица, обнаруживающего уязвимости, помимо выражения признательности за его участие в выявлении проблемы.

Подфункция 1.6.2.2 Учреждение денежной премии за обнаружение уязвимостей безопасности продукции

Одним из видов вознаграждения может быть денежная компенсация. Некоторые организации могут выплачивать денежные премии лицам, предоставляющим им информацию об уязвимостях безопасности продукции.

Подфункция 1.6.2.3 Создание системы начисления очков

Система начисления очков является еще одним способом вознаграждения. В рамках этой системы поиск и направление сообщений об уязвимостях безопасности продукции принимают форму игры, в которой поощряется дружеская конкуренция, выдвигаются лидеры и создается рейтинг лиц, обнаруживающих уязвимости. Занявшие первые места могут этим гордиться.

Услуга 1.7 Показатели для заинтересованных сторон

Представление подробной информации о размерах, результативности или других показателях PSIRT необходимо для того, чтобы заинтересованные стороны были осведомлены об эффективности группы. Различные заинтересованные стороны могут придерживаться различных точек зрения, и такие показатели следует представлять, используя различные форматы артефактов (или взглядов). PSIRT должна знать, в каком формате каждая группа заинтересованных сторон желает получать такую информацию. PSIRT может использовать формат ключевых показателей деятельности (KPI).В разделе Функция 2.5.1. Оперативные отчеты речь идет об оперативных отчетах и о том, как представление подобных отчетов может способствовать бесперебойной работе PSIRT. В разделе Функция 2.5.2. Отчеты о результатах деятельности говорится об отчетах о результатах деятельности, которые PSIRT может представлять заинтересованным сторонам.

***Цель**: представление данных об оценках и показателях работы PSIRT. Эти данные позволят заинтересованным сторонам оценить эффективность деятельности PSIRT в определенной области или при предоставлении определенной услуги.*

***Результат**: анализируя показатели PSIRT, заинтересованные стороны должны получить представление о том, насколько эффективно PSIRT предоставляет ту или иную услугу; им также должна быть дана возможность направлять отзывы в целях внесения корректировок в предоставление данной услуги.*

Функция 1.7.1 Понимание требований заинтересованных сторон в отношении артефактов

Для того чтобы эффективно разъяснить процесс предоставления услуг PSIRT, необходимо прежде всего понять уникальные потребности каждой группы заинтересованных сторон. Некоторые заинтересованные стороны могут обращать особое внимание на своевременность внесения корректировок в защиту продукции, в то время как для других первостепенное значение могут иметь финансовые аспекты деятельности PSIRT. Каждая точка зрения заслуживает внимания и требует использования различных артефактов для эффективной передачи желаемой информации. Необходимо провести опрос каждой группы заинтересованных сторон для того, чтобы понять, по каким аспектам деятельности PSIRT им требуется информация, а также для того, чтобы определить наиболее эффективный способ ее распространения.

***Цель**: определить аспекты деятельности и услуг PSIRT, вызывающие обеспокоенность заинтересованных сторон. После определения и согласования этих требований необходимо выбрать способ/средство и частоту представления обновленных данных.*

***Результат**: для внесения обновленных данных будет создан документально оформленный перечень требований заинтересованных сторон в отношении артефактов (отчет/обозрение/информационная панель).*

Подфункция 1.7.1.1 Сбор требований заинтересованных сторон в отношении показателей

Одни стороны могут быть заинтересованы в определенных данных, которые не представляют интереса для других заинтересованных сторон. Например, такие данные могут касаться показателей деятельности расширенной группы, занимающейся корректировками, стоимости и качества этих корректировок.

Функция 1.7.2 Сбор показателей для заинтересованных сторон

Процедуры и действия, необходимые для документирования показателей для всех групп заинтересованных сторон. Во всех возможных случаях с помощью своих инструментов PSIRT должна быть способна собирать и распространять информацию о процедурах и результатах своей деятельности. В идеале показатели должны храниться централизованно (в базе данных, таблице или в иной форме), с тем чтобы можно было периодически проводит обзоры показателей деятельности за прошлые периоды и реагировать на различные потребности заинтересованных сторон при минимальных дополнительных трудозатратах.

***Цель**: сбор, создание, накопление и /или хранение всех элементов данных, необходимых для удовлетворения потребностей заинтересованных сторон в измерении показателей деятельности PSIRT. Эта информация должна храниться централизованно, с тем чтобы можно было проводить обзоры показателей за прошлые периоды и использовать ее многократно (то есть двумя и более группами заинтересованных сторон, желающих получить доступ к одной и той же информации).*

***Результат**: сбор требуемых заинтересованными сторонами показателей для создания артефактов (отчетов, обозрений, информационных панелей и т. д.).*

Подфункция 1.7.2.1 Сбор показателей для заинтересованных сторон

PSIRT должна разработать процедуры и методы сбора необходимых показателей с установленной периодичностью (соглашения об уровне услуг/соглашения операционного уровня).

Подфункция 1.7.2.2 Хранение показателей для заинтересованных сторон

PSIRT должна будет проводить анализ статистических данных о результативности деятельности и других тенденциях, поэтому имеет смысл создать хранилище для этих данных, с тем чтобы продолжать эффективно использовать их в будущем.

Функция 1.7.3 Анализ показателей для заинтересованных сторон

Данные без контекста не имеют смысла. Отсутствие контекста может привести к неверным предположениям, и услуги могут не подвергнуться корректировкам, необходимым для удовлетворения изменяющихся потребностей бизнеса или заинтересованных сторон. После того как необходимые данные будут собраны, PSIRT должна изучить их и представить контекст, объясняющий значение этих данных для заинтересованной стороны.

***Цель**: понять значение собранных данных и предоставить заинтересованной стороне необходимый контекст для работы с этой информацией. В идеале заинтересованная сторона должна получить представление о том, как работает данный ключевой показатель деятельности (KPI), какие факторы влияли на него в течение рассматриваемого периода и какие тенденции просматриваются в этом KPI.*

***Результат**: сохранение и сопоставление исторических данных с текущими показателями в целях определения тенденций.*

Подфункция 1.7.3.1 Анализ и критический обзор показателей

PSIRT должна потратить определенное количество времени и усилий на критический обзор собранных данных и определение контекста, а также на представление отчета о собранных показателях.

Подфункция 1.7.3.2 Анализ динамики изменения данных и показателей за прошлые периоды

Собранные данные за прошлые периоды позволяют выявить уникальные тенденции или хронические проблемы, решением которых может заниматься PSIRT или ее партнеры.

Подфункция 1.7.3.3 Определение контекста данных

Определить контекст данных, с тем чтобы заинтересованные стороны могли лучше понять предоставляемую им информацию и найти способ решения возникших вопросов или проблем.

Функция 1.7.4 Предоставление заинтересованным сторонам артефактов показателей

Собранные и проанализированные данные по показателям должны быть предоставлены заинтересованным сторонам в заранее согласованном формате. Такой формат может рассматриваться как артефакт или как обозрение, предоставляемое с учетом точки зрения заинтересованной стороны. Артефакты могут быть предоставлены в виде веб-страницы, сообщения по электронной почте, формализованного отчета или в иной форме.

***Цель**: данные по показателям следует предоставить заинтересованным в удобном для них формате, с тем чтобы они могли получить полную картину и оценить показатели деятельности PSIRT в области предоставления услуг. Эти данные должны быть доступны для понимания и подкреплены необходимым контекстом, для того чтобы заинтересованная сторона могла принимать решения, исходя из этих показателей.*

***Результат**: показатели будут представлены заинтересованным сторонам в надлежащем формате в согласованные сроки.*

Подфункция 1.7.4.1 Предоставление заинтересованным сторонам артефактов показателей

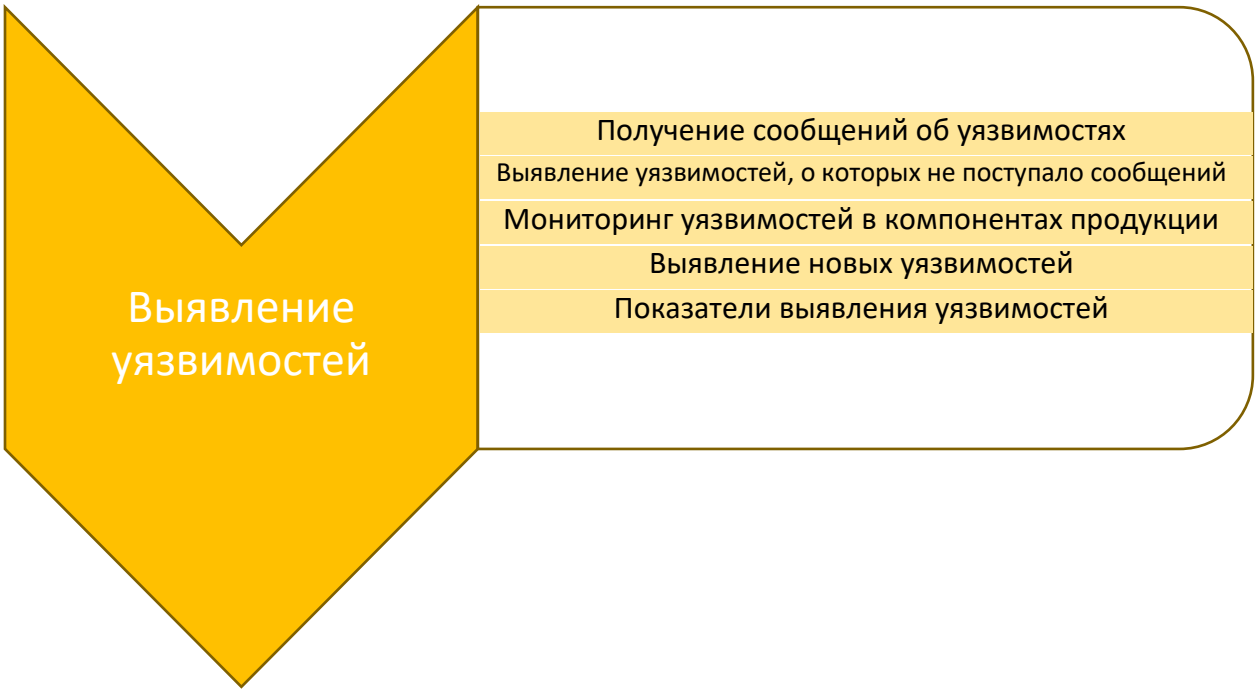
У каждой заинтересованной стороны есть своя точка зрения. Необходимо принимать во внимание точку зрения каждой заинтересованной стороны и

представлять данные в форме тех или иных отчетных артефактов. Возможно, возникнет необходимость в корректировке артефактов, с тем чтобы привести их в соответствие с различными точками зрения. К артефактам могут относиться отчеты, присланные по электронной почте или опубликованные на веб-странице, динамические веб-порталы, краткие справки, диаграммы, графики или другие механизмы предоставления данных.

Подфункция 1.7.4.2 Анализ показателей и извлеченных уроков

Одна из важнейших задач PSIRT заключается в непрерывном усовершенствовании процедур управления уязвимостями. Анализ показателей результативности и отзывов заинтересованных сторон дает возможность PSIRT определять области, требующие повышенного внимания или нуждающиеся в улучшении.

Сфера обслуживания 2



В описании настоящей сферы обслуживания рассматриваются осуществляемые PSIRT услуги и функции по выявлению потенциальных уязвимостей. В рамках данной сферы обслуживания начинается процесс обработки факторов уязвимости, описанный в других разделах настоящего документа. Доступность и эффективность различных услуг, предусмотренных в данной сфере обслуживания, могут служить критериями оценки зрелости PSIRT.

> ***Цель**: разработка процедур и механизмов сбора из различных источников данных, касающихся уязвимостей защиты продукции, уязвимых компонентов третьей стороны или архитектурных недостатков.*
>
> ***Результат**: повышение ситуационной осведомленности в отношении сообщений и потенциальных уязвимостей, которые требуют действий заинтересованных сторон.*

Услуга 2.1 Получение сообщений об уязвимостях

Основная задача PSIRT состоит в получении сообщений, затрагивающих продукцию заинтересованных сторон. Ключевыми элементами процесса получения сообщений об уязвимостях являются создание и поддержание необходимой инфраструктуры, определение контактных центров и распространение информации о них, а также определение и поддержание надлежащего уровня готовности.

***Цель**: разработка процедур и механизмов, которые позволяют организации беспрепятственно сообщать об уязвимости защиты продукции заинтересованной стороны и поддерживать надлежащий уровень готовности PSIRT в случае получения сообщения об уязвимости.*

***Результат**: готовность PSIRT к получению сообщений об уязвимостях и профессиональный прием этих сообщений.*

Функция 2.1.1 Обеспечение доступности

PSIRT должны повышать осведомленность о своем существовании и быть доступными для внешних сторон или внутренних структур. Надежные и четко определенные каналы связи обеспечивают лицам, обнаруживающим уязвимости, партнерам или заинтересованным сторонам возможность направлять PSIRT сообщения об уязвимостях.

***Цель**: предоставление организации, заинтересованной в направлении сообщений об уязвимостях, возможности беспрепятственно получить необходимую контактную информацию и использовать наиболее удобный способ подачи сообщения.*

***Результат**: получение большего числа сообщений и исключение возможности появления каких-либо жалоб на недоступность PSIRT для получения информации об уязвимостях.*

Подфункция 2.1.1.1 Определение предпочтительной формы подачи сообщений

Следует ожидать, что сообщения об уязвимостях будут поступать по различным каналам и в различном качестве. Тем не менее полезно определить наилучший способ подачи сообщения. Можно использовать веб-форму, открытую систему электронных запросов, электронную почту, горячую линию поддержки или любые другие каналы для подачи сообщений.

Подфункция 2.1.1.2 Публикация контактной информации

Информацию о предпочитаемых способах связи с PSIRT следует публиковать в документации по продукции, размещать на веб-сайте компании, индексировать в поисковых системах, регистрировать в списках основных CSIRT/PSIRT, а также сообщать организациям, занимающимся выпуском перечней общеизвестных уязвимостей (CVE), например органам по нумерации общеизвестных уязвимостей (CNA), и распространять в сообществах по вопросам безопасности.

Подфункция 2.1.1.3 Регистрация общих источников контактной информации

Было бы полезно зарезервировать общие термины, касающиеся PSIRT – такие как psirt@, inciedents@ или security@, – в составе доменного имени вашей компании. Благодаря этому вам будет удобнее поддерживать непосредственную связь с соответствующей PSIRT.

Подфункция 2.1.1.4 Связь с PSIRT внутри компании

Убедитесь в том, что служба заинтересованной стороны (отвечающая за подачу запросов заинтересованной стороны или сообщений об уязвимости), департамент по связям с общественностью (отвечающий за подачу запросов со стороны средств массовой информации), а также ваши группы по разработке продукции (и отвечающие за распространение важных внутренних сведений) осведомлены о PSIRT и знают, как с ней связаться.

Подфункция 2.1.1.5 Определение и поддержание готовности

В зависимости от отрасли и требований заинтересованных сторон для обеспечения необходимой готовности к реагированию на сообщения о критических уязвимостях следует создавать дежурные службы или поддерживать круглосуточный режим работы.

Подфункция 2.1.1.6 Подготовка к принятию шифрованных сообщений

В сообщениях об уязвимостях часто содержится конфиденциальная информация о рабочих условиях и продукции, в которой была выявлена уязвимость. Для того чтобы избежать случайных утечек или раскрытия информации, следует поощрять подачу шифрованных сообщений, например электронных сообщений, защищенных ключами S/MIME или PGP, или подачу сообщений через веб-форму с поддержкой HTTPS.

Функция 2.1.2 Обработка сообщений об уязвимостях

Сообщения об уязвимости поступают в различном виде и из различных источников. Крайне важно регулярно проводить мониторинг каналов поступающих сообщений и своевременно отвечать на получаемые сообщения. Сроки направления ответа на сообщение внешних лиц, обнаруживающих уязвимости, следует определить в соглашении об уровне обслуживания, сроки направления ответа на сообщения внутренних лиц определяет компания.

***Цель**: обеспечить процедуры и механизмы для получения сообщений об уязвимости из других отделений компании-поставщика, от заинтересованных*

сторон и третьих сторон (лиц, обнаруживающих уязвимости, других PSIRT, CSIRT и т. д.).

***Результат**: профессиональная обработка сообщений об уязвимости, полученных от третьих сторон.*

Подфункция 2.1.2.1 Мониторинг каналов связи

Проведение регулярной проверки предлагаемых каналов связи с PSIRT, а также других доступных каналов связи, таких как электронные почтовые ящики общего назначения или аккаунты компании в социальных сетях.

Подфункция 2.1.2.2 Изолированная обработка сообщений

PSIRT проводит расследование в отношении сообщений об уязвимости и вследствие этого может стать объектом для рассылки вредоносных сообщений. Необходимо разработать политику и технические процедуры для защиты рабочей среды от попыток злоумышленного воздействия и предоставить средства для безопасной обработки сообщений об уязвимости.

Подфункция 2.1.2.3 Своевременное уведомление о получении сообщений

Проведение подробного анализа полученного сообщения часто является сложной задачей, требующей большого количества времени, но для отправки простого уведомления о получении сообщения много времени не требуется. Оперативная реакция свидетельствует о серьезном отношении к полученному сообщению и способствует созданию доверительных отношений. Дальнейшая коммуникация в ходе процесса обработки полученного сообщения может основываться на этом первом обмене сообщениями и свидетельствовать о готовности PSIRT к приемлемому решению проблемы.

Услуга 2.2 Выявление уязвимостей, о которых не поступало сообщений

Уязвимости, о которых напрямую сообщает компания-поставщик или стороны, присылающие сообщения об уязвимости, заметить достаточно просто. Тем не менее важно понимать, что существуют дополнительные уязвимости, информация о которых может поступать по неофициальным каналам, таким как новостные каналы, технические блоги, экспертные базы данных, социальные сети, технические публикации или конференции.

***Цель**: поддержание осведомленности о ситуации, уменьшение времени, необходимого для выявления угроз, затрагивающих продукцию заинтересованной стороны, а также снижение вероятности полного раскрытия информации.*

***Результат**: повышение уровня осведомленности о ситуации в отношении угроз безопасности для портфеля продукции заинтересованной стороны.*

Функция 2.2.1 Мониторинг баз данных об эксплойтах

Следует проводить активный мониторинг общедоступных баз данных об эксплойтах или каналов коммерческой информации для выявления потенциальных уязвимостей нулевого дня, требующих изучения. При выявлении полностью функционирующего эксплойта компания может заранее предупредить заинтересованные стороны о его наличии.

***Цель**: выявление уязвимостей, о которых не поступало сообщений по надлежащим каналам.*

***Результат**: больший объем сведений о наличии на рынке функционирующих эксплойтов.*

Функция 2.2.2 Мониторинг программ конференций

Следует проводить мониторинг соответствующих конференций по вопросам безопасности, на которых можно услышать доклады, представляющие интерес. Помимо прямых ссылок на продукцию или торговые марки, эти доклады могут содержать материалы обсуждения более широких тем, таких как дефекты протоколов, требующие принятия мер со стороны PSIRT. Если сообщение вызывает вопросы, то представляется разумным сразу же вступить в контакт с лицом, обнаружившим дефект, чтобы определить, необходимо ли предпринимать какие-либо действия по этому поводу. Кроме того, участие в конференциях и активное налаживание контактов с авторами докладов может способствовать установлению прямой связи с PSIRT, полезной для будущих исследований.

***Цель**: предотвращение внезапного несогласованного раскрытия информации или выявление еще не изученных авторами дефектов, способных оказать прямое или косвенное воздействие на продукцию заинтересованных сторон.*

***Результат**: возможность наладить активный контакт с авторами до появления каких-либо публикаций, с тем чтобы выяснить, не затронута ли, какая-либо продукция заинтересованных сторон и не было ли проблем с подачей сообщения об уязвимости.*

Функция 2.2.3 Мониторинг публикаций известных лиц, обнаруживающих уязвимости

Следует обращать внимание на публикации лиц, обнаруживающих уязвимости, которые уже неоднократно выступали с соответствующими публикациями или обладают солидным опытом работы с продукцией отрасли или конкретно

с продукцией и услугами компании. В их научных работах, постах в блогах или списках рассылки можно найти намек на возможные уязвимости или слабые места, заслуживающие внимания.

***Цель**: поддержание высокого уровня научных и технических знаний по вопросам безопасности, имеющим большое значение для заинтересованных сторон.*

***Результат**: накопление сведений об общих угрозах, слабых местах и возможных мерах борьбы с ними для оказания поддержки заинтересованным сторонам при решении проблем, связанных с безопасностью продукции.*

Функция 2.2.4 Мониторинг средств массовой информации

Средства массовой информации часто бывают первыми, кто сообщает об инцидентах, особенно о катастрофических инцидентах, затрагивающих установки или персонал заинтересованных сторон. Мониторинг средств массовой информации может способствовать выявлению ситуаций, в которых заинтересованные стороны PSIRT могут выступать в качестве значимого или преобладающего поставщика.

***Цель**: устранение уязвимости продукции, способствовавшей возникновению инцидента.*

***Результат**: повышение готовности в случаях, когда от заинтересованных сторон или средств массовой информации поступают вопросы об уязвимостях продукции, которые могли способствовать возникновению инцидента.*

Услуга 2.3 Мониторинг уязвимостей в компонентах продукции

Уязвимости можно приблизительно разделить на три категории: 1) уязвимости в исходном коде продукции; 2) уязвимости в компонентах продукции, обслуживаемых внутренними структурами компании-поставщика; и 3) уязвимости в компонентах, предоставляемых внешними по отношению к компании-поставщику структурами (третьими сторонами). Применительно к продукту пункты 2) и 3) являются внешними компонентами, однако уязвимости в этих компонентах могут в конечном счете повлиять на весь продукт в целом. Хотя владелец продукта может лишь косвенным образом контролировать исправление лежащей в основе проблемы, заинтересованная сторона чувствует определенную ответственность за цепочку поставок и устранение уязвимости в затронутой продукции. Это касается, среди всего прочего, тех случаев, когда уязвимый компонент не может быть исправлен в отрыве от продукта, в состав которого он включен. Включенные в продукцию компоненты из открытых источников также считаются компонентами третьей стороны.

***Цель**: выявление, сбор и мониторинг уязвимостей на протяжении всей цепочки поставок продукции заинтересованной стороны и уведомление группы разработчиков продукции об уязвимостях, затрагивающих их продукцию.*

***Результат**: более эффективное выявление уязвимостей, затрагивающих продукцию заинтересованных сторон, на ранних этапах цепочки поставок.*

Функция 2.3.1 Составление списка компонентов продукции

Следует составлять списки включенных в продукцию компонентов, продуктов и версий, поставляемых внешними и внутренними сторонами. Это необходимо для быстрого выявления изначально существующих уязвимостей в затронутой продукции.

***Цель**: выявление продуктов с уязвимыми компонентами, которые могут привести к появлению уязвимости в самой продукции.*

***Результат**: составление полного списка счетов для оплаты материалов по всем видам продукции в целях выявления уязвимых компонентов.*

Функция 2.3.2 Мониторинг бюллетеней третьих сторон

Получение своевременной информации об уязвимостях в компонентах третьих сторон при помощи подписки на выпускаемые компаниями-поставщиками бюллетени или путем создания специальных каналов связи с поставщиками. Подписка на рассылки по вопросам безопасности проектов с открытым исходным кодом. Также можно использовать услуги поставщиков информации об уязвимостях.

***Цель**: выявление уязвимостей в компонентах третьих сторон, которые могут привести к уязвимости в продукции заинтересованной стороны.*

***Результат**: возможность начать процесс обработки уязвимости до появления поступающих извне сообщений о затронутой продукции.*

Функция 2.3.3 Мониторинг источников информации об уязвимостях

Не всегда существует возможность подписаться на выпускаемые организаций-поставщиком справочные издания для выявления компонентов третьей стороны – например, когда организация-поставщик не публикует такие справочники, когда организация-поставщик выходит из бизнеса или когда в сообществе с открытым исходным кодом данный компонент предварительно не обсуждался. В таком случае такие ресурсы, как национальная база данных об уязвимостях (NVD) или источники коммерческой информации, могут помочь в выявлении уязвимостей, по которым нет справочной информации.

***Цель**: выявление уязвимостей в компонентах третьей стороны, по которым нет справочной информации.*

***Результат**: получение более полного представления об уязвимостях, которые могли бы остаться незамеченными.*

Функция 2.3.4 Разработка процедур получения сообщений об уязвимостях, существующих во внутренней цепочке поставок организации-поставщика

В большинстве случаев организация-поставщик не публикует общедоступных информационных материалов о решении проблем безопасности в отношении компонентов продукции, полученных из ее внутренних источников. Для получения информации об уязвимостях во внутренней цепочке поставок организации-поставщика следует создать специальные каналы связи с поставщиками.

***Цель**: выявление уязвимостей во внутренней цепочке поставок организации-поставщика, которые могут привести к появлению уязвимостей в продукции заинтересованной стороны.*

***Результат**: получение более полного представления об уязвимостях во внутренней цепочке поставок организации-поставщика, которые могли бы остаться незамеченными.*

Функция 2.3.5 Оповещение внутренних команд разработчиков

Создание автоматизированных каналов для прямого оповещения команд разработчиков затронутой продукции о выявленных сторонних уязвимостях. Зачастую для устранения уязвимости в конечном продукте достаточно выполнить инструкции организации-поставщика верхнего уровня. В соответствии с политикой определения приоритетов следует определить порядок устранения уязвимостей и их передачи для исправления в PSIRT. Этот момент особенно важен в случаях, когда заинтересованная сторона должна предпринять какие-либо действия, чтобы получить исправленную версию продукта для обеспечения его безопасной эксплуатации.

***Цель**: предоставление командам разработчиков выборочной информации о взаимозависимых уязвимостях и корректировках (если она имеется) для внесения исправлений в следующий выпуск продукции.*

***Результат**: сокращение усилий PSIRT по исправлению уязвимостей вручную, так как справочная информация, полученная от третьей стороны, может приниматься в расчет непосредственно в ходе разработки продукции.*

Услуга 2.4 Выявление новых уязвимостей

PSIRT может принимать активное участие в процессе выявления новых уязвимостей, что позволяет решать проблемы защиты продукции и уменьшить необходимость в поддержании внешних связей и в перспективе затрачивать меньше усилий на координацию действий. Эта деятельность должна дополнять меры по проверке безопасности, являющиеся одним из компонентов жизненного цикла безопасной разработки (SDL). Среди всего прочего PSIRT может проводить оценку безопасности продукции до ее выпуска или на этапе технического обслуживания, а также передавать сотрудникам отдела исследований и разработки опыт использования средств проверки безопасности. Устранение уязвимостей, выявленных в ходе внутренней проверки и способных затронуть конечных пользователей, следует проводить таким же образом, как и устранение уязвимостей, выявленных внешними сторонами, в том числе путем проведения количественной оценки и составления отчетности, согласованной с выпуском исправлений.

***Цель**: выявление и устранение уязвимостей в продукции до того, как они будут выявлены внешними сторонами.*

***Результат**: накопление опыта, разработка процедур и механизмов внутреннего выявления уязвимостей продукции и потенциальное сокращение усилий, затрачиваемых на координацию действий.*

Функция 2.4.1 Оценка безопасности продукции

Оценка безопасности продукции – это проведение активного поиска еще не выявленных уязвимостей. Эта деятельность может включать широкий круг различных методов и инструментов, например тестирование на возможность проникновения или сканирование уязвимостей. Оценка защиты продукции методом серого ящика/черного ящика имитирует хакерскую атаку на компанию извне при том допущении, что злоумышленник не имеет информации о системе, подвергающейся атаке или имеет очень ограниченную информацию о ней.

***Цель**: выявление уязвимостей при помощи упреждающих механизмов.*

***Результат**: проведение контроля качества, дополняющего меры по проверке безопасности в рамках SDL.*

Подфункция 2.4.1.1 Оценка безопасности вашей продукции

Анализ результатов оценки безопасности, в ходе которой проверяются средства контроля безопасности вашей продукции, может оказаться весьма полезным для разработчиков, стремящихся к улучшению своей продукции до ее выпуска на рынок или в ходе подготовки исправления.

Подфункция 2.4.1.2 Оценка безопасности сторонних компонентов

Рекомендуется проводить расширенную специализированную оценку безопасности компонентов, полученных от третьей стороны, в дополнение к общим процедурам управления закупками. Это особенно касается критически важных компонентов, обеспечивающих надлежащее высокое качество продукции.

Функция 2.4.2 Поддержание высокого уровня осведомленности о новейших инструментах проверки безопасности

Коммерческие предприятия и соответствующие сообщества постоянно разрабатывают новые инструменты для проведения анализа безопасности и наступательные инструменты ее проверки. PSIRT должна поддерживать высокий уровень осведомленности об имеющихся новейших инструментах. Это необходимо для проведения оценок продукции, проверки фактов, выявленных внешними сторонами, или инструктирования команд разработчиков относительно выбора нужных инструментов для проведения внутренних проверок.

***Цель**: снабдить хорошо подготовленную группу экспертов необходимыми навыками по работе со сложными инструментами и предоставлять рекомендации по их использованию.*

***Результат**: использование наилучших имеющихся инструментов.*

Подфункция 2.4.2.1 Обучение сотрудников PSIRT использованию инструментов проверки безопасности

Обучение сотрудников – это основное условие поддержания высокого уровня осведомленности об имеющихся новейших инструментах проверки безопасности. Дополнительную информацию об обучении сотрудников PSIRT см. в разделе Услуга 6.3. Профессиональная подготовка валидационной группы.

Услуга 2.5 Показатели выявления уязвимостей

Рисунок 8. Показатели процесса выявления уязвимостей

Предоставление подробной информации о размерах, результативности или других показателях деятельности PSIRT необходимо для того, чтобы заинтересованные стороны были осведомлены об эффективности группы (см. также Основы оперативной деятельности, раздел III. B. Оценка и усовершенствование). Различные заинтересованные стороны могут придерживаться различных точек зрения, и такие показатели следует представлять, используя различные форматы артефактов (или взглядов). PSIRT должна знать, в каком формате каждая группа заинтересованных сторон желает получать такую информацию. PSIRT может использовать формат ключевых показателей деятельности (KPI).

***Цель**: предоставление данных о показателях и деятельности PSIRT. При помощи этих данных заинтересованные стороны могут оценить эффективность деятельности PSIRT в определенной области или при предоставлении определенной услуги.*

***Результат**: анализируя показатели PSIRT, заинтересованные стороны должны получить представление о том, насколько эффективно PSIRT предоставляет ту или иную услугу; им также должна быть дана возможность направлять отзывы в целях внесения корректировок в предоставление данной услуги.*

Функция 2.5.1 Оперативные отчеты

В оперативных отчетах представлена информация о числе и видах выявленных уязвимостей. Такие отчеты могут публиковаться на регулярной основе как внутри PSIRT, так и при участии внешних заинтересованных сторон.

***Цель**: регулярный сбор данных для составления отчетов общего характера.*

***Результат**: выявление областей, нуждающихся в проведении анализа, привлечении ресурсов, улучшениях.*

Подфункция 2.5.1.1 Сопоставление общего числа выявленных уязвимостей с числом подтвержденных уязвимостей

Эти данные помогают определить, какой объем ресурсов PSIRT тратит на устранение указанного числа уязвимостей. Данные могут быть представлены в разбивке по уровню подразделения, типу продукции или конкретным продуктам.

Подфункция 2.5.1.2 Общее число подтвержденных уязвимостей в разбивке по компонентам третьей стороны

Эти данные помогают оценить уровень риска, связанного с конкретными встроенными компонентами третьей стороны.

Подфункция 2.5.1.3 Общее число подтвержденных уязвимостей в разбивке по перечню общеизвестных слабых мест (CWE)

Эти данные могут быть учтены в жизненном цикле безопасной разработки и оказать воздействие на сферу обслуживания подготовки и обучения. Данные могут быть представлены в разбивке по уровню подразделения, типу продукции или конкретным продуктам.

Подфункция 2.5.1.4 Общее число выявленных уязвимостей в разбивке по использованному методу выявления уязвимостей

Эти данные позволяют определить уязвимости, легко поддающиеся выявлению. Данные могут быть учтены в жизненном цикле безопасной разработки и представлены в разбивке по уровню подразделения, типу продукции или конкретным продуктам.

Подфункция 2.5.1.5 Общее число выявленных уязвимостей в разбивке по источнику

Данные позволяют оценить степень известности PSIRT.

Функция 2.5.2 Отчеты о результатах деятельности

В отчетах о результатах деятельности представлена информация об эффективности реагирования организации на уязвимости с учетом принимаемых организацией мер по устранению уязвимостей защиты продукции и реагирования на них.

***Цель**: разработка показателей, определяющих успешность деятельности организации, и регулярный сбор данных для информирования руководства о выявленных рисках.*

***Результат**: информационные панели с информацией об успехах организации и возможностях усовершенствования ее деятельности.*

Подфункция 2.5.2.1 Показатель своевременного реагирования

Эти данные позволяют определить, насколько эффективно PSIRT соблюдает сроки, определенные в соглашении об уровне обслуживания, в отношении направления ответов на сообщения об уязвимостях.

Подфункция 2.5.2.2 Общее время недоступности каналов связи PSIRT

Эти данные позволяют определить, были ли каналы связи PSIRT доступны так, как это предусмотрено в соглашении об уровне обслуживания.

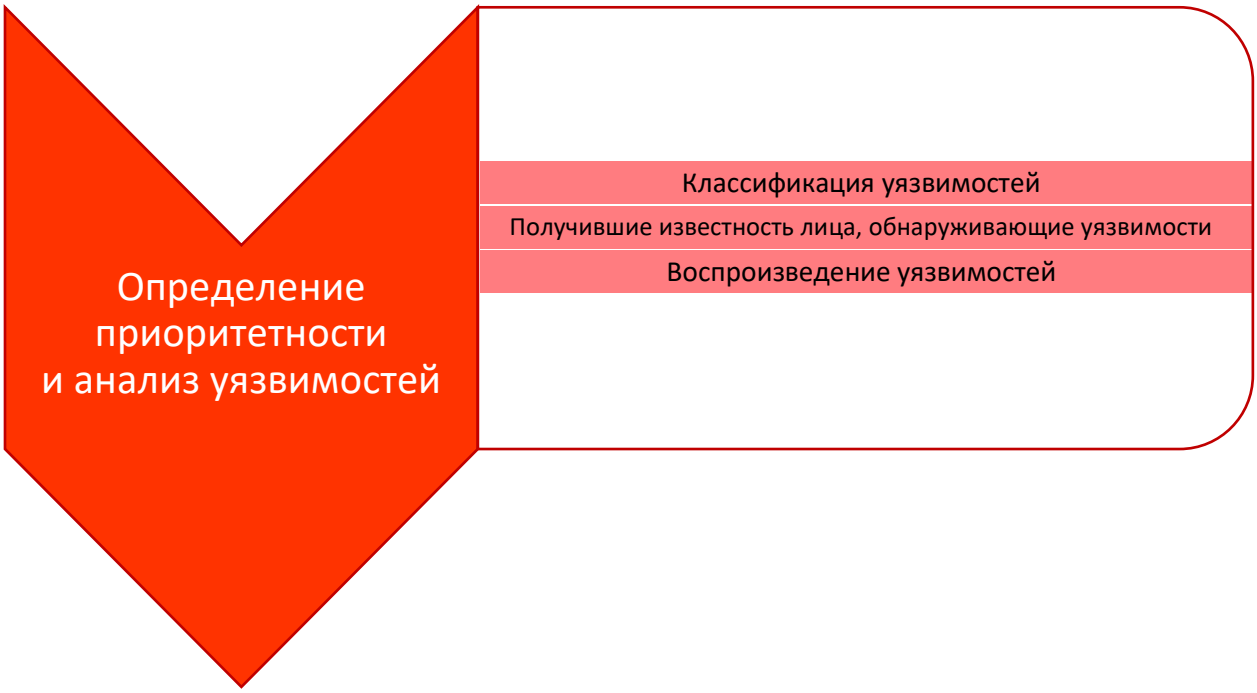
Подфункция 2.5.2.3 Показатель времени, затраченного на приоритизацию

Эти данные используются для определения времени, прошедшего с момента получения первого сообщения до завершения действий по приоритизации. Эти данные позволяют оценить результативность и/или рабочую нагрузку сотрудников PSIRT.

Подфункция 2.5.2.4 Число случаев полного раскрытия информации, число случаев активной эксплуатации уязвимостей на практике и число случаев выявления уязвимостей при помощи средств массовой информации

Эти данные позволяют оценить уровень риска для продукции заинтересованных сторон.

Сфера обслуживания 3



Получение сообщений об уязвимостях и определение их приоритетности входят в состав функции PSIRT по ведению дел. Порядок действий, которого придерживаются различные PSIRT, во многом одинаков, однако есть и определенные отличия, например, касающиеся непосредственного момента открытия дела или функций сотрудников в рамках этого дела. Если организации получают большое количество сообщений об уязвимостях, они могут рассмотреть возможность проведения первоначального отбора полученных сообщений для их подтверждения до открытия дела. Напротив, организации, получающие небольшое количество сообщений об уязвимостях, могут открыть дело и до определения их приоритетности. Конечная цель PSIRT заключается в разработке эффективной и четко определенной процедуры.

> ***Цель**: установить, каким образом будет определяться приоритетность сообщений об уязвимостях.*
>
> ***Результат**: разработка процедур для PSIRT и соответствующих групп разработчиков.*

Услуга 3.1 Классификация уязвимостей

Организации разрабатывают надлежащие критерии, позволяющие классифицировать подлежащие рассмотрению проблемы в зависимости от их типа и масштаба. Эти квалификационные критерии позволяют установить базовый уровень безопасности и эффективно определять приоритетность поступивших сообщений об уязвимости.

Рисунок 9. Процедура классификации уязвимости

Функция 3.1.1 Границы качества и пороги ошибок

Система оценки общеизвестных уязвимостей (CVSS) позволяет выделить основные характеристики уязвимости и дать количественную (числовую) оценку степени ее серьезности. Количественная оценка затем может быть преобразована в качественную (низкая, средняя, высокая или критическая), чтобы помочь организациям надлежащим образом оценить и определить приоритетность процессов управления уязвимостями, которые иногда называют границы качества и/или порог ошибок и используют для установления минимальных приемлемых уровней качества защиты и критериев определения приоритетности уязвимостей. Определение этих критериев до выпуска продуктов обеспечивает прозрачность процедуры обработки факторов уязвимости, так как PSIRT заранее определяет, что именно будет классифицировано как уязвимость продукции и должно быть устранено. Список общеизвестных уязвимостей и незащищенности (CVE) представляет собой перечень уязвимостей с идентификационными номерами, описаниями и по крайней мере одной наиболее часто упоминаемой публичной ссылкой, позволяющей понять, о какой проблеме идет речь.

***Цель**: определить четкие минимальные стандарты и критерии определения приоритетности для предоставления прозрачной информации внутренним и внешним заинтересованным сторонам.*

***Результат**: разработчики и лица, обнаружившие уязвимость, получают четкое представление о том, что является уязвимостью. Дополнительные критерии определения приоритетности позволят уменьшить неопределенность и разногласия в процессе управления жизненным циклом уязвимости – от первоначального определения приоритетности до распространения сообщений об исправлениях.*

Подфункция 3.1.1.1 Документальное оформление определений уязвимости безопасности продукции

Определения границ качества или порога ошибок должны быть задокументированы, храниться централизованно и составить компонент стандартной подготовки разработчиков/инженеров.

Подфункция 3.1.1.2 Взаимодействие с группами разработчиков продукции

Если организация выпускает широкий ассортимент продукции и в ее рамках действует несколько групп по разработке продуктов, крайне важно привлечь все эти группы к участию в разработке стандартных определений уязвимости безопасности продукции.

Функция 3.1.2 Непрерывное совершенствование

Зрелой PSIRT следует ориентироваться на непрерывное совершенствование и в случае необходимости проводить пересмотр своих квалификационных критериев, с тем чтобы отразить в них полученный ранее опыт, передовую отраслевую практику, изменения в продуктах и отзывы заинтересованных сторон. Крайне важно сообщать внутренним и внешним заинтересованным сторонам о произошедших переменах, чтобы изменить их ожидания.

***Цель**: признать, что квалификационные критерии подлежат пересмотру. Влияющие на PSIRT динамические факторы – такие как ожидания заинтересованных сторон, тенденции в отрасли или количество появляющихся уязвимостей – скорее всего приведут к частым корректировкам.*

***Результат**: гибкие критерии классификации уязвимостей будут способствовать развитию эффективной практики их классификации.*

Подфункция 3.1.2.1 Сбор данных

Сбор данных о процессе определения приоритетности, в том числе о количестве принятых сообщений, о количестве сообщений, соответствующих критериям уязвимости о количестве сообщений, не соответствующих критериям уязвимости и о любых выявленных расхождениях.

***Цель**: способствовать улучшениям за счет собранных данных.*

***Результат**: изменения границ качества и порогов ошибок ориентированы на данные.*

Услуга 3.2 Получившие известность лица, обнаруживающие уязвимости

С обретением зрелости PSIRT может заметить существование группы лиц, постоянно сообщающих об обнаружении уязвимостей в количестве, превышающем обычный объем. В таком случае рекомендуется, приняв во внимание репутацию лица, обнаружившего уязвимость, и традиционно высокое качество направляемых сообщений, обойти некоторые функции, такие как классификация и определение приоритетности, и сразу перейти к анализу причин уязвимости и проработке путей ее устранения. Это может помочь повысить эффективность процесса и укрепить отношения с лицами, обнаруживающими уязвимости.

> ***Цель**: изучить сообщество исследователей и узнать, кто чаще всего сообщает об уязвимостях в ваших продуктах и услугах, и рассмотреть возможность незамедлительного распространения сообщений, поступающих от заслуживающих особого доверия лиц, обнаруживающих уязвимости.*
>
> ***Результат**: сокращение сроков реагирования на сообщения, поступающие от лиц, занимающихся выявлением уязвимостей на высоком профессиональном уровне.*

Функция 3.2.1 База данных лиц, обнаруживающих уязвимости

Создание и ведение базы данных лиц и организаций, направлявших вам сообщения об уязвимостях, позволяет отслеживать историю сообщений, результаты и другие аспекты рассмотрения дел применительно к конкретному лицу, обнаружившему уязвимость**.**

> ***Цель**: повысить эффективность процедуры определения приоритетности и способствовать укреплению отношений с лицами, сообщения которых, как правило, отличаются высоким качеством.*
>
> ***Результат**: ускоренное рассмотрение сообщений, получаемых от квалифицированных специалистов. Лица, обнаруживающие уязвимости, удовлетворены результатами, а уязвимости устраняются до наступления возможных сроков обнародования соответствующей информации.*

Функция 3.2.2 Ускоренная обработка сообщений от получивших известность лиц, обнаруживающих уязвимости

Некоторые лица могут часто или постоянно (проверка/надежность) отыскивать дефекты программного обеспечения в ваших продуктах или услугах и сообщать о них. Например, они могут использовать стандартные инструменты фаззинга и направлять сообщения о сбоях без конкретного описания или подтверждения концепции. Если это лицо вам уже хорошо известно и вы убедились, что большинство указанных им проблем поддаются исправлению, рассмотрите вопрос

о том, чтобы полностью пропустить всю процедуру классификации/проверки и сразу перейти к процессу устранения уязвимости.

***Цель**: повысить эффективность процедуры определения приоритетности и способствовать укреплению отношений с лицами, сообщения которых, как правило, отличаются высоким качеством.*

***Результат**: ускоренное рассмотрение сообщений, получаемых от квалифицированных специалистов. Лица, обнаруживающие уязвимости, удовлетворены результатами, а уязвимости устраняются до наступления возможных сроков обнародования соответствующей информации.*

Функция 3.2.3 Сведения о лицах, обнаруживающих уязвимости

Рассмотрите возможность сбора сведений о лицах, обнаруживающих уязвимости, с тем чтобы соответствующие специалисты знали, как можно сотрудничать с ними наиболее эффективно. К числу таких сведений могут относиться данные о местонахождении лица, обнаружившего уязвимость, языках, на которых говорит это лицо, конференциях, в которых это лицо принимало участие, методологиях, использованных им для обнаружения уязвимостей, продуктах/технологиях, обычно привлекающих его внимание. Могут быть включены его ответы на вопросы о том, применяет ли данное лицо практику скоординированного раскрытия информации об уязвимости, хотело бы данное лицо представить результаты своих поисков на конференции, выплачивали ли вы данному лицу вознаграждение или предлагали другие льготы и т. д. Проконсультируйтесь с юридическим отделом и/или отделом по контролю за соблюдением требований, чтобы определить, какую информацию можно собирать и как долго ее можно хранить.

***Цель**: получить представление о людях, обнаруживающих уязвимости в ваших продуктах.*

***Результат**: возможность адаптации процедуры обработки сообщения с учетом конкретного лица, обнаружившего уязвимость, в целях получения оптимальных результатов.*

Функция 3.2.4 Определение качества сообщений от лиц, обнаруживших уязвимость

Организации могут рассмотреть возможность составления и публикации руководящих указаний, определяющих минимальные критерии качества сообщений об уязвимостях, с тем чтобы указать лицам, обнаружившим уязвимость, в какой информации вы нуждаетесь для того, чтобы оперативно оценить их сообщение. Основные виды необходимой информации могут включать в себя, помимо прочего, подробное описание уязвимости, ее пошаговое

воспроизведение, сведения о платформе (платформах), на которой производилось тестирование, и подтверждение концепции.

***Цель**: предоставить лицам, обнаружившим уязвимость, руководящие указания по базовым критериям качества сообщений об уязвимости.*

***Результат**: сведение к минимуму дискуссий между поставщиком и лицом, обнаружившим уязвимость, что позволяет поставщику быстро перейти к разработке плана устранения уязвимости.*

Услуга 3.3 Воспроизведение уязвимостей

Помимо классификации уязвимости, если не указано иное, PSIRT необходимо убедиться в том, что уязвимость, описанная в сообщении, может быть воспроизведена в целях проверки и изучения условий, приведших к ее возникновению.

***Цель**: предоставить инструменты и создать условия для классификации сообщений об уязвимостях.*

***Результат**: проведение эффективной, надежной и безопасной проверки сообщения об уязвимости.*

Рисунок 10. Подтверждение/воспроизведение уязвимости

Функция 3.3.1 Разработка соглашения об уровне обслуживания для воспроизведения уязвимости

PSIRT может не располагать достаточными техническими знаниями и опытом, чтобы воспроизводить все уязвимости, о которых поступают сообщения. PSIRT может нуждаться в консультациях, поддержке в работе или экспертных знаниях групп по разработке продукции или других групп, поэтому крайне важно подготовить и согласовать подробное соглашение, обеспечивающее доступ

к необходимым знаниям. В идеале рекомендуется привлекать к этой работе постоянных или временных сотрудников. Тем не менее если бюджетные ограничения не позволяют этого сделать, то в рамках деятельности PSIRT следует, как минимум, заранее найти технических специалистов в данной области, которых в случае возникновения инцидента можно будет незамедлительно привлечь к работе на ограниченный период времени.

***Цель**: признать, что PSIRT не располагает техническими знаниями и опытом для воспроизведения всех уязвимостей, о которых поступают сообщения.*

***Результат**: предварительное согласование с внутренними структурами позволит незамедлительно использовать их опыт и знания для воспроизведения уязвимостей.*

Функция 3.3.2 Тестовая среда для воспроизведения уязвимости

Для PSIRT или специализированной группы сотрудников следует создать специальную тестовую среду для воспроизведения уязвимости. Эту тестовую среду следует изолировать, чтобы защитить ее от действий злоумышленников, а также создать условия для подтверждения сообщения лица, обнаружившего уязвимость. Для создания безопасной среды можно использовать, при наличии такой возможности, специальную сетевую среду, имитационные модели или виртуализацию.

***Цель**: создание безопасной среды для изучения и воспроизведения уязвимостей.*

***Результат**: надлежащим образом развернутая тестовая среда для воспроизведения уязвимостей позволяет эффективно обрабатывать и классифицировать уязвимости, при этом ограничивая сферу действия уязвимости тестовой средой.*

Функции 3.3.3 Инструменты для воспроизведения уязвимостей

Группам сотрудников, занимающимся воспроизведением уязвимостей, о которых поступают сообщения, для выполнения этих операций необходимо иметь в своем распоряжении инструменты (например, средства отладки) и обновленные лицензии на продукты.

***Цель**: обеспечить группы сотрудников, занимающихся воспроизведением уязвимостей, необходимыми инструментами.*

***Результат**: обеспечение максимально возможной эффективности воспроизведения уязвимостей, о которых поступают сообщения.*

Функция 3.3.4 Хранение информации об уязвимостях

Рекомендуется обеспечивать безопасное хранение конфиденциальной информации, такой как сообщения об уязвимостях, файлы с подтверждением концепции и т. д., а также предоставлять доступ к этой информации только лицам, нуждающимся в доступе к ней, и обеспечивать безопасность сохраняемой и передаваемой информации. Например, см. ISO 27001.

***Цель**: обеспечить безопасность конфиденциальной и потенциально вредящей информации об уязвимостях.*

***Результат**: обеспечена сохранность конфиденциальной информации, доступ к ней ограничен, ее не затрагивает несанкционированное проникновение в первичную сеть организации.*

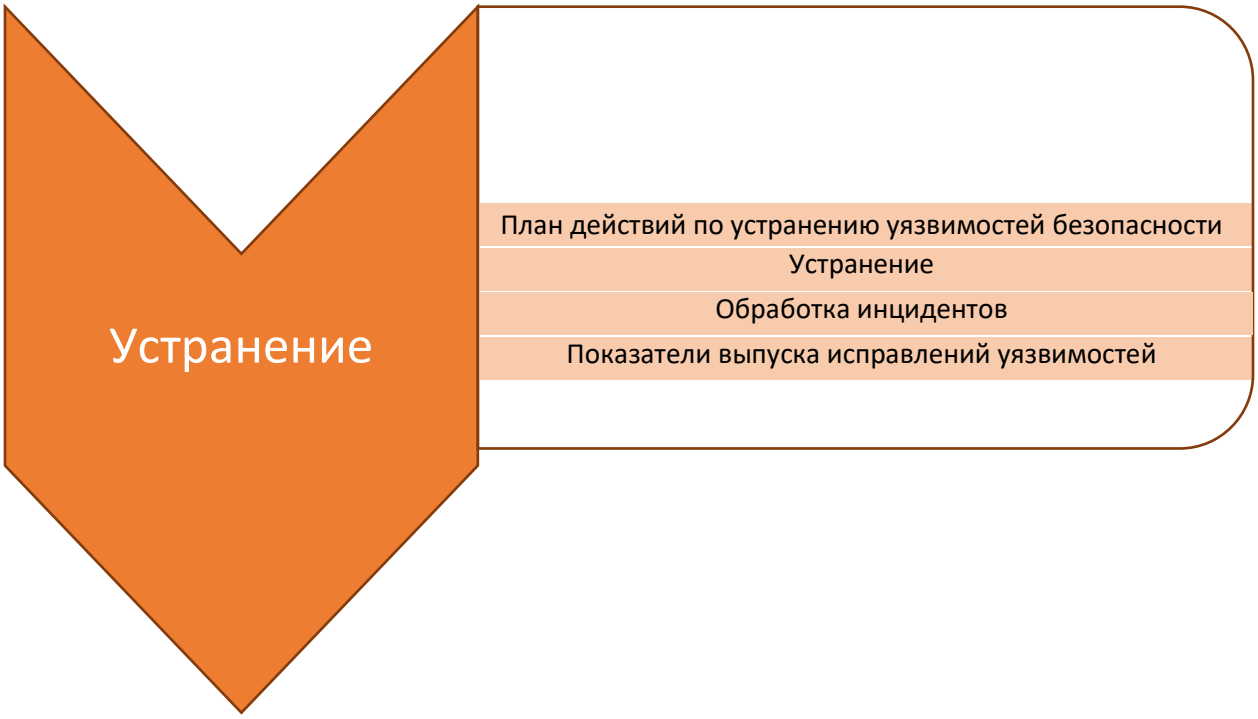
Функция 3.3.5 Продукты, находящиеся под воздействием уязвимости

В процессе воспроизведения уязвимости группа, проводящая анализ, должна установить, какие продукты оказались под воздействием уязвимости и существуют ли какие-либо варианты данной уязвимости. См. также раздел Функция 4.1.1. Управление жизненным циклом продукта.

***Цель**: получить полное представление о характере и масштабах уязвимости в продуктах.*

***Результат**: исправление уязвимости распространяется на все поддерживаемые продукты.*

Сфера обслуживания 4



Эта сфера обслуживания включает различные услуги, необходимые для внесения исправлений и передачи информации о них как заинтересованным сторонам, так и поставщикам нижнего уровня. Механизм внесения исправлений следует определять в зависимости от воздействия уязвимости на заинтересованные стороны в случае ее эксплуатации. Следует разработать процедуры, обеспечивающие внесение исправлений по предсказуемому графику, с тем чтобы заинтересованные стороны и поставщики нижнего уровня могли составить соответствующие планы тестирования и внесения исправлений.

> ***Цель**: определить необходимые процедуры и механизмы для внесения исправлений и передачи информации о них заинтересованным сторонам и поставщикам нижнего уровня.*
>
> ***Результат**: заинтересованные стороны и поставщики нижнего уровня получают возможность составлять соответствующие планы внесения исправлений.*

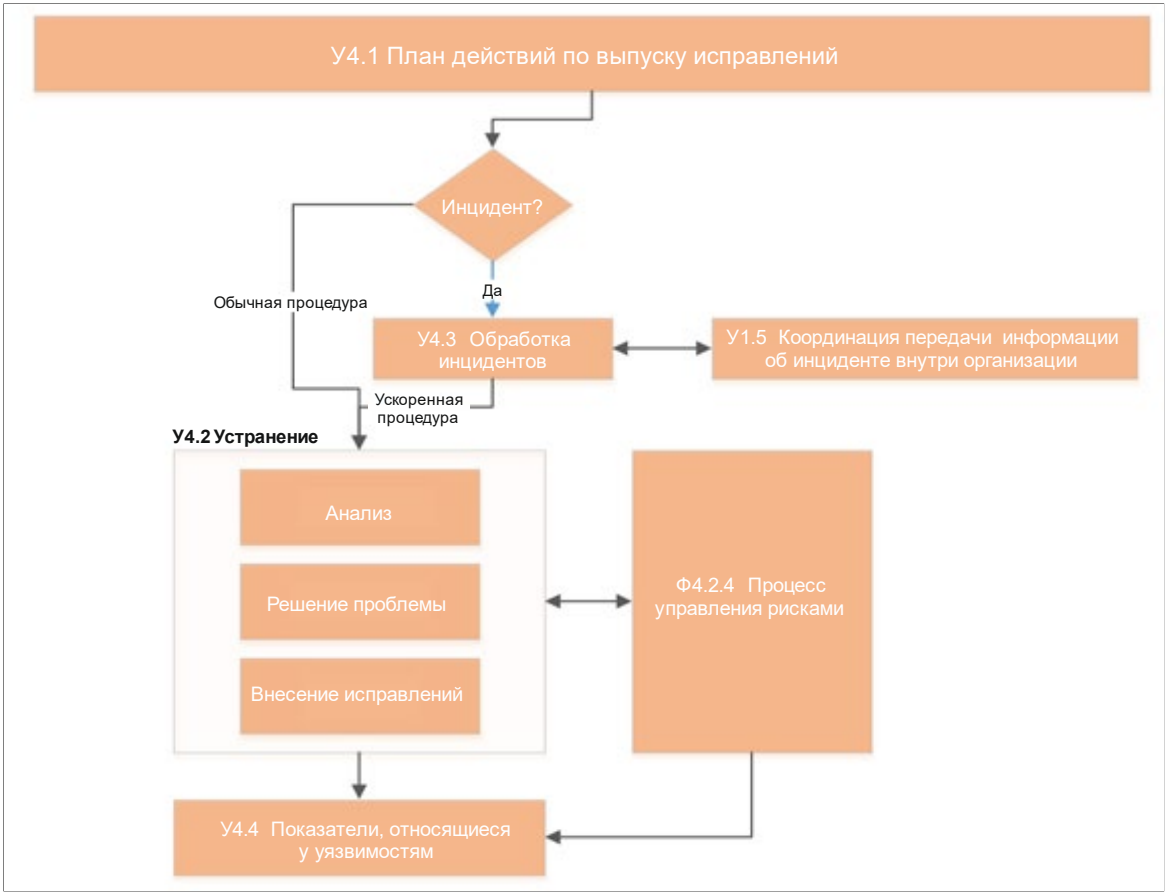


Рисунок 11. Пример базовой процедуры выпуска исправлений

Услуга 4.1 План действий по выпуску исправлений

Основная цель данной услуги – предоставление поставщику рекомендаций, касающихся его планов по установлению периодичности выпуска исправлений для поддерживаемых версий продукта на рынке. Заинтересованным сторонам, особенно в бизнес-среде, необходимо составить план размещения исправлений. В некоторых местах размещения, например в облаке, может действовать система автоматических обновлений или иная стратегия установки исправлений.

> ***Цель**: предоставить клиентам информацию о поддерживаемых продуктах, механизмах внесения исправлений и периодичности их внесения.*
>
> ***Результат**: заинтересованные стороны получат возможность заранее планировать установку исправлений уязвимостей.*

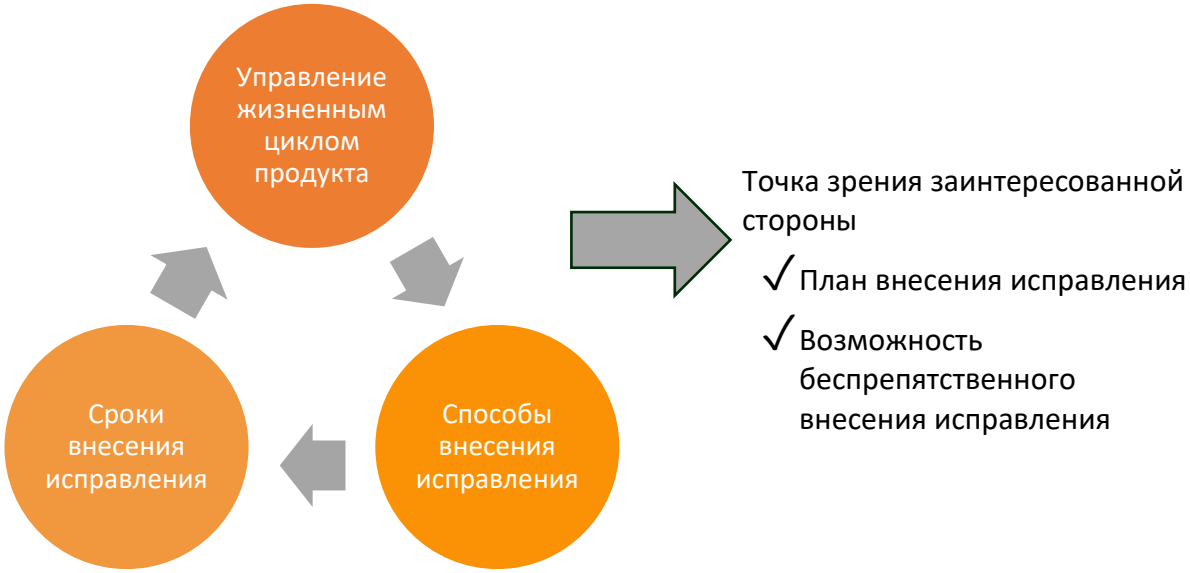


Рисунок 12. Создание основ для согласованных действий

Функция 4.1.1 Управление жизненным циклом продукта

Различные компании могут использовать разные стратегии оказания поддержки и заключать разные соглашения с заинтересованными сторонами. Учитывая эти факторы, PSIRT может совместно с бизнес-подразделениями/направлениями бизнеса и службами поддержки заинтересованных сторон определить порядок и условия поддержки продуктов, на которые больше не распространяется сфера действия поддержки или обязательства по ее оказанию. Это может зависеть от серьезности уязвимости и привести к необходимости вложений со стороны бизнес-подразделений/направлений бизнеса и помощи заинтересованных сторон.

***Цель**: предоставить группам разработчиков продуктов четкую стратегию оказания организацией поддержки по продуктам с уязвимостями безопасности.*

***Результат**: наличие отвечающей ожиданиям бизнес-подразделений/ направлений бизнеса четкой стратегии внесения исправлений в данные виды продукции.*

Подфункция 4.1.1.1 Перечень продуктов

Создание перечня всех выпущенных на рынок продуктов, чтобы гарантировать, что все поддерживаемые применимые продукты прошли оценку и в них были внесены исправления.

Подфункция 4.1.1.2 Модели поддержки

Получение представления о различных типах моделей поддержки продуктов, в том числе о платных услугах, расширенных гарантиях, договорах на техническое обслуживание или контрактах с конкретными заинтересованными сторонами.

Подфункция 4.1.1.3 Жизненный цикл продукта

Определение момента прекращения поддержки продукта в рамках его жизненного цикла.

Функция 4.1.2 Способ поставки исправлений

PSIRT могут совместно с группами разработчиков продуктов и группами поддержки заинтересованных сторон определить варианты поставки исправлений заинтересованным сторонам. Также следует разработать критерии, определяющие момент установки исправления с использованием указанных средств.

***Цель**: поддержка согласованного механизма поставки исправлений уязвимостей на основании ряда определенных условий.*

***Результат**: заинтересованные стороны получают возможность планировать и беспрепятственно осуществлять установку исправлений.*

Подфункция 4.1.2.1 Форматы упаковки продуктов

Получить представление о различных форматах упаковки, непосредственно относящихся к поставке исправлений (например, двоичный выполняемый формат, определение различий исходного кода (diff) и т. д.).

Подфункция 4.1.2.2 Поставка исправлений

Получить представление о различных механизмах поставки исправлений, таких как оперативные исправления, заплаты, корректировочные версии, обновления встроенного программного обеспечения, а также о способах распространения исправлений.

Подфункция 4.1.2.3 Установка исправлений

Определить способы установки исправлений в различные продукты, например, дистанционная установка исправлений, установка пользователем, автоматическое обновление или установка с выездом на место.

Функция 4.1.3 Периодичность поставки исправлений

Заинтересованным сторонам и поставщикам нижнего уровня необходимо составить план установки исправлений, чтобы поддержать уровень безопасности своей рабочей среды. Определение периодичности поставки исправлений позволит заинтересованным сторонам составлять график и планировать использование ресурсов для внесения необходимых обновлений в свою рабочую среду.

***Цель**: поддержание строгой периодичности предоставления исправлений заинтересованным сторонам.*

***Результат**: заинтересованные стороны получают возможность планировать и осуществлять установку исправлений.*

Подфункция 4.1.3.1 Периодичность поставки исправлений

Совместно с группами управления продуктами и выпуска продуктов определите желаемую периодичность поставки исправлений. Некоторые исправления являются частью выпускаемых обновлений функциональных средств и поставляются в соответствии с графиком выпуска этих обновлений. Для исправления других уязвимостей может понадобиться внесение экстренных корректировок; в таком случае выпуск исправлений проводится вне графика.

Подфункция 4.1.3.2 Документирование исключений

Определение и документирование исключений, при которых исправления не будут предоставляться с обычной периодичностью.

Услуга 4.2 Устранение

Эта услуга связана с управлением уязвимостями, о которых сообщили обнаружившие их лица, и включает анализ мер реагирования и смягчение последствий, определяет версии, в которые будут внесены исправления, и может учитывать способы предоставления исправлений. В рамках этой услуги могут быть также рассмотрены любые обходные решения, которые заинтересованная сторона может реализовать немедленно, до внесения исправлений.

***Цель**: обеспечить наличие процессов и примеров передового опыта по поставке исправления заинтересованной стороне исходя из того, какие именно продукты, версии и заинтересованные стороны затронуты.*

***Результат**: исправление, совместимое с затронутыми продуктами и потребностями заинтересованных сторон.*

Рисунок 13. Процесс устранения уязвимостей, о которых поступила информация

Функция 4.2.1 Анализ

Затронутый продукт может включать единичное программное приложение, микропрограмму или многочисленные аппаратные программы с различными версиями программных приложений или микропрограмм. Чтобы обеспечить удовлетворение потребностей заинтересованных сторон, при разработке плана устранения уязвимостей необходимо учитывать целый ряд параметров.

***Цель**: определить затронутые продукты, версии и заинтересованные стороны.*

***Результат**: исправление, совместимое с затронутыми продуктами и потребностями заинтересованных сторон.*

Подфункция 4.2.1.1 Проверка уязвимости

Проверка сообщения об уязвимости или инциденте на соответствие границам качества или порогу ошибок. См. Функция 3.1.1. Границы качества и пороги ошибок.

Подфункция 4.2.1.2 Внесение исправлений в версии продукта

Выявление затронутых продуктов и версий, а также любых вариантов, которые могут нуждаться в одновременном исправлении.

Подфункция 4.2.1.3 Пересмотр соглашений о поддержке

Проведение пересмотра соглашений о поддержке и моделей, связанных с затронутыми версиями продуктов. См. Подфункция 4.1.1.2 Модели поддержки.

Подфункция 4.2.1.4 Анализ основных причин

Определение дефектов разработки или внедрения, которые привели к возникновению уязвимости.

Подфункция 4.2.1.5 Определение механизма отсева уязвимостей

Например, уязвимость может представлять собой ложное срабатывание или ошибку в проекте системы безопасности.

Подфункция 4.2.1.6 Анализ способов устранения

Определение способов смягчения или устранения рисков, возникших в результате уязвимости.

Подфункция 4.2.1.7 Обходные приемы для устранения дефектов

Определить, существуют ли какие-либо обходные приемы для уменьшения воздействия уязвимости пока идет разработка исправления.

Подфункция 4.2.1.8 Исключения

Определить любые исключения, когда уязвимость не может быть устранена. См. Функция 4.2.4. Процесс управления рисками.

Функция 4.2.2 Проверка исправления

Перед выпуском исправления обнаруженной уязвимости оно должно быть проверено службой обеспечения качества (ОК), группой тестирования безопасности, а в соответствующих случаях – и лицом, обнаружившим уязвимость. Это включает процедуры и механизмы внутренней проверки исправления и сотрудничества с лицом, обнаружившим уязвимость, необходимые для проверки и утверждения исправления.

Цель: *разработать процедуры и механизм внутренней проверки исправления, а также, при необходимости, сотрудничества с лицом, обнаружившим уязвимость, для утверждения исправления.*

Результат*: утверждение выпускаемого исправления внутренними структурами и/или сторонним лицом, обнаружившим уязвимость.*

Подфункция 4.2.2.1 Проверка устранения уязвимостей, о которых были получены сообщения

Проверка с целью убедиться, что уязвимости, о которой были получены сообщения, устранены во всех случаях и во всех затронутых версиях продукта.

Подфункция 4.2.2.2 Завершение контроля исправления

Получение подтверждения завершения контроля исправления от ответственного инженера или группы специалистов по ОК. Проверку исправлений следует включить в стандартную практику тестирования или обеспечения качества.

Подфункция 4.2.2.3 Проверка исправления лицами, обнаруживающими уязвимость

Обеспечение взаимодействия со сторонними лицами, обнаруживающими уязвимости, или заинтересованными сторонами в целях проверки исправления.

Функция 4.2.3 Выпуск исправления

Сроки раскрытия информации в процессе выпуска исправления уязвимости, о которой поступило сообщение, могут разниться в зависимости от бизнес-требований вашей организации. Например, в некоторых случаях раскрытие информации увязывается с момента, когда исправление становится доступным; в других случаях раскрытие информации происходит после выпуска исправления, особенно если исправление вносится поэтапно; в некоторых случаях последовательность раскрытия информации может зависеть от отношений с заинтересованными сторонами (например, если это партнеры или особо значимые организации). Во всех случаях об этих сроках должны быть проинформированы ключевые отраслевые заинтересованные стороны, в том числе лицо, обнаружившее уязвимость.

Цель: *раскрытие информации увязывается с выпуском исправления, и заинтересованные стороны оповещаются об этих сроках.*

Результат*: выпуск исправления согласован с раскрытием информации заинтересованным сторонам.*

Подфункция 4.2.3.1 Вид раскрытия информации

Определение предпочтительного механизма раскрытия информации об уязвимости. Это может зависеть от серьезности или вида уязвимости.

Подфункция 4.2.3.2 При необходимости – координирование действий по раскрытию информации.

Подфункция 4.2.3.3 Размещение информации об исправлении во внутренней базе данных

Во взаимодействии со службой поддержки заинтересованных сторон или с иными заинтересованными сторонами разместите информацию об

исправлении, например на веб-портале, сайте поддержки заинтересованных сторон или в виде готовой к тиражированию версии (RTM).

Подфункция 4.2.3.4 Раскрытие информации об исправлении

Раскрытие информации о выявленной уязвимости во взаимодействии со службой поддержки заинтересованных сторон или с заинтересованными сторонами.

Функция 4.2.4 Процесс управления рисками

В обязанности PSIRT входит предоставление заинтересованным сторонам достаточной информации, позволяющей им оценить риски для своих систем, возникающие вследствие уязвимостей в их системах и в продуктах, поддерживаемых организацией, в которую входит PSIRT. Оценки управления рисками необходимо проводить во всей организации, если уязвимость не была устранена в течение определенного периода времени (в соответствии с соглашениями об уровне обслуживания или целями и задачами организации). Это предусматривает наличие прозрачного механизма для количественной оценки риска, а также информирование соответствующих заинтересованных сторон, включенных в реестр рисков организации.

***Цель**: определить процесс официального принятия рисков для любых уязвимостей, не устраненных в предусмотренные внутренним SLA сроки.*

***Результат**: прозрачность в отношении рисков во всей организации и гарантия того, что риски признаются и информация о них надлежащим образом передается на рассмотрение соответствующим заинтересованным сторонам.*

Подфункция 4.2.4.1 Уполномоченные должностные лица

Определить, какие должностные лица уполномочены принимать риск, например руководитель службы информационной безопасности (CISO)/ руководитель службы безопасности (CSO) или директор по управлению рисками, и каких должностных лиц необходимо информировать о риске.

Подфункция 4.2.4.2 Определение процесса управления рисками

Определить методы управления рисками для обработки и реагирования на риски в рамках организации, включая совокупность условий, запускающих этот процесс.

Подфункция 4.2.4.3 Оценка риска, в том числе количественная

Проведения оценки рисков, в том числе количественной, в целях понимания угрозы и ее последствий для бизнеса.

Подфункция 4.2.4.4 Внесение риска в реестр рисков

Оказание помощи CSO, директору по управлению рисками или другим заинтересованным сторонам в отслеживании статуса оценки риска и последующем осуществлении рекомендаций.

Подфункция 4.2.4.5 Рекомендации

Обновление реестра рисков с указанием выводов и рекомендаций.

Услуга 4.3 Обработка инцидентов

PSIRT необходимо иметь механизм для сокращения времени на устранение критических уязвимостей, которые можно определить как активные по-прежнему используемые эксплойты, уязвимости нулевого дня и несогласованное публичное раскрытие информации. Это услуга предусматривает вынесение рекомендаций в отношении инцидентов, а также оповещение заинтересованных сторон и координация действий по реагированию на инциденты, смягчению их последствий и возобновлению деятельности в целях сокращения времени с момента получения сообщения до выпуска исправления.

***Цель**: разработать план устранения критических уязвимостей и развить способность мобилизации всех ресурсов, необходимых для их устранения.*

***Результат**: выпуск экстренных исправлений в преддверии запланированного или публичного раскрытия информации об уязвимости или в иной ситуации, в которой заинтересованные стороны могут подвергаться риску и которая требует срочных действий.*

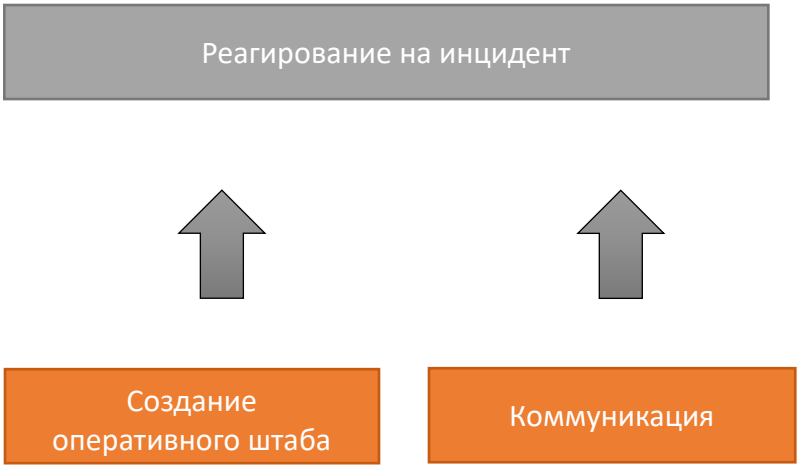


Рисунок 14. Обработка инцидентов

Функция 4.3.1 Создание оперативного штаба

Если требуется урегулировать инцидент, необходимо создать оперативный штаб, включающий PSIRT, юридический отдел, отделы по коммуникации, разработке, поддержке заинтересованных сторон, работе с поставщиками, а также иные подразделения при необходимости. Он может функционировать как в очном, так и в онлайновом формате, при условии что все стороны готовы по мере необходимости отвечать на запросы в безопасном режиме. Как правило, для обеспечения участия заинтересованных сторон используются как очные, так и онлайновые варианты работы. Для надлежащей поддержки процесса урегулирования инцидента необходимо заранее выделить ресурсы.

***Цель**: обеспечить доступность заинтересованных сторон, их готовность ответить на вопросы и дать руководящие указания. Обеспечить выделение соответствующих ресурсов для урегулирования инцидента.*

***Результат**: организация предоставления проверенных ресурсов.*

Подфункция 4.3.1.1 План урегулирования инцидента

Разработать план устранения критических уязвимостей и обеспечить возможность мобилизации всех ресурсов, необходимых для их устранения. Важно поддерживать готовность к реагированию на инциденты и проверять готовность этого плана на случай урегулирования непредвиденных и чрезвычайных ситуаций.

Подфункция 4.3.1.2 Определение ресурсов, необходимых для обработки инцидента и управления им

К ресурсам может относиться наличие конференц-залов, выделенных каналов связи и дополнительного персонала. Если для обработки инцидента требуется длительное время, необходимо решить вопросы проживания и питания участников.

Подфункция 4.3.1.3 Привлечение заинтересованных сторон к реализации плана реагирования на инцидент

Определить все основные заинтересованные стороны, чье участие в обработке инцидента предусмотрено вашим планом реагирования на инцидент. Определить все основные заинтересованные стороны, чье участие в обработке инцидента необходимо в соответствии с вашим планом реагирования на инцидент. См. Услуга 1.1. Взаимодействие с внутренними заинтересованными сторонами и Услуга 1.5. Координация деятельности по информированию об инцидентах в рамках организации.

Подфункция 4.3.1.4 Четкое распределение функций и ответственности в рамках управления инцидентом

Сотрудники должны знать свои обязанности и порядок действий в ситуации, требующей реагирования. Для подготовки основных участников реагирования необходимо проводить подготовку и ситуационные учения.

Функция 4.3.2 Управление инцидентом

При получении известия об инциденте основной задачей PSIRT и ее партнеров из числа заинтересованных сторон является уменьшение воздействия инцидента и восстановление бизнес-функций продукта, а также деятельности заинтересованных сторон.

***Цель**: разработка инструкции и следование плану действий для ограничения влияния инцидента.*

***Результат**: максимально оперативное восстановление нормального режима работы групп разработчиков продуктов и заинтересованных сторон.*

Подфункция 4.3.2.1 Сбор информации

Получение, каталогизация и хранение связанной с инцидентом информации.

Подфункция 4.3.2.2 Анализ

Обработка инцидентов зависит от аналитической деятельности, описанной в разделе "Анализ".

Подфункция 4.3.2.3 Реагирование

Услуги по уменьшению воздействия инцидента и принятию мер, направленных на восстановление бизнес-функций клиентов.

Подфункция 4.3.2.4 Отслеживание инцидентов

Документирование информации о действиях, предпринятых для разрешения инцидента, включая сбор критической информации, проведение анализа, меры по устранению инцидента и смягчению его последствий, а также разрешению инцидента и закрытию соответствующего вопроса.

Подфункция 4.3.2.5 Анализ результатов устранения инцидента

Рассмотрение принятых мер с целью определить, какие улучшения следует внести в процессы, политику, процедуры, ресурсы и инструменты для смягчения последствий и предотвращения нарушений в будущем.

Функция 4.3.3 План коммуникации

Все заинтересованные стороны и ответственные за выполнение задания должны быть проинформированы о последних по времени планах и ходе их реализации, чтобы не упускать ситуацию из-под контроля. При необходимости можно обращаться к руководству, чтобы устранить любые барьеры, которые могут препятствовать открытой коммуникации на основе сотрудничества во время инцидента.

***Цель**: разработать план коммуникации и определить основное лицо для связи по касающимся инцидента вопросам, чтобы держать всех в курсе последних событий.*

***Результат**: организация строго контролируемой коммуникации.*

Подфункция 4.3.3.1 Публикация информации для внутренних заинтересованных сторон

Ведение списков предназначенных для рассылки объявлений, предупреждений, массивов данных или других публикаций в целях обеспечения ситуационной осведомленности.

Подфункция 4.3.3.2 Четкое управление и координация деятельности по связи с общественностью

Предоставление средствам массовой информации и заинтересованным сторонам сведений только через уполномоченные организацией каналы. Сюда относятся и публикации в социальных сетях.

Подфункция 4.3.3.3 Информирование о деятельности по восстановлению

Информация о деятельности по восстановлению доводится до сведения внутренних заинтересованных сторон, высшего руководства и групп управления.

Подфункция 4.3.3.4 Сбор отзывов о результатах анализа работы в ходе инцидента

PSIRT проводит брифинги, посвященные анализу работы в ходе инцидента, и сбор отзывов для улучшения реагирования на инциденты, а также выполняет требования цикла по обеспечению безопасности на этапах разработки (SDL) (например, как выполнение SDL могло или должно было изначально предотвратить возникновение проблемы?).

Услуга 4.4 Показатели, относящиеся к уязвимостям

К подлежащим сбору данным относятся, помимо прочего, такие показатели, как масштаб проблемы, классификация, сроки исправления, затронутые продукты или услуги.

***Цель**: регулярный сбор данных для административной отчетности.*

***Результат**: выявление областей, требующих анализа, привлечения ресурсов, усовершенствования.*

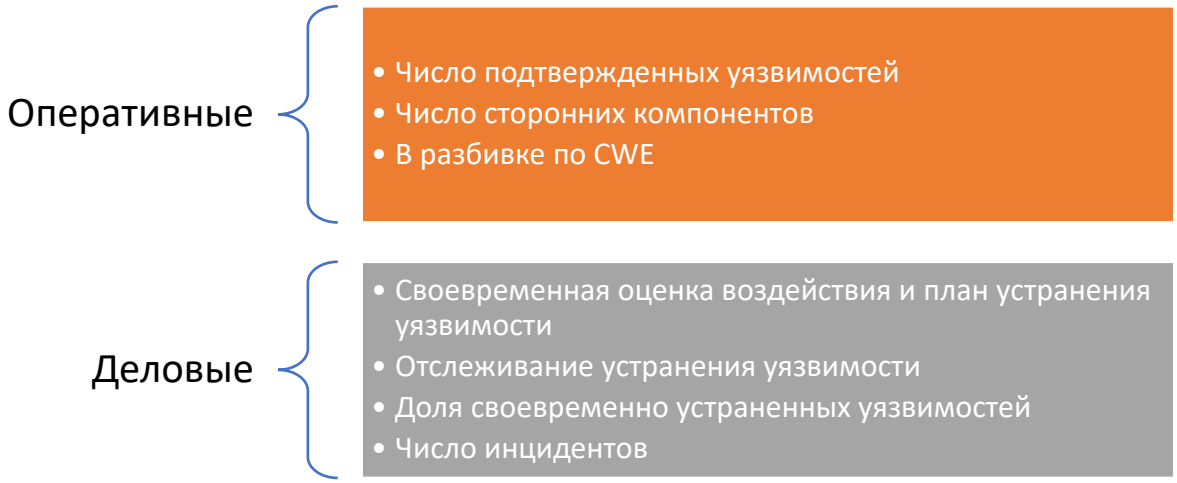


Рисунок 15. Оперативные и деловые показатели

Функция 4.4.1 Оперативные отчеты

Оперативные отчеты содержат информацию о числе и видах уязвимостей, о которых было сообщено, и о подтвержденных уязвимостях в различных продуктах и их версиях. Такие отчеты следует публиковать на регулярной основе внутри PSIRT при участии внутренних заинтересованных сторон.

***Цель**: регулярный сбор данных для составления отчетов общего характера.*

***Результат**: выявление областей, требующих анализа, привлечения ресурсов, усовершенствования.*

Подфункция 4.4.1.1 Отношение общего числа уязвимостей, о которых было сообщено, к числу подтвержденных уязвимостей (в разбивке по продуктам или подразделениям)

Эти данные помогают определить, какой объем ресурсов PSIRT тратит на устранение указанного числа уязвимостей.

Подфункция 4.4.1.2 Общее число подтвержденных уязвимостей в разбивке по сторонним компонентам

Эти данные помогают оценить уровень риска, связанного с конкретными встроенными сторонними компонентами.

Подфункция 4.4.1.3 Общее число подтвержденных уязвимостей в разбивке по перечню общеизвестных слабых мест (CWE) (по продуктам или подразделениям)

Эти данные могут быть переданы в сферу обслуживания цикла обеспечения безопасности на этапах разработки и учтены в сфере обслуживания по подготовке и обучению.

Функция 4.4.2 Отчеты о результатах деятельности

Отчеты о результатах деятельности содержат информацию о способности организации реагировать на уязвимости.

Цель: *разработка показателей успешности организации в выполнении ограниченных по срокам обязательств, определенных в SLA. Регулярные сбор, изучение и распространение данных, позволяющих оценить уровень достижения этих целей.*

Результат*: создание информационной панели с информацией об успехах возможностях усовершенствования.*

Подфункция 4.4.2.1 Своевременная оценка воздействия

Этот показатель позволяет определить, в какой мере группы разработчиков продукции соблюдают сроки завершения оценок воздействия, установленные в SLA.

Подфункция 4.4.2.2 Своевременное представление плана внесения исправлений

Этот показатель позволяет определить, в какой мере группы разработчиков продукции соблюдают установленный в SLA порядок представления плана внесения исправлений.

Подфункция 4.4.2.3 Отслеживание устранения уязвимости

Этот показатель позволяет определить, в какой мере группы разработчиков продукции соблюдают установленные в SLA сроки устранения уязвимости.

Подфункция 4.4.2.4 Доля своевременно устраненных уязвимостей

Этот показатель позволяет определить, в какой мере группы разработчиков продукции выполняют общие цели или соглашения в отношении внесения

исправлений с момента получения информации об уязвимости и до внесения исправления. Данные могут быть представлены в разбивке по степени серьезности или типу уязвимости (ассортимент продуктов, тип уязвимости).

Подфункция 4.4.2.5 Количество инцидентов

Эти данные позволяют оценить уровень риска для организации.

Сфера обслуживания 5

Важно создать основанную на принципах прозрачности и сотрудничества среду, в рамках которой поставщики, координаторы и лица, обнаружившие уязвимость, могут обмениваться информацией с заинтересованными сторонами и друг с другом и согласовывать взаимоприемлемые планы раскрытия информации. Благодаря таким партнерским отношениям могут быть удовлетворены основные потребности в области устранения уязвимостей, защиты заинтересованных сторон и выражения признательности лицам, обнаружившим уязвимость. Поставщик должен опубликовать свою политику раскрытия информации об уязвимостях, чтобы с ней могли ознакомиться координаторы, другие поставщики, а также лица, обнаруживающие уязвимости.

Рисунок 16. Процесс уведомления об уязвимости

***Цель**: обеспечение прозрачности для заинтересованных сторон и партнеров посредством сотрудничества с лицами, обнаружившими уязвимость, координаторами и поставщиками нижнего уровня в целях ответственного раскрытия информации об уязвимостях и их исправлениях.*

***Результат**: повышение уровня доверия, сотрудничества и контроля за раскрытием информации.*

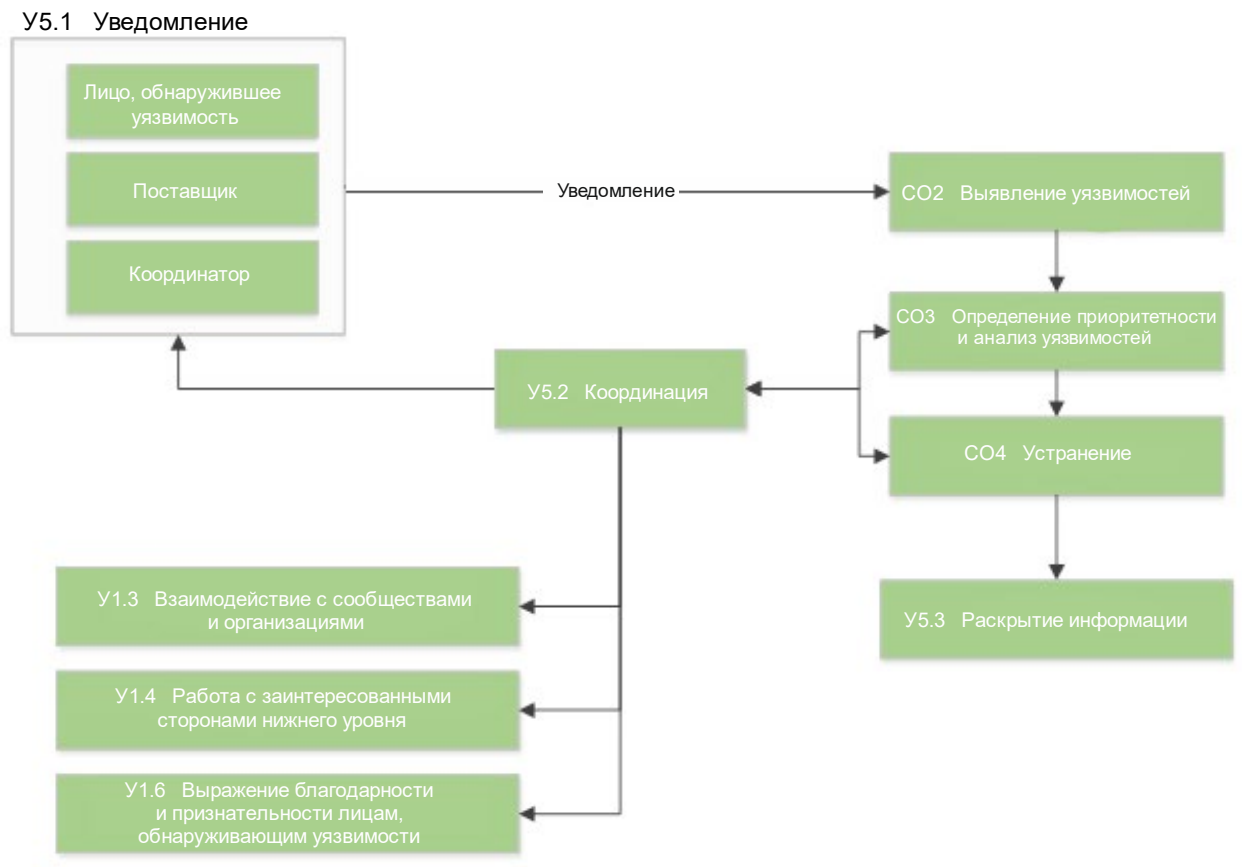


Рисунок 17. Общий пример координации действий при обнаружении уязвимости

Услуга 5.1 Уведомление

Эта услуга предусматривает определение надлежащего процесса уведомления, в рамках которого заинтересованным сторонам своевременно предоставляется информация о стратегии смягчения последствий, исправлениях уязвимости и обходных решениях, с тем чтобы они на основе этой информации могли надлежащим образом осуществлять

планирование. В некоторых случаях между поставщиками могут заключаться договорные соглашения, согласно которым, например, поставщик верхнего уровня должен будет предупредить о выявленных уязвимостях или известных инцидентах поставщика нижнего уровня. Цель процесса уведомления заключается в том, чтобы все поставщики и заинтересованные стороны могли получить представление о риске, возникающем в результате уязвимости, и управлять им.

***Цель**: обеспечение прозрачности для поставщиков и лиц, обнаруживающих уязвимости, на основе сотрудничества.*

***Результат**: повышение уровня доверия и сотрудничества с лицами, обнаруживающими уязвимости.*

Функция 5.1.1 Промежуточный поставщик (поставщик нижнего уровня)

Промежуточный поставщик, например OEM или партнер, может разрабатывать и/или производить комплектующие, подсистемы или программное обеспечение, которые используются в конечном продукте другого поставщика. В этих случаях их PSIRT должны принять меры для предоставления своим поставщикам информации об уязвимостях, полученной в результате обмена. Они должны быть осведомлены о политике устранения уязвимостей, которой придерживаются различные поставщики. Иногда эти ожидания закрепляются договорными соглашениями. Необходимо как можно скорее достигнуть договоренности о сроках устранения уязвимостей и раскрытия информации.

***Цель**: создание условий для сотрудничества и четкое определение ожиданий во взаимоотношениях между OEM и партнерами и другими поставщиками.*

***Результат**: повышение уровня доверия, сотрудничества и контроля за раскрытием информации между всеми участвующими сторонами.*

Подфункция 5.1.1.1 Обязанность PSIRT предоставлять информацию промежуточным поставщикам

Получив информацию об уязвимостях от своих заинтересованных сторон, PSIRT должна уведомлять об этих уязвимостях PSIRT промежуточных поставщиков.

Подфункция 5.1.1.2 Обязанность промежуточных поставщиков в отношении предоставления информации

Промежуточный поставщик, поставляющий компоненты или инструменты поставщику, получив напрямую информацию об уязвимостях, должен уведомлять о них PSIRT своего поставщика.

Подфункция 5.1.1.3 Договорные соглашения

PSIRT должна выявить всех промежуточных поставщиков и рассмотреть возможность сотрудничества с юридическим отделом, с тем чтобы добиться включения в договорные соглашения дополнительных пунктов, обеспечивающих своевременное реагирование на уязвимости.

Подфункция 5.1.1.4 Направление PSIRT уведомлений заинтересованным сторонам

PSIRT поставщиков могут передавать информацию своим заинтересованным сторонам, особенно если промежуточный поставщик не может устранить уязвимость или устранение занимает значительное время. В некоторых случаях PSIRT поставщика может использовать многоэтапную процедуру уведомления и информировать те заинтересованные стороны, которые в наибольшей степени могут быть затронуты конкретной уязвимостью.

Функция 5.1.2 Координаторы

PSIRT может обратиться к координатору с просьбой принять участие в информировании других поставщиков, а также в согласовании сроков внесения исправлений в их бюллетени безопасности, особенно если задействованы несколько поставщиков. Координаторы, такие как Координационный центр групп CERT (CERT/CC)[12]или сторонние координаторы, играют весьма полезную роль, привлекая множество различных организаций к взаимодействию и совместной работе над устранением уязвимости.

***Цель**: координаторов можно попросить включиться в процесс и помочь организации, в рамках которой функционирует PSIRT, как в информировании всех поставщиков об уязвимости, так и в совместной работе над ее устранением.*

***Результат**: повышение уровня доверия, сотрудничества и контроля за раскрытием информации между всеми участвующими сторонами.*

Подфункция 5.1.2.1 Выявление координаторов

Документирование и классификация координаторов на основании политики раскрытия информации об уязвимостях.

Подфункция 5.1.2.2 Вовлечение координаторов

Сотрудничество с координаторами в целях гарантированного предоставления информации PSIRT всех затронутых поставщиков.

[12] www.cert.org

Функция 5.1.3 Лицо, обнаружившее уязвимость

Лицо, обнаружившее уязвимость, например клиент или сторонний исследователь, может уведомить PSIRT об уязвимости, используя каналы, описанные в разделе Сфера обслуживания 2. Выявление уязвимостей.

***Цель**: создание условий для сотрудничества с лицами, выявляющими уязвимости, и четкое формулирование их ожиданий.*

***Результат**: повышение уровня доверия, сотрудничества и контроля за раскрытием информации с участием лиц, обнаруживших уязвимость.*

Услуга 5.2 Координация

В соответствующих случаях PSIRT поставщика следует предусмотреть возможность обмена информацией об уязвимостях с координаторами или другими поставщиками. Они должны быть осведомлены о политике поставщика в отношении обработки уязвимостей. Следует незамедлительно согласовать сроки устранения уязвимостей и раскрытия соответствующей информации.

***Цель**: документирование уязвимостей, устраненных из продукта в результате установки исправления.*

***Результат**: ясность в отношении преимуществ установки исправления и его источника.*

Функция 5.2.1 Двусторонняя координация

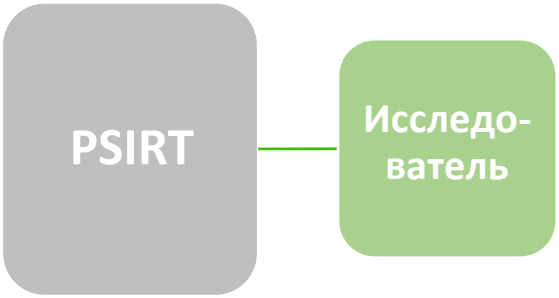


Рисунок 18. Двусторонняя координация

PSIRT поставщика отвечает за поддержание связи с лицами, сообщающими о потенциальных уязвимостях. Для поставщиков важно иметь представление о намерениях лиц, обнаруживающих уязвимость, их планах и позиции в отношении уязвимостей в целом, с тем чтобы способствовать скоординированному раскрытию информации в согласованные сроки. PSIRT следует рассмотреть возможность

выражения признательности лицам, сообщающим об уязвимостях, если они придерживаются принципов публичного раскрытия информации.

***Цель**: создание атмосферы сотрудничества, придающей лицам, обнаруживающим уязвимости, уверенность в том, что к ним отнесутся серьезно.*

***Результат**: согласованный план раскрытия информации, предусматривающий высокую оценку усилий лица, обнаружившего уязвимость.*

Подфункция 5.2.1.1 Получение сообщения

Подтвердить получение сообщения об уязвимости от стороннего лица, обнаружившего уязвимость.

Подфункция 5.2.1.2 Регулярное обновление информации

Регулярно предоставлять лицу, обнаружившему уязвимость, обновленную информацию о текущем положении дел в отношении выявленной уязвимости.

Подфункция 5.2.1.3 Проверка исправления лицом, обнаружившим уязвимость

Предоставить лицу, обнаружившему уязвимость, средство для ее устранения, чтобы он также мог проверить факт исправления.

Подфункция 5.2.1.4 Выражение признательности лицу, обнаружившему уязвимость

Выразить признательность лицу, обнаружившему уязвимость, упомянув его вклад в устранение уязвимости. Поставщику следует убедиться в том, что лицо, обнаружившее уязвимость, не возражает против такого упоминания.

Функция 5.2.2 Координация действий с несколькими поставщиками

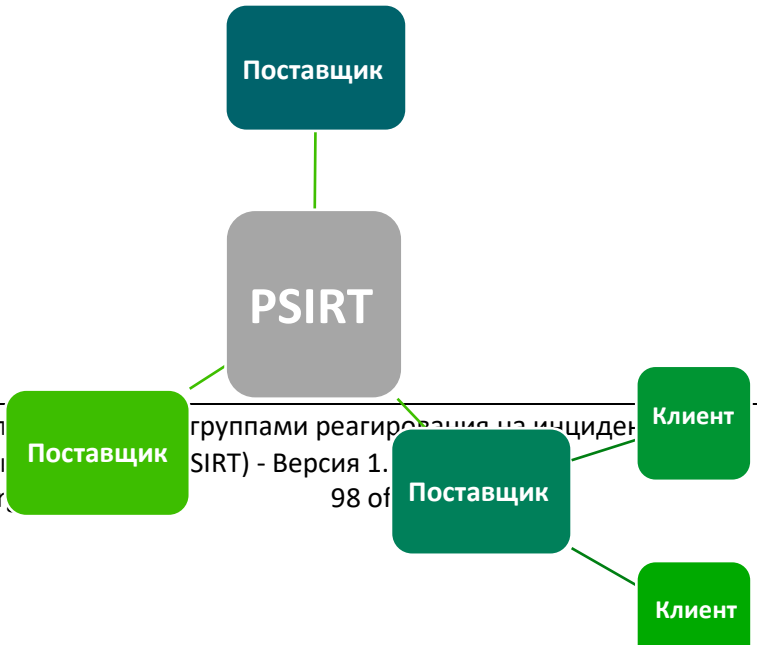


Рисунок 19. Координация действий с несколькими поставщиками

В соответствующих случаях PSIRT поставщика следует предусмотреть возможность обмена информацией об уязвимостях с координаторами или другими поставщиками. Они должны быть осведомлены о политике поставщика в отношении обработки уязвимостей. Следует незамедлительно согласовать сроки устранения уязвимостей и раскрытия соответствующей информации.

***Цель**: обеспечение прозрачности для заинтересованных сторон и партнеров посредством сотрудничества со всеми сторонами в целях ответственного раскрытия информации об уязвимостях и их устранения.*

***Результат**: повышение уровня доверия, сотрудничества и контроля за раскрытием информации.*

Таблица 1. Пример многосторонней координации

Широкий круг заинтересованных сторон	Взаимоотношения	Заинтересованность в координации
Поставщики верхнего уровня	Технологии предоставляет поставщик OEM	Для обеспечения внесения исправлений поставщикам верхнего уровня рекомендуется вести работу со своими заинтересованными сторонами нижнего уровня (см. Услуга 1.4)
Поставщики нижнего уровня	Получают технологии от поставщика верхнего уровня	Чтобы получать уведомления о необходимости внесения исправления, поставщикам нижнего уровня рекомендуется выявлять сообщества поставщиков партнеров верхнего уровня и взаимодействовать с ними (см. Функция 1.3.1)

Подфункция 5.2.2.1 Получение сообщения

PSIRT поставщика подтверждает получение сообщения об уязвимости от поставщика или координатора.

Подфункция 5.2.2.2 Выявление затронутых поставщиков

PSIRT поставщика или координатору может потребоваться выявить поставщиков, затронутых сообщением об уязвимости.

Подфункция 5.2.2.3 Распространение информации об уязвимости

PSIRT поставщика или координатор распространяют информацию об уязвимости среди различных поставщиков.

Подфункция 5.2.2.4 Планирование выпуска исправлений

PSIRT поставщика или координатор согласуют с поставщиками сроки разработки и выпуска исправления, а также возможность получения исправления поставщиками нижнего уровня.

Подфункция 5.2.2.5 Проверка исправления

PSIRT поставщика или координатор совместно с поставщиками проверяют, устраняет ли данное исправление дефекты безопасности.

Подфункция 5.2.2.6 Координация действий по раскрытию информации

PSIRT поставщика или координатор проводят переговоры со всеми поставщиками, чтобы согласовать способы раскрытия информации об уязвимости и сроки ее публикации.

Услуга 5.3 Раскрытие информации

После выпуска исправления дефектов безопасности необходимо надлежащим образом раскрыть информацию, чтобы заинтересованные стороны и поставщики были уведомлены об этом исправлении. Необходимо четко определить аудиторию для каждого уведомления (для различных видов уведомлений может быть своя целевая аудитория).

***Цель**: документирование внесения изменений в код и выпуск исправления дефектов безопасности.*

***Результат**: ясность в отношении исправлений, внесенных в код, и их источника.*

Функция 5.3.1 Сопроводительная записка

Сопроводительная записка, включая файл readme и хронологию изменений, должна содержать ссылку(и) на CVE для этого исправления. В сопроводительной записке должно быть четко указано, как именно была устранена уязвимость.

***Цель**: предоставить информацию об исправлениях, внесенных в обновленный код.*

***Результат**: заинтересованные стороны могут защититься от возможных рисков, связанных с уязвимостью.*

Подфункция 5.3.1.1 Раскрытие информации в сопроводительной записке

Определите, информация о каких уязвимостях должна быть раскрыта в сопроводительной записке.

Подфункция 5.3.1.2 Рассмотрение сопроводительной записки

Определите порядок рассмотрения.

Подфункция 5.3.1.3 Утверждение сопроводительной записки

Провести рассмотрение и утвердить раскрытие информации.

Функция 5.3.2 Бюллетень безопасности

Поставщикам следует иметь механизм, позволяющий публиковать на открытой веб-странице бюллетень безопасности для заинтересованных сторон и раскрывать информацию об устраненных уязвимостях.

***Цель**: создание публичного хранилища опубликованных бюллетеней безопасности.*

***Результат**: бюллетени безопасности доступны широкому кругу лиц для рассмотрения и принятия мер.*

Подфункция 5.3.2.1 Шаблон бюллетеня безопасности

Создайте шаблон бюллетеня безопасности. Он должен включать заголовок, резюме, перечень CVE, статус поддерживаемого продукта и его воздействия, выражение признательности, справочные материалы и информацию о пересмотрах.

Подфункция 5.3.2.2 Способ распространения бюллетеней безопасности

Определите механизмы распространения бюллетеней безопасности, включая, помимо прочего, веб-документ, RSS-канал или подписку.

Подфункция 5.3.2.3 Форматирование бюллетеней безопасности

Чтобы заинтересованные стороны и клиенты могли ознакомиться с бюллетенями при помощи средств автоматизации, рассмотрите возможность публикации этих документов в машиночитаемом формате, таком как единая основа бюллетеней безопасности[13] (Common Security Advisory Framework или CSAF).

Подфункция 5.3.2.4 Инициирование публикации бюллетеней безопасности

Определите набор условий, при которых может быть инициирована публикация бюллетеней безопасности. Например, необходимость предпринять действия для уведомления заинтересованных сторон о том, что среда выполнения программ исправлена (сценарий несанкционированного проникновения).

Подфункция 5.3.2.5 Присвоение CVE

Определите процедуру присвоения уязвимости идентификатора CVE.

Подфункция 5.3.2.6 Выражение признательности лицу, обнаружившему уязвимость

Выясните, понравится ли лицу, обнаружившему уязвимость, если ему будет публично выражена признательность или будет упомянуто его имя.

Подфункция 5.3.2.7 Планирование раскрытия информации

Определите процедуру рассмотрения, в частности выявите заинтересованные стороны и определите сроки раскрытия информации.

Подфункция 5.3.2.8 Процедура пересмотра инструкций по безопасности

Проведите пересмотр вместе с определенными заинтересованными сторонами.

Функция 5.3.3 Статьи базы знаний

Поставщикам следует иметь механизм публикации статей базы знаний, которые могут сопровождать определенные средства устранения уязвимостей безопасности, считающиеся менее серьезными, или же использоваться для объяснения, почему некоторые уязвимости, о которых поступили сообщения, были отклонены как ложно позитивные.

***Цель**: создать хранилище статей базы знаний.*

[13] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf

***Результат**: статьи базы знаний доступны для ознакомления и использования клиентами.*

Подфункция 5.3.3.1 Раскрытие информации в статьях базы знаний

Определите, информацию о каких уязвимостях следует раскрывать в статьях базы знаний.

Подфункция 5.3.3.2 Пересмотр статей базы знаний

Определите процедуру пересмотра статей базы данных.

Подфункция 5.3.3.3 Утверждение статей базы данных

Проведите пересмотр процедуры раскрытия информации и утвердите ее.

Функция 5.3.4 Коммуникация с внутренними заинтересованными сторонами

Помимо руководителей и владельцев компании, которых необходимо уведомлять о планах распространения информации об уязвимости, имеется также множество сотрудников, которые ежедневно непосредственно взаимодействуют с заинтересованными сторонами как лично, так и по телефону. Заблаговременное конфиденциальное уведомление их о предстоящем выпуске бюллетеней безопасности и ответах на часто задаваемые вопросы позволит подготовиться сотрудникам, которым будут задавать вопросы после публикации.

***Цель**: информирование руководителей и владельцев компании, подразделения, отвечающие за глобальные коммуникации, и сотрудников, взаимодействующих с заинтересованными сторонами, о готовящихся к выпуску бюллетенях безопасности и утвержденных ответах.*

***Результат**: сотрудники смогут отвечать на вопросы заинтересованных сторон и средств массовой информации в день публикации бюллетеня, что позволяет контролировать подачу информации.*

Подфункция 5.3.4.1 Взаимодействие с внутренними заинтересованными сторонами

Вместе с внутренними заинтересованными сторонами разработайте и/или пересмотрите формулировки, которые их сотрудники смогут использовать при общении с клиентами по вопросам уязвимостей.

Услуга 5.4 Показатели уязвимости

К подлежащим сбору данным относятся, помимо прочего, такие показатели, как масштаб проблемы, классификация, сроки исправления, затронутые продукты или услуги.

***Цель**: регулярный сбор данных для административной отчетности.*

***Результат**: выявление областей, требующих анализа, привлечения ресурсов, усовершенствования.*

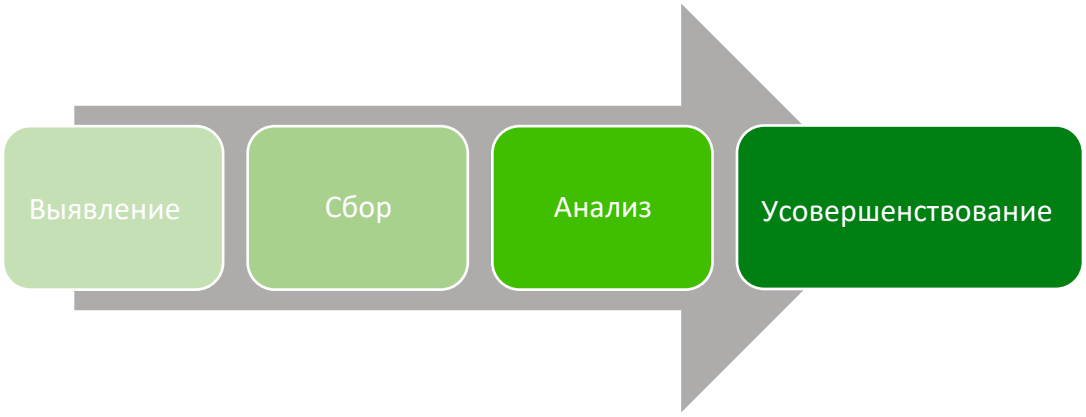


Рисунок 20. Процесс сбора данных об уязвимости

Функция 5.4.1 Оперативные отчеты

Оперативные отчеты могут содержать дополнительную информацию об объеме раскрываемой информации, а также о количестве просмотров страницы. Такие отчеты следует публиковать на регулярной основе как внутри PSIRT, так и среди внутренних заинтересованных сторон.

***Цель**: регулярный сбор данных для составления отчетов общего характера.*

***Результат**: выявление областей, требующих анализа, привлечения ресурсов, усовершенствования.*

Подфункция 5.4.1.1 Количество опубликованных бюллетеней безопасности

Можно сообщить о числе различных случаев раскрытия информации в целом и в разбивке по продукту. Это может помочь группе разработчиков получить необходимые технические ресурсы.

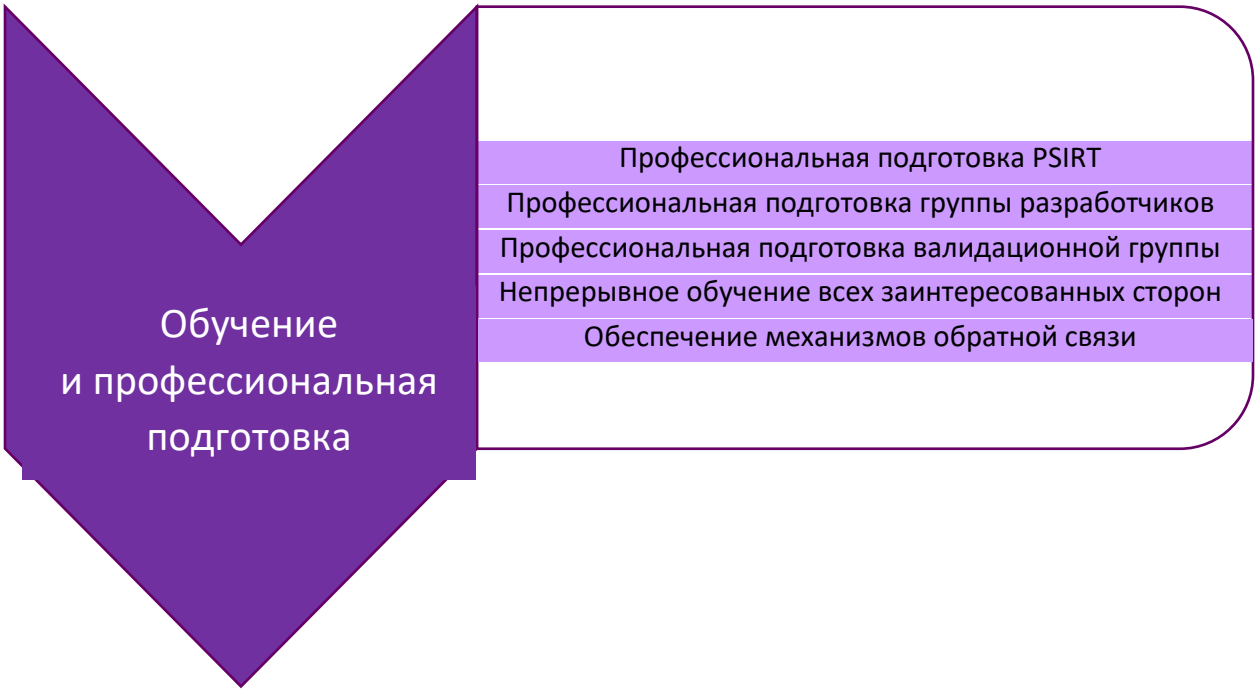
Подфункция 5.4.1.2 Количество CVE, опубликованных в национальной базе данных об уязвимостях (NVD)

Количество присвоенных CVE может способствовать повышению вашего статуса до организации, обладающей правом присвоения CVE идентификатора (CNA).

Подфункция 5.4.1.3 Просмотры страниц бюллетеней безопасности

Если ваш бюллетень безопасности просматривает небольшое число заинтересованных сторон, это может побудить вас переориентировать вашу стратегию на заблаговременное направление уведомлений.

Сфера обслуживания 6



Сфера обеспечения безопасности продукции претерпевает постоянные изменения, поскольку новые технологии, услуги и интеграция делают профессиональную подготовку и обучение одним из основных приоритетов для специалистов в области безопасности. Программное обеспечение используется во всех компонентах окружающего нас мира, от автомобилей до холодильников, и поэтому удовлетворение потребностей в обеспечении безопасности продукции никогда еще не было столь важным. PSIRT играют ключевую роль в обеспечении поддержки насыщенной учебной программы для обучения всех заинтересованных сторон тонкостям разработки, валидации и поставки продуктов или услуг, соответствующих стандартам современного соединенного мира.

Потребности в профессиональной подготовке и обучении могут значительно отличаться в различных подразделениях корпорации. Задачи, которые стоят перед разработчиками микропрограммного обеспечения и разработчиками программных услуг, существенно отличаются и зачастую требуют узкоспециализированной и уникальной подготовки. Для данного документа мы распределим потребности в подготовке заинтересованных сторон на четыре группы: PSIRT, разработка продукции, проверка продукции и иные заинтересованные стороны, вовлеченные в деятельность PSIRT.

1) **Подготовка PSIRT** уникальна, поскольку члены PSIRT должны разбираться во многих аспектах, таких как правовые вопросы, связь и разработка продукции.

2) **Разработка продукции** (внутреннее проектирование и разработка) — разработчикам требуется подготовка в конкретных областях, следовательно, им необходимо соответствующее специализированное обучение. К разработке защищенного микропрограммного обеспечения, которое сложно обновить в производственных условиях, предъявляются совсем иные требования, чем к проектированию настольных приложений.

3) **Проверка продукции** (внутреннее проектирование и разработка) — проверяющим требуется непрерывное обучение для ознакомления с новейшими инструментами и методами для проведения таких операций, как тестирование на возможность проникновения, сканирование на предмет уязвимостей и ранняя проверка проекта в целях выявления проблем до того, как возникнет необходимость в их устранении.

4) **Все остальные заинтересованные стороны** — эта группа представляет собой аудиторию с более низким уровнем технической подготовки, которой требуется надежная база для понимания основ разработки, проверки и поставки безопасных продуктов, а также реагирования в том случае, если в поставляемом продукте имеется уязвимость.

Обучение безопасной разработке не рассматривается в рамках программы подготовки PSIRT и выходит за рамки ее деятельности. Тем не менее важно, чтобы PSIRT занимали ведущие позиции в отношении всех аспектов, связанных с выводом на рынок безопасных продуктов, в связи с чем они должны сотрудничать с различными группами разработчиков, чтобы обеспечить проведение соответствующего обучения. Во многих небольших организациях может не быть отдельной группы, отвечающей за разработку продуктов с акцентом на безопасность. В этих случаях PSIRT могут участвовать в преодолении этого разрыва (это выходит за рамки данного документа).

В каждом разделе мы выделим различные группы заинтересованных сторон и дадим краткую информацию о некоторых приоритетных областях, которые могут способствовать участию PSIRT в содержательных дискуссиях, касающихся обучения и профессиональной подготовки их заинтересованных сторон. Для подготовки заинтересованных сторон PSIRT могут использовать учебные материалы, созданные собственными силами, сторонние материалы или сторонние ресурсы.

Услуга 6.1 Профессиональная подготовка сотрудников PSIRT

Сотрудники PSIRT должны в первую очередь быть в курсе происходящего в сфере безопасности, включая, в частности, тенденции, новые эксплойты и отраслевые мероприятия. Для этого широкого круга знаний требуется прочная основа в виде

осведомленности об общих аспектах безопасности, что видно на примере ведущих сертификационных программ по вопросам безопасности. Однако сертификационные программы обеспечивают только основы, которые необходимо постоянно обновлять посредством таких мероприятий, как конференции по вопросам безопасности, участие в работе отраслевых консорциумов и глубокое понимание ситуации в отрасли в целом за счет активного изучения блогов, отраслевой прессы, публикаций консорциумов и т. д. Членам PSIRT также необходимо быть в курсе постоянно изменяющегося законодательства в области безопасности и конфиденциальности.

Функция 6.1.1 Техническая подготовка

Важно, чтобы сотрудники PSIRT обладали глубоким пониманием основных принципов безопасности и знаниями о поддерживаемых продуктах. Учебные материалы необходимо регулярно пересматривать, чтобы обеспечить включение в них новых методов использования уязвимостей, возникающих по мере изменения ситуации в сфере безопасности.

***Цель**: обеспечить подготовку сотрудников PSIRT таким образом, чтобы они понимали суть проблемы, о которой сообщается, и могли надлежащим образом определить ее приоритетность, прежде чем передать ее группам, отвечающим за разработку, проверку и выпуск неисправностей.*

***Результат**: сотрудники PSIRT обладают достаточным уровнем технической подготовки для выполнения своих обязанностей.*

Подготовка в области принципов обеспечения безопасности варьируется в зависимости от типа продуктов, поддерживаемых поставщиком (например, аппаратное обеспечение, микропрограммное обеспечение, программное обеспечение, организация сетей, облачные продукты или все вышеперечисленное). Подготовка самого общего уровня должна охватывать основные аспекты безопасности, в том числе такие, как распространенные виды атак, криптографию, конфиденциальность, целостность, доступность, аутентификацию, авторизацию, модели управления доступом, режим с множеством арендаторов, соблюдение соответствующих стандартов и нормативное регулирование. Необходимо, чтобы программа подготовки также включала любое отраслевое регулирование, которое может влиять на деятельность PSIRT, например HIPAA для сферы здравоохранения и PCI DSS для поставщиков платежных карт и банковской деятельности. Также персонал PSIRT должен на определенном уровне изучить продукты, чтобы понимать суть проблем, о которых им сообщают.

Функция 6.1.2 Подготовка в области коммуникации

Поскольку PSIRT получает сообщения от сторонних лиц, обнаруживающих уязвимости, важно, чтобы сотрудники PSIRT прошли подготовку в области политики связи и коммуникативных навыков, которая охватывает вопросы обеспечения своевременного взаимодействия со сторонними лицами, обнаруживающими уязвимости, и внутренними заинтересованными сторонами.

***Цель**: обеспечение соблюдения персоналом PSIRT политики организации в области связи при взаимодействии с внешними субъектами, что позволяет устранить любые проблемы нормативного/правового характера, которые могут возникать вследствие некорректного общения.*

***Результат:** сотрудники PSIRT обладают навыками в области коммуникации, достаточными для четкого выполнения своих должностных обязанностей и исключающими неоднозначность при общении.*

Функция 6.1.3 Подготовка в области технологии работы

Необходимы руководящие указания, определяющие порядок отслеживания, урегулирования и оценки проблем, о которых поступают сообщения. Следует определить роли различных заинтересованных сторон, вовлеченных в процесс разрешения таких проблем. Необходимо, чтобы этот процесс включал своевременное реагирование на сообщения лиц, обнаруживающих уязвимости, и периодическое информирование их по всем нерешенным вопросам. Также необходимы четко определенные и безопасные средства обмена информацией между сторонним лицом, обнаружившим уязвимость, и поставщиком.

***Цель**: обеспечение бесперебойной передачи информации в процессе управления инцидентом в области безопасности продукции, позволяющее добиться своевременного решения проблем.*

***Результат**: сотрудники PSIRT пройдут обучение внутренним процессам в объеме, достаточном для выполнения своих обязанностей.*

Функция 6.1.4 Подготовка в области использования инструментария

Подфункция 6.1.4.1 Средства отслеживания дефектов и другие инструменты управления для сотрудников PSIRT и инженерного состава

В конкретной организации необходимо определить официально признанное средство отслеживания дефектов для каждого продукта (предпочтительно одно и то же для всех продуктов). Этот механизм должен выявлять все дефекты, а дефекты в системе безопасности должны единообразно идентифицироваться

как таковые. Возможность просмотра и доступа к информации, связанной с уязвимостями защиты в продукте, следует предоставлять только тем, кому эта информация необходима. Кроме того, в этом инструменте следует предусмотреть техническую возможность поддержки требований к программным показателям с возможностью составления отчетов как в ручном, так и в автоматическом режиме.

***Цель**: обеспечить эффективное отслеживание проблем и защиту информации об уязвимостях посредством сертифицированных механизмов отслеживания, предоставляющих возможность получения доступа, отслеживания и урегулирования этих проблем только в силу очевидной служебной необходимости.*

***Результат**: сотрудники PSIRT будут обладать уровнем подготовки и знаниями об инструментарии, достаточными для выполнения своих обязанностей.*

Подфункция 6.1.4.2 Средства отслеживания сторонних компонентов

Большинство продуктов включают несколько компонентов сторонних производителей (в том числе с открытым исходным кодом), которые поставляются вместе с ними. Клиенты часто не знают о стороннем программном обеспечении, поставляемом вместе с продуктом, и, следовательно, будут рассчитывать на то, что поставщик примет меры для выявления неисправности или предоставит информацию об устранении уязвимости. Важно определить внутренние средства отслеживания сторонних компонентов, чтобы учесть зависимость продуктов поставщика от различных компонентов, поставляемых третьими лицами. Необходимо вести мониторинг национальной базы данных об уязвимостях (NVD), бюллетенях безопасности сторонних поставщиков и других внешних структур в целях отслеживания уязвимостей и методов их устранения в сторонних компонентах, чтобы эти методы можно было предоставить клиенту.

***Цель**: определить средства отслеживания сторонних компонентов, встроенных в продукты, в целях выявления и устранения уязвимостей в этих компонентах.*

***Результат**: сотрудники PSIRT будут иметь представление о сторонних компонентах в поставляемых продуктах и смогут отслеживать их.*

Функция 6.1.5 Отслеживание всех учебных инициатив

PSIRT необходимо отслеживать все варианты подготовки, доступные для различных заинтересованных сторон. Группе будет необходимо обеспечить

проведение этих учебных мероприятий с определенной периодичностью, поскольку ситуация в области безопасности меняется очень быстро и, следовательно, учебные мероприятия и процессы необходимо постоянно пересматривать.

***Цель**: обеспечить отслеживание всех учебных мероприятий для различных заинтересованных сторон.*

***Результат**: сотрудники PSIRT будут знать, что различные заинтересованные стороны прошли подготовку в отношении их роли в деятельности PSIRT.*

Услуга 6.2 Профессиональная подготовка группы разработчиков

Безопасная разработка относится к методам работы и шагам, предпринимаемым на протяжении всего процесса разработки, которые специально предназначены для снижения количества и степени серьезности уязвимостей в продуктах и услугах, связанных с программным обеспечением. При наличии эффективной программы подготовки и акценте на методологии безопасной разработки можно намного уменьшить факторы уязвимости еще до выпуска продукта, что является гораздо менее затратным, чем устранение уязвимостей после выхода продукта на рынок.

Безопасная разработка начинается с требований, предъявляемых к продукту, и его архитектуры. Кроме того, анализ проекта с точки зрения безопасности является ключом к выявлению возможных уязвимостей еще до начала разработки продукта.

Существует множество мероприятий, связанных с программой обеспечения безопасности на этапах разработки, подробности которых выходят далеко за пределы охвата этого документа. Настоятельно рекомендуется создать отдельную программу для управления соответствующими усилиями в рамках цикла обеспечения безопасности на этапах разработки. Эта программа должна соответствовать принятой в отрасли модели типовой программы. Примером цикла обеспечения безопасности на этапах разработки является методика разработки безопасных программ компании Microsoft[14].

***Цель**: способствовать наличию в организации соответствующей программы обеспечения безопасности на этапах разработки (SDL), в рамках которой сотрудники, занимающиеся разработкой, проходят обучение созданию безопасного кода и использованию официальных руководящих указаний в области безопасности в ходе разработки архитектуры и дизайна продукта.*

***Результат**: группы разработчиков смогут создать безопасный код и выпускать более безопасные продукты.*

[14] https://www.microsoft.com/en-us/sdl/

Подготовка в области безопасной разработки не всегда рассматривается как зона ответственности PSIRT и может осуществляться за рамками деятельности PSIRT. В любом случае это важный этап, который должен учитывать любой поставщик, который заботится о безопасности своих продуктов.

Функция 6.2.1 Подготовка в области процессов, связанных с деятельностью PSIRT

Все участники процесса разработки должны понимать, почему существует процесс PSIRT, как он функционирует и что они должны делать в ходе разработки продуктов для поддержки этого процесса. Часто после выпуска продукта группы разработчиков переходят к другим проектам, снижая до минимума усилия по поддержке продукта. Подготовка этих подразделений и обеспечение их соответствующими методами хранения ключевой информации о продукте имеет решающее значение для PSIRT с точки зрения полноценного решения проблемы уязвимости продукта. Необходимо документировать информацию, касающуюся, в частности, лиц, занимавшихся архитектурой безопасности, возглавлявших группу разработчиков и группу тестирования, чтобы PSIRT могла обратиться к наиболее осведомленным лицам для оценки рисков и разработки мер по их смягчению. Эта документация должна также охватывать такие вопросы, как использованные сторонние компоненты, особенности процесса обновления продукта, существующая регистрация данных, допустимые исключения безопасности и процесс уведомления заинтересованных сторон. Эта информация является крайне важной для PSIRT с точки зрения устранения уязвимости защиты. Также особое значение имеет проведение переподготовки, поскольку состав групп разработчиков меняется.

***Цель**: обеспечить понимание всеми заинтересованными сторонами особенностей процессов, связанных с деятельностью PSIRT, и связи этих процессов с их ролью в разработке продукта.*

***Результат**: формирование среди разработчиков культуры безопасности и улучшение взаимодействия в рамках борьбы с уязвимостями.*

Услуга 6.3 Профессиональная подготовка валидационной группы

Сотрудники этого подразделения должны постоянно быть в курсе новейших инструментов и методов для осуществления таких проверок, как тестирование на проникновение, сканирование на уязвимости, фаззинг, этичный взлом и другие. Их обучение по этим вопросам относится к сфере SDL и выходит за рамки охвата этого документа. Однако PSIRT следует поощрять организации создавать группы, сосредоточенные на выполнении этих задач.

Цель: *поощрение наличия в организации соответствующей программы SDL, в рамках которой определены надлежащие инструменты проверки безопасности.*

Результат: *повышение качества и безопасности продуктов.*

Так же как и безопасная разработка, подготовка в области проверки безопасности не относится к зоне ответственности PSIRT и осуществляется вне процесса PSIRT. Тем не менее это столь же важный этап, который поставщику надлежит осуществить в рамках SDL продукта.

Функция 6.3.1 Подготовка в области процессов, связанных с деятельностью PSIRT

Ряд членов валидационной группы могут принимать участие в тестировании исправлений, которые необходимы для устранения уязвимостей продукта. Эти члены группы должны иметь представление о процессе PSIRT, его особенностях, предполагаемых временны́х рамках и своей роли в этом процессе. Им также потребуется четкое представление о жизненном цикле продукта и знания о его поддерживаемых версиях, которые необходимо проверить на наличие устраненных уязвимостей. Кроме того, им потребуется провести тестирование обходных решений, если таковые имеются. Еще одной важной задачей будет регрессионное тестирование.

Цель*: обеспечить понимание всеми заинтересованными сторонами особенностей процессов, связанных с деятельностью PSIRT, и связи этих процессов с их ролью в проведении проверки продукта.*

Результат*: формирование среди членов валидационной группы культуры безопасности и улучшение взаимодействия в рамках борьбы с уязвимостями.*

Услуга 6.4 Непрерывное обучение всех заинтересованных сторон

Всем заинтересованным сторонам потребуется определенный уровень подготовки и осведомленности о программе PSIRT. Многие заинтересованные стороны вовлечены в сквозные процессы с участием PSIRT. Таким образом, важно выявить различные группы заинтересованных сторон и разработать программы обучения, соответствующие их потребностям.

Цель*: обеспечить для всех групп заинтересованных сторон прохождение подготовки или получение базовых знаний, которые необходимы им для выполнения своих функций в рамках программы PSIRT.*

Результат*: хорошо информированные внутренние заинтересованные группы, имеющие представление о том, как они будут работать с PSIRT в рамках решения возникающих проблем уязвимости и какие услуги PSIRT будет предлагать в таких ситуациях.*

Функция 6.4.1 Обучение высшего руководства

Эта группа, как правило, принимает участие в первоначальном утверждении политики компании в области связи, защиты от уязвимостей и других стратегий. Разработка бюллетеней безопасности также может потребовать утверждения со стороны руководства. Помимо этого, санкция высшего руководства нередко требуется для действий в критических ситуациях, которые создают высокий уровень риска, привлекают повышенное внимание или требуют повышенной ответственности. Также руководство может требовать проведения периодических проверок средств обеспечения безопасности всех продуктов. В связи с этим важно информировать руководство о процессах PSIRT.

***Цель**: ознакомить управленческий состав с их ролью в программе PSIRT.*

***Результат**: своевременная подготовка и принятие решений по действиям, требующим санкции руководства.*

Функция 6.4.2 Обучение подразделения по правовым вопросам

Подразделение по правовым вопросам принимает участие в первоначальной разработке политики компании. Некоторые проблемы, о которых сообщают лица, обнаружившие уязвимость, могут включать вопросы о зоне ответственности и потому требовать помощи со стороны подразделений по правовым вопросам, в связи с чем важно заранее определить контактных лиц.

***Цель**: ознакомить сотрудников подразделения по правовым вопросам с их ролью в рамках программы PSIRT и информировать их о соответствующих сроках.*

***Результат**: своевременное решение проблем безопасности, требующих одобрения со стороны юристов.*

Функция 6.4.3 Обучение подразделения по взаимодействию с государственными структурами и контролю за соблюдением законодательства

Подразделение по взаимодействию с государственными структурами участвует в обеспечении соблюдения нормативно-правовых требований. Таким образом важно заранее определить контактных лиц.

***Цель**: ознакомить сотрудников подразделения по взаимодействию с государственными структурами с их ролью в рамках программы PSIRT.*

***Результат**: своевременное устранение уязвимостей системы безопасности, требующих соблюдения определенных нормативных стандартов.*

Функция 6.4.4 Обучение группы по маркетингу

Специалистов по маркетингу часто привлекают в случае возникновения угрозы для бренда. Кроме того, сотрудники этого подразделения могут проводить обзор бюллетеней безопасности, а также публиковать соответствующую маркетинговую информацию. Группы по маркетингу также занимаются продвижением аспектов безопасности продуктов.

***Цель**: ознакомить группы по маркетингу с их ролью в рамках программы PSIRT и разъяснить, какие утверждения относительно безопасности продукта допустимы, а какие нет.*

***Результат**: надлежащая координация действий между PSIRT и группами по маркетингу позволит обеспечить единообразие публичной позиции по вопросам безопасности в маркетинговых материалах и бюллетеней безопасности.*

Функция 6.4.5 Обучение подразделения по связям с общественностью

Подразделения по связям с общественностью (PR) могут отвечать за реагирование на внешние посты или блоги, посвященные безопасности, или отвечать на запросы прессы, связанные с критическими уязвимостями продукта. Необходимо определить контактных лиц, чтобы привлечь подразделение по связям с общественностью, если потребуются какие-либо публикации на внешних информационных ресурсах.

***Цель**: ознакомить сотрудников подразделений по связям с общественностью с их ролью в рамках программы PSIRT.*

***Результат**: надлежащая координация действий между PSIRT и подразделениями по связям с общественностью позволит определить надлежащую публичную позицию поставщика по вопросам безопасности.*

Функция 6.4.6 Обучение группы по продажам

Сотрудникам группы по продажам может понадобиться подготовка по основам обеспечения безопасности и по вопросам коммуникации, связанной с методами обеспечения безопасности. Лицам, занимающимся продажами, также важно знать, какие сведения могут быть разглашены за пределами компании, а какие нет. Сотрудникам отдела продаж рекомендуется перенаправлять любые проблемные вопросы, связанные с безопасностью, которые поступили от заинтересованных сторон/потенциальных клиентов, либо сотрудникам PSIRT, либо сотрудникам службы поддержки, а не заниматься их решением самостоятельно.

***Цель:** информировать сотрудников группы по продажам о том, какие утверждения относительно безопасности продукта допустимы, а какие нет и куда обращаться с вопросами, на которые они не могут дать ответ.*

***Результат**: надлежащая координация действий между PSIRT и подразделениями по продажам приведет к удовлетворению ожиданий клиентов.*

Функция 6.4.7 Обучение службы поддержки

Сотрудники службы поддержки должны пройти обучение, посвященное работе с сообщениями об уязвимостях системы безопасности, полученными от клиентов. В ряде случаев к решению этих вопросов может быть привлечена PSIRT. В обязанности службы поддержки входит публикация регламентирующих документов, определяющих срок службы каждого продукта, поддерживаемые версии и возможности выпуска бюллетеней безопасности. Большинство поставщиков предоставляют бюллетени безопасности только в отношении поддерживаемых версий. Следовательно, эти регламентирующие документы являются существенными и должны быть опубликованы на веб-сайте поставщика, чтобы заинтересованные стороны могли легко найти их. Как правило, PSIRT поддерживает тесную связь со службой поддержки, поэтому ее сотрудники понимают, о каких проблемах сообщают клиенты. Иногда лицо, обнаружившее уязвимость, также является клиентом, в связи с чем вопрос может передаваться для решения от службы поддержки к PSIRT и наоборот.

***Цель**: ознакомить сотрудников службы поддержки с их ролью в рамках процесса PSIRT.*

***Результат**: надлежащая координация действий между PSIRT и службой поддержки приведет к удовлетворению ожиданий клиентов и лиц, направляющих сообщения.*

Услуга 6.5 Обеспечение механизмов обратной связи

Используйте информацию, полученную в ходе анализа первопричины инцидента, для обучения вовлеченных лиц и предотвращения появления аналогичных уязвимостей в будущем.

***Цель**: постоянно совершенствовать процесс обучения, чтобы не отставать от стремительно изменяющейся ситуации в сфере безопасности.*

***Результат**: обеспечение более высокого качества обучения приведет к повышению качества услуг, предоставляемых всем заинтересованным сторонам.*

ПРИЛОЖЕНИЕ 1. Вспомогательные материалы

Architecture Content Framework[15]

ISO 31000:2009, Risk management – Principles and guidelines[16]

ISO/IEC 27000/2018, Information technology – Security techniques – Information security management systems

ISO/IEC 30111:2013, Information technology – Security techniques – Vulnerability handling processes[17]

ISO/IEC 29147:2014, Information technology – Security techniques – Vulnerability disclosure[18]

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure[19]

The Project Management Body of Knowledge (PMBBOK) Guide and Standards

[15] http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap35.html

[16] https://www.iso.org/iso-31000-risk-management.html

[17] https://www.iso.org/obp/ui/#iso:std:53231:en

[18] https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-1:v1:en

[19] https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRSTMultiparty-Vulnerability-Coordination-v1.0.pdf

ПРИЛОЖЕНИЕ 2. Выражение признательности

- Барбара Косгриф, MetLife
- Беверли Финч, Lenovo
- Карл Денис, Siemens
- Крис Робинсон, Red Hat
- Джефф Хан, Honeywell
- Джерри Брайант, Intel
- Джош Демблинг, Intel
- Жан-Робер Унтоме, Broadcom
- Кевин Райан, NetApp
- Лэнгли Рок, Red Hat
- Лайза Брэдли, Dell Technologies
- Питер Эллор, Red Hat
- Решма Банерджи, Oracle
- Руперт Уиммер, Siemens
- Шон Ричардсон, NVIDIA
- Стив Брукбахер, Johnson Controls
- Таня Уорд, Dell Technologies
- Вик Чунг, SAP

ПРИЛОЖЕНИЕ 3. Таблицы и рисунки

ПРИЛОЖЕНИЕ 4. Преимущества и недостатки организационных моделей PSIRT

Модель	Описание	Преимущества	Недостатки
Распределенная	Небольшая основная операционная группа PSIRT распределяет обязанности среди представителей PSIRT в различных функциональных областях (например, в области поддержки, проектирования, управления продуктами)	❖ Идеально подходит для крупных компаний с обширным и разнообразным ассортиментом продукции. ❖ Распределение затрат, связанных с выполнением функций PSIRT. ❖ Распределение рабочей нагрузки между сотрудниками, выполняющими различные функции. ❖ Возможность масштабирования в случае роста ассортимента продукции	❖ Организация PSIRT обладает определенными полномочиями по определению политики и направлению деятельности. ❖ Нередко PSIRT не может непосредственно контролировать ресурсы, необходимые для устранения уязвимостей, что снижает возможности контроля. ❖ Подразделения, разрабатывающие различные продукты, могут отдавать предпочтение своим интересам в ущерб деятельности PSIRT
Централизованная	Более крупная организация PSIRT, непосредственно участвующая во всех видах деятельности PSIRT (например, управление продуктами, приоритизация, выявление и устранение уязвимостей и распространение информации) для различных продуктов	❖ Идеально подходит для небольших организаций с небольшим ассортиментом продуктов. ❖ Централизованная группа, состоящая из специалистов с высокой квалификацией в сфере безопасности. ❖ Организация PSIRT принимает все решения в отношении бюджета, политики и ресурсов PSIRT. ❖ Обеспечение более эффективного контроля и подотчетности оперативной деятельности PSIRT	❖ Слабые возможности для масштабирования в случае расширения ассортимента продукции. ❖ Принятие значимых решений возможно только в сотрудничестве с другим функциональным менеджером или при его одобрении. ❖ Содержание централизованной специализированной группы обходится дорого
Гибридная	Представляет собой сочетание свойств как распределенной, так и централизированной моделей		

ПРИЛОЖЕНИЕ 5. Виды групп реагирования на инциденты

– **Национальная CSIRT (группа реагирования на инциденты в сфере компьютерной безопасности)** – под национальной CSIRT подразумевается организация, учрежденная органом государственной власти для координации реагирования на инциденты в сфере кибербезопасности на национальном уровне. В число ее клиентов, как правило, входят все государственные департаменты и ведомства, правоохранительные органы и институты гражданского общества. Кроме того, такая CSIRT, как правило, является тем органом, который отвечает за взаимодействие с национальными CSIRT других стран, а также с региональными и международными игроками.

– **CSIRT по важнейшей инфраструктуре/отраслевая CSIRT** отвечает за мониторинг, управление и реагирование на инциденты в сфере кибербезопасности в конкретной отрасли (например, энергетике, электросвязи, финансах).

– **Ведомственная (на уровне организации) CSIRT** – под ведомственной CSIRT, как правило, подразумевается группа, отвечающая за мониторинг, управление и обработку инцидентов в сфере кибербезопасности, оказывающих воздействие на внутренние услуги и инфраструктуру ИКТ конкретной организации.

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

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

Глоссарий

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

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

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

– **Общеизвестные уязвимости и незащищенность (CVE**) – перечень общеизвестных уязвимостей с указанием идентификационного номера, описанием и по меньшей мере одной ссылкой на публичный источник.

– **Система оценки общеизвестных уязвимостей**[20] **(CVSS)** – количественная оценка, отражающая степень серьезности уязвимости.

– **Перечень общеизвестных слабых мест**[21] **(CWE)** – официальный перечень категорий слабых мест в программном обеспечении, разработанный для того, чтобы:

- служить общим языком для описания слабых мест в архитектуре, проектировании или кодах программного обеспечения;
- выступать в качестве стандартного количественного показателя для инструментальных средств по защите программного обеспечения, работающих с такими слабыми местами;
- предоставлять общий базовый стандарт при выявлении слабых мест, смягчении их воздействия и предупреждении их возникновения.

– **Закон о переносимости и подотчетности медицинского страхования**[22] **(HIPPA)** – закон США, разработанный для обеспечения стандартов конфиденциальности в целях защиты медицинских карт пациентов и другой медицинской информации, предоставляемой программам медицинского страхования, врачам, больницам и иным поставщикам медицинских услуг.

[20] https://www.first.org/cvss/
[21] https://cwe.mitre.org/about/index.html
[22] https://www.medicinenet.com/script/main/art.asp?articlekey=31785

– **Ключевой показатель деятельности**[23] – 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, который демонстрирует, 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, либо в результате совокупности осуществления функций и предоставления услуг.

– **Стандарт безопасности данных индустрии платежных карт**[24] **(PCI DSS) –** стандарт информационной безопасности, который способствует обеспечению безопасности данных держателей банковских карт во всем мире.– **Задачи** – перечень действий, которые необходимо предпринять для выполнения той или иной задачи.

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

[23] https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator
[24] https://www.pcisecuritystandards.org/pci_security/