TLP:WHITE

Проект Кодекса этики и профессионального поведения Форума групп реагирования на инциденты и обеспечения безопасности (FIRST)

Члены групп реагирования на инциденты и обеспечения безопасности (Группы) имеют доступ ко множеству цифровых систем и источников информации. Их деятельность может изменить мир. Как представитель этой профессиональной области, член Группы должен осознавать свою ответственность перед клиентурой и другими специалистами в области обеспечения безопасности, а также перед обществом в целом. Частные лица также должны осознавать свою ответственность за обеспечение собственного благополучия.

Задача настоящего Кодекса заключается в том, чтобы стимулировать и направлять этичное поведение всех членов Группы, включая действующих и потенциальных специалистов-практиков, инструкторов, студентов, влиятельных лиц и любых лиц, эффективно использующих компьютерные технологии. В Кодексе содержатся принципы, сформулированные как заявления об ответственности и основанные на представлении о приоритетной роли общественного блага во всех случаях. Каждый принцип дополняется руководящими указаниями, в которых содержатся предназначенные для специалистов в области вычислительной техники разъяснения, обеспечивающие понимание и применение этого принципа.

Обязанности членов Группы перечислены ниже (не в порядке приоритетности). Эти обязанности следует воспринимать не как абсолютные предписания, но как рекомендации, соответствующие по своей значимости определению "СЛЕДУЕТ" в документе IETF RFC2119:

> "могут существовать веские условия при определенных обстоятельствах, в которых данное условие можно игнорировать, но перед тем как выбрать другой вариант, необходимо полностью осознать последствия и тщательно взвесить ситуацию".

Подробную информацию о способах решений возможных дилемм см. в Дополнении А.

Обязанность поддерживать доверие

Доверие лежит в основе множества взаимоотношений между Группами и зачастую является обязательным условием содержательного обмена информацией. Сообщество FIRST зиждется на этом доверии и может продолжать свою деятельность только при наличии достаточного уровня доверия между Группами.
В соответствии с обязанностью поддерживать доверие членам Групп следует: 1) принимать на себя только выполнимые обязательства; 2) вести себя предсказуемым образом по отношении к другим Группам (например, соблюдать стандарт TLP); и 3) поддерживать существующие отношения с другими Группами на основе взаимного доверия.
Следует изначально предполагать создание переходных отношений на основе взаимного доверия, то есть опирающихся на принцип доверия при первом использовании (TOFU) и обеспечивающих доверие к Группам, которым доверяют другие Группы.

Обязанность осуществлять скоординированное раскрытие информации об уязвимостях

Членам Группы, получившим информацию об уязвимости, следует осуществлять скоординированное раскрытие информации об уязвимости, вступив в сотрудничество с заинтересованными сторонами для устранения уязвимостей системы безопасности и минимизации ущерба, связанного с раскрытием информации. К заинтересованным сторонам относятся, в частности, лицо, сообщившее об уязвимости, затронутый поставщик (поставщики), координаторы, защищающие стороны, а также нижестоящие потребители, партнеры и пользователи.

Членам Группы следует координировать свои действия с соответствующими заинтересованными сторонами для согласования четких графиков и порядка раскрытия информации, сообщая пользователям подробности в объеме, достаточном для того, чтобы они могли оценить риски и принять действенные меры защиты.

Обязанность соблюдать конфиденциальность

Члены Группы обязаны в соответствующих случаях соблюдать конфиденциальность. Членам Группы может быть направлен прямой запрос на сохранение конфиденциальности определенной информации, например посредством применения протокола маркировки информации (TLP). Членам Группы следует, по мере возможности, выполнять эти запросы. При невозможности сохранения конфиденциальности информации, например если это противоречит требованиям местных законов, условиям договоров или обязанности предоставлять информацию, члену Группы следует немедленно сообщить владельцу информации об этом противоречии.
Некоторые обязанности по сохранению конфиденциальности основываются на законах, нормах или обычаях. Если в процессе реагирования на инцидент некоторые стороны вынуждены соблюдать эти требования или рассчитывают на сохранение конфиденциальности на основании данных соображений, им следует приложить все

усилия для того, чтобы заранее открыто заявить о своих ожиданиях. В таком случае всем сторонам следует принять во внимание данные ожидания и выполнить прямой запрос на сохранение конфиденциальности информации там, где это возможно.

Обязанность подтверждать получение информации

Группы получают информацию из множества различных источников – от исследователей, клиентов, других Групп, государственных учреждений и т. д. Членам Группы следует своевременно отвечать на запросы, даже если этот ответ содержит только подтверждение получения запроса. По возможности членам Группы следует наметить ожидаемые сроки получения следующих обновлений.

Обязанность получать разрешение

Члены Группы имеют законные необходимость и право изучать области своей ответственности, действуя только в системах, куда им разрешен доступ. Члены Группы должны быть осведомлены о том, как их действия могут затронуть их клиентов, и принимать меры к тому, чтобы не причинить дополнительного ущерба в процессе выполнения своих обязанностей. Следует разъяснять затронутым заинтересованным сторонам суть возможных последствий этих действий. При наличии возможности следует проводить консультации с клиентами, прежде чем вносить изменения в их системы.

Обязанность предоставлять информацию

Членам Группы следует считать своей обязанностью предоставление клиентам информации о существующих угрозах безопасности и рисках. Если члены Группы располагают информацией, способной либо оказать негативное воздействие на безопасность и защиту, либо повысить их эффективность, они обязаны принять надлежащие меры по предоставлению этой информации соответствующим сторонам или другим сторонам, способным оказать помощь, должным образом соблюдая при этом обязательства по сохранению конфиденциальности информации, законы и нормативные акты о неприкосновенности частной жизни или иные обязательства.

Обязанность соблюдать права человека

Членам Группы следует иметь в виду, что их действия могут затрагивать права человека иных лиц в результате распространения информации, возможного проявления предвзятости в их действиях или посягательств на имущественные права. В процессе урегулирования инцидентов члены Группы получают доступ к широкому спектру личной, закрытой и конфиденциальной информации. Эту информацию следует обрабатывать так, чтобы обеспечить соблюдение прав человека.

В процессе урегулирования инцидента лицам, принимающим меры реагирования, не следует действовать предвзято. Они должны прилагать все усилия для того, чтобы устранить предвзятость из процедур и процессов принятия решений как

осуществляемых лицами, принимающими меры реагирования, так и встроенных в алгоритмы.

Для целей применения настоящего принципа в понятие "имущество" (Декларация прав человека ООН, статья 17) включены также нематериальные виды собственности, например объекты интеллектуальной собственности, а также идеи и концепции в целом, вне зависимости от того, находятся ли они под защитой закона (например, являются запатентованными).

Обязанность заботиться о здоровье членов Группы

Группы должны быть в состоянии на постоянной основе предоставлять своим клиентам услуги, которые они обещали предоставить. Эта обязанность включает в себя заботу о физическом и эмоциональном здоровье членов Группы.

В целях соблюдения прав лиц, являющихся членами Группы, а также в целях обеспечения долгосрочной жизнеспособности Группы и надлежащего уровня обслуживания Группе следует стремиться к созданию здоровой, безопасной и позитивной рабочей среды, способствующей сохранению физического и эмоционального здоровья (всех) членов Группы. В целях эффективного реагирования на кризис следует принимать меры по защите эмоционального здоровья и смягчению стрессов в рамках обычной деятельности Группы.

Обязанность укреплять потенциал Группы

Управление инцидентами является постоянно развивающейся областью исследований, и членам Группы следует непрерывно изучать ее. Группе следует предоставлять своим членам необходимые ресурсы для изучения, применения и совершенствования научно-технических знаний в сфере (сферах) их деятельности. В данном случае полезными могут быть учебные занятия или программы дополнительного профессионального образования/повышения квалификации, однако для надлежащего выполнения этой обязанности недостаточно только осуществлять соответствующие мероприятия. Группе следует обеспечивать функционирование технической инфраструктуры, достаточной для оказания услуг Группы, в том числе посредством принятия надлежащих мер для защиты этой инфраструктуры от вмешательства внешних сторон.

Обязанность осуществлять ответственный сбор данных

Сбор данных является необходимым условием реагирования на инциденты, однако следует поддерживать баланс между достижением целей реагирования на инциденты и соблюдением прав заинтересованных сторон, работающих с данными.

Объем подлежащей сбору информации может меняться в процессе расследования. По мере рассмотрения инцидента членам Группы следует приводить объем собираемой информации в соответствие с меняющимися требованиями. Следует

исключать из отчетности данные, не имеющие прямого отношения к инциденту и его урегулированию.

Собранные и извлеченные данные следует обрабатывать в соответствии с действующими законами и при условии соблюдения неприкосновенности частной жизни пользователя (пользователей). Следует получить разрешение владельца данных перед тем, как проводить сбор и обработку данных, находящихся под его контролем. Следует соблюдать действующие нормативно-правовые акты, касающиеся обработки данных.

Следует предоставлять другим группам реагирования, занимающимся рассмотрением других инцидентов, доступ к данным, которые могут быть для них полезны, возможно, в отредактированном виде. Доступ к конфиденциальной и частной информации следует предоставлять только при обеспечении надлежащей защиты.

Следует оценить риски и выгоды, прежде чем делиться данными с третьими сторонами в целях уменьшения объема ущерба. Делиться данными следует только в том случае, если выгоды заметно перевешивают риски. Конфиденциальные данные следует хранить таким образом, чтобы их можно было легко уничтожить после завершения рассмотрения инцидента. Следует осуществлять безопасное уничтожение собранных данных в соответствии с политикой сохранения данных.

Обязанность признавать границы юрисдикций

Членам Группы следует признавать и уважать границы юрисдикций, законные права, правовые нормы и органы власти сторон, принимающих участие в действиях, связанных с реагированием на инциденты.

В участвующих в рассмотрении инцидента юрисдикциях могут существовать различные законы, нормы и другие правовые аспекты, в том числе связанные с защитой неприкосновенности частной жизни или направлением уведомлений об утечке данных. Для определения границ юрисдикций могут использоваться как фактическое местоположение вовлеченных сторон (например, страна или место юридической регистрации), так и другие факторы, имеющие отношение к этим сторонам. Законы и нормы могут различаться даже в разных административных регионах одной страны (например, в отдельных штатах США), а также в разных субъектах предпринимательской деятельности, отраслях или секторах этого государства (например, в сфере здравоохранения, в сфере финансовых услуг или в государственных учреждениях). Национальные CSIRT могут иметь определенные сферы ответственности и/или полномочий для осуществления деятельности с участием клиентов в рамках своих юрисдикций. Кроме того, они могут сотрудничать с другими учреждениями, обладающими необходимыми полномочиями для деятельности в других юрисдикциях, или передавать им информацию и право предпринимать определенные действия.

Членам Группы следует иметь представление о ключевых факторах, влияющих на

вовлеченные юрисдикции, включая, в частности, нормы обеспечения неприкосновенности частной жизни или требования к направлению уведомлений об утечке данных. Ввиду того что во всем мире идет непрерывное развитие и обновление законов и норм, касающихся кибербезопасности и защиты неприкосновенности частной жизни, рекомендуется проводить консультации с осведомленным юристом, чтобы определить, относится ли тот или иной вопрос к нескольким юрисдикциям.

Обязанность строить логические рассуждения на основе фактических данных

Группам следует основывать свою оперативную деятельность на поддающихся проверке фактах. При совместном использовании информации, например индикаторов компрометации (IOC) или описаний инцидента, члены Группы должны представлять прозрачные доказательства и данные о масштабах инцидента. При отсутствии такой возможности следует представить имеющуюся информацию и сообщить о причинах, препятствующих совместному использованию доказательств и данных о масштабах инцидента.

Членам Группы следует воздержаться от распространения слухов или обмена слухами. Любые предположения следует четко называть таковыми.

Прозрачные процессы сбора доказательств и построения логических рассуждений имеют большое значение даже при автоматическом совместном использовании данных, то есть при автоматическом совместном использовании больших массивов информации. В таком случае следует распространить подробное описание глубинного анализа данных.

Дополнение A

Разрешение дилемм

Члены Группы нередко могут оказываться в ситуациях, когда предпринимаемые ими действия не соответствуют всем этическим принципам. В подобной ситуации необходимо выбрать наиболее важные принципы. В этой ситуации лицам, занимающимся рассмотрением инцидента, следует определить, желательно в ходе обсуждения с коллегами, какие заинтересованные стороны могут оказаться затронуты их действиями и каким образом они будут затронуты. Как правило, следует выбирать решение, предусматривающее минимальное нарушение настоящего Кодекса. Иногда это может быть неосуществимо, например, из-за внешнего давления. В таком случае рекомендуется продолжать принимать необходимые меры, даже под возможным давлением, отметив при этом существование этической дилеммы.