УДК 004.056

Имамвердиев Я.Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az

СОЗДАНИЕ CERT-КОМАНДЫ ДЛЯ НАУЧНОЙ КОМПЬЮТЕРНОЙ СЕТИ AZSCIENCENET

Реагирование на инциденты является важным аспектом управления информационной безопасностью. В этой работе описывается методология создания команды AZ-CERT для научной компьютерной сети AzScienceNet. Дается обзор нормативных и научно-методических документов в области управления инцидентами, обосновывается выбор организационной структуры и набора услуг для команды AZ-CERT, предлагается модель поэтапного создания CERT-команды. Приводится также описание общего процесса реагирования на инциденты в сети AzScienceNet и технической инфраструктуры AZ-CERT.

Ключевые слова: *информационная безопасность, инцидент информационной безопасности, реагирование на инциденты, команда оперативного реагирования на инциденты.*

Введение

На современном этапе развития человечества информация и информационные технологии превращаются в решающий фактор экономики, науки, образования и других областей политической и общественной деятельности. Различные информационные и коммуникационные системы выступают как важный аспект развития общества и государства. Наряду с этим расширяются также возможности преступных групп по использованию информационных и коммуникационных технологий в преступных целях. С быстрым развитием Интернета и технологий мобильных коммуникаций угрозы для информационных и коммуникационных систем становятся все более вероятными, а результаты их реализации все более масштабными.

Поэтому очень важным является быстрое реагирование на аномальные события и незаконные действия, происходящие в системах информационной безопасности (ИБ). Одной из таких контрмер является создание команд реагирования на компьютерные чрезвычайные события *(Computer Emergency Response Team, CERT)*, которые широко используются в мировой практике.

CERT – это специально созданная организация, которая ответственна за получение, рассмотрение и реагирование на сообщения о компьютерных инцидентах и их действиях. Основная цель CERT состоит в оказании услуг по обработке компьютерных инцидентов для минимизации ущерба и эффективного восстановления после инцидента, связанного с компьютерной безопасностью [1].

Первый CERT в мире был создан на базе Института Программной Инженерии Университета Карнеги Меллона сразу после компьютерной эпидемии, парализовавшей тогдашний прототип Интернета в ноябре 1988 года (ныне действует как Координационный Центр CERT, *CERT Coordination Center – CERT/CC*). В настоящее время в разных странах действует большое количество команд CERT.

Термин «CERT» официально зарегистрирован в США Координационным Центром CERT/CC как торговый знак. Кроме того, значение термина «CERT» изменилось. По прошествии лет команды CERT расширили свой потенциал и теперь наряду с услугами реагирования на инциденты предоставляют полный список сервисов ИБ. Поэтому в конце 1990-х годов преимущественно в Европе начал использоваться новый термин «CSIRT» *(Computer Security Incident Responce Team*, команда реагирования на инциденты компьютерной безопасности). В настоящее время оба термина (*CERT и CSIRT*) используются как синонимы, однако CSIRT является более точным термином. Отметим,

что встречаются также различные аббревиатуры, обозначающие такие группы [2]: *CIRT, IRT, SERT, SIRT, CSIRC, CIRC* и т.д.

В Азербайджане также осуществляется целенаправленная работа по созданию таких команд. Уже несколько лет в Институте Информационных Технологий НАНА действует команда *AZ-CERT.* Пользователями услуг AZ-CERT являются научно-исследовательские институты и организации НАНА и конечные пользователи, использующие информационные ресурсы сети AzScienceNet.

Основными задачами AZ-CERT являются оказание содействия сетевым/системным администраторам и пользователям AzScienceNet в предотвращении, расследовании и ликвидации компьютерных инцидентов, связанных с безопасностью информационных ресурсов в сети AzScienceNet. К другим целям и задачам AZ-CERT относятся составление и публикация докладов об уязвимостях и новостях по ИБ, сбор и составление статистики по инцидентам ИБ в сети AzScienceNet.

Создание CERT-команды и ее эксплуатация не являются исключительно технической проблемой, они имеют многие управленческие, юридические, технические и социальные аспекты, поэтому создание новой CERT-команды сопровождается большими трудностями и часто приходится ссылаться на опыт действующих команд. Учитывая это, в настоящей работе обобщается методология создания команды AZ-CERT для научной компьютерной сети AzScienceNet.

Обзор нормативных документов по управлению инцидентами ИБ

К настоящему времени разработано большое количество международных и национальных нормативных документов, регламентирующих вопросы управления инцидентами ИБ. По тематике управления инцидентами существуют стандарты *ISO/IEC*, стандарты ITU-T E.409:2004 для организаций электросвязи, набор документов CERT/CC, NIST SP 800-61 и ряд других стандартов.

В стандарте ISO/IEC 27001-2005 выдвигаются общие требования к построению системы управления ИБ (СУИБ), относящиеся в том числе и к процессам управления инцидентами.

Стандарт ISO/IEC TR 18044 [3] описывает инфраструктуру управления инцидентами ИБ, даются подробные спецификации для стадий планирования, эксплуатации, анализа и улучшения процесса управления инцидентами.

Документ CMU/SEI-2004-TR-015 [4] описывает методологию планирования, внедрения, оценки и улучшения процессов управления инцидентами. Вводится ряд критериев для оценки эффективности услуг предотвращения, обработки и реагирования на инциденты ИБ, приводятся подробные процессные карты.

В рекомендациях NIST SP 800-61 [5] представлен сборник лучших практик по построению процессов управления инцидентами и реагирования на них. Подробно разбираются вопросы реагирования на разные типы угроз, такие как распространение вредоносного программного обеспечения, несанкционированный доступ и другие.

Основным источником научно-методических разработок по тематике CSIRT являются организации CERT/CC, Институт *SANS* (*SysAdmin, Audit, Network, Security*) и *ENISA* (*European Network and Information Security Agency,* Европейское агентство по сетевой и информационной безопасности).

CERT/CC помогает организациям в планировании, формировании и развитии потенциала по управлению инцидентами ИБ. Организации могут воспользоваться обширным набором технических отчетов, продуктами, курсами тренинга и семинарами, которые доступны глобальному интернет-сообществу (http://www.cert.org/csirts/). CERT/CC предоставляет следующие курсы для менеджеров и технического персонала: создание CSIRT; управление CSIRT; основы обработки инцидентов; глубокая обработка инцидентов; программа обучения по обезвреживанию вредоносных программ. CERT/CC предлагает также программу сертификации CERT – *Certified Computer Security Incident*

Handler (CSIH) для технического персонала и членов CSIRT, сетевых и системных администраторов с опытом обработки инцидентов, профессионалов в области управления инцидентами.

Институт SANS (США) занимается подготовкой и сертификацией специалистов в области ИБ. В онлайновом читальном зале Института SANS можно найти интересные статьи по тематике управления инцидентами ИБ (http://www.sans.org/reading_room/whitepapers/incident/). В середине 1990-х годов SANS подготовил документ Computer Security Incident Handling. Step By Step [6]. В версии 2.3.1 этого документа предлагаются шесть последовательных процессов обработки инцидентов: подготовка, идентификация, локализация, устранение причин, восстановление, извлечение уроков. Приводится описание специальных действий для восьми типов инцидентов (вредоносный код, сканирование, DoS (*Denial of Service*), незаконное использование, шпионаж, мистификация (hoax), неавторизованный доступ, интеллектуальное право). Институт SANS также предлагает курс SANS Security 504 Hacker Techniques, Exploits and Incident Handling.

Для поддержки создания новых групп CSIRT организация ENISA (http://www.enisa.europa.eu/act/cert/support) разработала «Пошаговое руководство по созданию CSIRT» [7], которое доступно почти на 20 языках, в том числе и на русском языке. Данный документ детально описывает процесс создания CSIRT с точки зрения управления бизнес-процессом, а также технической перспективы. В документ включены примеры и контрольные таблицы в форме проектного плана. Агентство ENISA также разработало и сделало доступными несколько документов:

- базовый набор хороших практик эксплуатации CSIRT;
- набор материалов упражнений для тренинга CSIRT-команды;
- потенциальные возможности для национальных/государственных CSIRT;
- руководство по управлению инцидентами;
- обзор распространенных инструментов обработки инцидентов [8].

Этапы создания AZ-CERT

В работах [9–11] предлагается модель построения национальных CSIRT, состоящая из пяти этапов: 1) обучение; 2) планирование CSIRT; 3) реализация CSIRT; 4) эксплуатация CSIRT; 5) сотрудничество. Эта модель с некоторыми изменениями была использована для создания AZ-CERT. Ниже дается краткое описание этих этапов.

Этап 1 – обучение заинтересованных лиц о формировании и развитии команды CSIRT. Этап 1 – это информирующая стадия, где заинтересованные стороны с помощью различных методов обучения изучают, что требуется для создания CSIRT:

- бизнес-процессы и мотивы, стимулирующие необходимость создания CSIRT;
- определение людей, которые будут вовлечены в обсуждение для построения CSIRT;
- каналы коммуникаций, которые будут использованы для связи с клиентами CSIRT;
- источники финансирования, которые могут быть использованы для создания и развития CSIRT;
- техническая инфраструктура, которая будет необходима для поддержки работы CSIRT;
- потенциальный список основных услуг, которые CSIRT может оказать своим клиентам;
- передовой опыт и практическое руководство.

Этап 2 – планирование CSIRT. На этапе 2 осуществляется планирование CSIRT на основе знаний и информации, полученной на этапе 1. Вопросы, рассмотренные на этапе 1, пересматриваются и обсуждаются далее, затем определяются точные детали для выполнения плана. Вкратце укажем контуры деятельности на этом этапе:

- идентификация круга требований к CSIRT (законы и нормативы, которые будут влиять на работу CSIRT, критические ресурсы, которые должны быть защищены, инциденты, о которых будут информировать и т.д.);
- формулирование миссии CSIRT;
- определение организационной модели;
- определение клиентов, которых CSIRT намеревается обслуживать;
- определение методов взаимодействия CSIRT с клиентурой и другими CSIRT или внешними партнерами;
- идентификация коммуникационных интерфейсов между клиентами и CSIRT;
- определение набора предоставляемых услуг;
- определение места физического расположения, персонала, оборудования и инфраструктуры;
- разработка предложений по бюджету, вопросам финансирования проектных планов или планов бизнес-операций.

Этап 3 – реализация CSIRT. На этом этапе используются информация и планы, разработанные на этапах 1 и 2. Процесс реализации состоит из следующих действий:

- получение финансовых средств из источников, определенных на этапе планирования;
- широкое объявление о создании CSIRT;
- согласование механизмов координации и коммуникации с заинтересованными сторонами;
- внедрение безопасных информационных систем и сетевой инфраструктуры для работы CSIRT;
- разработка внутренней политики, регламентов работы и процедур для персонала CSIRT;
- осуществление процессов для взаимодействия CSIRT с ее клиентами;
- выявление и наем (или переназначение) персонала, предоставление соответствующей профессиональной подготовки и образования для персонала CSIRT.

Этап 4 – эксплуатация CSIRT. На этапе эксплуатации CSIRT обладает основными средствами управления инцидентами и команда активно принимает сообщения об инцидентах и координирует реагирование на них. На основе результатов работы услуг оценивается эксплуатационная эффективность CSIRT и совершенствуются операционные моменты. Основные работы, осуществляемые на этом этапе, следующие:

- активное предоставление различных услуг, оказываемых CSIRT;
- разработка и осуществление механизма оценки эффективности работы CSIRT;
- совершенствование работы CSIRT по результатам оценки;
- расширение миссии, услуг и увеличение численности персонала, необходимого для увеличения обслуживаемых пользователей;
- продолжение развития и укрепления политики и процедур CSIRT.

Этап 5 – сотрудничество. CSIRT продолжает свою деятельность и параллельно развивает доверительные отношения с основными спонсорами, партнерами и другими CSIRT. Команда, формируясь за определенный промежуток времени, набирает большой опыт по управлению инцидентами и превращается в доверенного партнера в глобальном сообществе CSIRT. Деятельность на данном этапе включает:

- участие в обмене данными и информацией между другими CSIRT, партнерами, клиентами и экспертами по ИБ;
- участие в глобальных акциях «наблюдения и предупреждения» для поддержки сообщества CSIRT;
- повышение качества деятельности CSIRT путем организации тренингов, семинаров, конференций;

- сотрудничество с другими членами сообщества для разработки документов передового опыта, стратегий и планов реагирования.

Организационная модель AZ-CERT

Существуют разные виды команд реагирования. Команды CSIRT можно классифицировать в зависимости от особенностей обслуживаемого сообщества клиентов (внутренняя, внешняя, коммерческая, государственная, академическая и т.д.) или формы существования и формирования (формальная, ad hoc и т.д.). С учетом различных условий, таких как окружающая среда, финансовое положение и человеческие ресурсы, должна быть выбрана наиболее подходящая организационная модель CSIRT. Детальный анализ организационных моделей CSIRT приводится в [12]. Преимущества и недостатки различных типов CSIRT обсуждаются в [13,14]. Существуют пять основных организационных моделей для CSIRT:

1) ***модель службы безопасности*** – в данной модели нет централизованной организации, которая несет ответственность за обработку инцидентов ИБ. Задачи по обработке инцидентов решаются системными и сетевыми администраторами или другими специалистами по обслуживанию информационной системы;

2) ***модель внутренней распределенной CSIRT*** – в данной модели CSIRT состоит из менеджера CSIRT, ответственного за отчетность и общее управление, а также сотрудников из других подразделений организации. Поскольку служба построена в пределах организации, ее считают «внутренней». CSIRT в данной модели является официально признанной организацией, несущей ответственность за управление реагированием на инциденты;

3) ***модель внутренней централизованной CSIRT*** – в данной модели отдельная команда CSIRT несет общую ответственность за отчетность, анализ и реагирование на все инциденты. Участники команды не могут выполнять другую работу и проводят все свое время, работая на службу и реагируя на все инциденты. Кроме того, менеджер CSIRT отчитывается вышестоящему руководству;

4) ***модель комбинированной распределенной и централизованной CSIRT*** – в тех случаях, когда централизованная CSIRT не может контролировать и поддерживать всю организацию и некоторые участники команды распределены по подразделениям организации для обеспечения в пределах своих областей ответственности того же уровня услуг, который предусмотрен централизованной CSIRT;

5) ***модель координационной CSIRT*** - сотрудники команды сгруппированы в независимые CSIRT по таким характеристикам, как подключение к сети, географические границы и т.п. Они находятся под управлением централизованной CSIRT. Модель координационной CSIRT является подходящей для национальной CSIRT.

Учитывая преимущества и недостатки этих организационных моделей, а также структуру и уровень развития услуг сети AzScienceNet, для команды AZ-CERT была выбрана модель внутренней централизованной CSIRT.

Инциденты и процессы реагирования на инциденты

В нормативных документах и научно-методической литературе можно найти различные, иногда даже противоречивые определения понятия «инцидент». В широком смысле под инцидентом ИБ понимаются любые незаконные, неразрешенные (в том числе по политике ИБ) или неприемлемые действия, происходящие в информационной системе.

В стандарте управления инцидентами ИБ ISO/IEC TR 18044:2004 понятие «инцидент» используется в узком смысле. В этом стандарте вводится понятие «событие ИБ», и понятие «инцидент ИБ» определяется через него.

Согласно стандарту ISO/IEC TR 18044:2004, под событием ИБ понимается состояние системы, сервиса или сети, которое свидетельствует о возможном нарушении политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности. Инцидент ИБ – это одно или серия событий ИБ, которые могут привести к

ущербу и потерям для организации. Потери могут быть как материальными (стоимость информации, эксплуатационные издержки и т.п.), так и нематериальными (репутация организации, изменение морально-психологического климата и т.п.).

Типовые действия, выполняемые в рамках процесса управления инцидентами ИБ, включают:

– идентификация инцидента ИБ (получение информации об инциденте, регистрация инцидента, оценка критичности инцидента, классификация инцидента);

– реагирование на инцидент ИБ (может включать действия CSIRT по эскалации инцидента, идентификации причин возникновения инцидента, изоляции инцидента и устранении его причин);

– восстановление после инцидента ИБ (может включать действия по оперативному внесению изменений в конфигурацию систем, восстановление данных и закрытие инцидента);

– последующие действия по инциденту (могут включать анализ причин инцидента, проведение расследования и предоставление отчета об инциденте заинтересованным сторонам).

Услуги, предоставляемые AZ-CERT

CSIRT может предоставлять своим клиентам большое количество услуг, они могут быть классифицированы как услуги реагирования, профилактические услуги и услуги по управлению качеством обслуживания [1]. Правильный выбор услуг, предоставляемых своим клиентам, является важным шагом. Выбор услуг должен поддержать и давать возможность достижения цели клиентурой CSIRT.

Услуги реагирования являются основными сервисами CSIRT. Они направлены на обработку инцидентов и уменьшение потенциального ущерба. AZ-CERT выбрал следующие услуги реагирования для предоставления своим пользователям:

1) оповещение и предупреждение – данные услуги включают в себя распространение информации, описывающей атаки, уязвимости безопасности, попытки вторжения, компьютерные вирусы и предоставление кратких наборов рекомендованных действий для решения проблемы;

2) ***обработка инцидентов*** – данная услуга включает в себя получение, систематизацию и реагирование на запросы и сообщения, анализ и определение приоритетности инцидентов и событий;

3) ***реагирование на инциденты на месте*** – AZ-CERT обеспечивает непосредственную помощь на месте для того, чтобы помочь клиентам восстановить системы после инцидента;

4) ***поддержка реагирования на инцидент*** – при восстановлении систем после инцидента AZ-CERT помогает и руководит жертвой (-ами) инцидента с помощью телефона, электронной почты, факса или документации;

5) ***координация реагирования на инцидент*** – координируются усилия по реагированию сторон, вовлеченных в инцидент. Они, как правило, включают в себя жертву инцидента, другие стороны, вовлеченные в инцидент, а также любые стороны, нуждающиеся в помощи при анализе инцидента;

6) ***обслуживание артефакта.*** «Артефакт» – это любой файл или объект, найденный в системе, который мог бы быть вовлечен в исследование или атаку системы и сети. Данная услуга состоит из анализа и обработки артефактов, связанных с компьютерными вирусами, «троянскими» программами, «червями», эксплойт-скриптами и прочим инструментарием.

Профилактические услуги нацелены на предотвращение инцидентов посредством повышения осведомленности и тренингов. Из профилактических услуг AZ-CERT оказывает следующие услуги:

1) ***уведомления*** – они включают сигналы тревоги, предупреждения уязвимости, консультации о безопасности и т.п. Такие уведомления дают информацию клиентам о текущих угрозах и шагах, предпринимаемых для борьбы с ними, а также о тенденциях в области ИБ;

2) ***отслеживание технологий*** – для идентификации будущих угроз AZ-CERT наблюдает за развитием новых технических средств, деятельностью злоумышленников и новыми тенденциями в области ИБ. Результатом данной услуги могут быть объявления, руководства или рекомендации;

3) ***услуги по обнаружению вторжений*** – AZ-CERT пересматривает существующие журналы систем обнаружения вторжений (Intrusion Detection Systems, IDS), анализирует их и приступает к реагированию на события, которые возникают в пределах ее действия.

Услуги по управлению качеством систем безопасности имеют долгосрочные цели и состоят из консультирования и образовательных мероприятий. AZ-CERT оказывает следующие услуги по управлению качеством безопасности:

1) ***консультация по безопасности*** – AZ-CERT может предоставить практические советы и рекомендации по управлению ИБ;

2) ***повышение информированности*** – AZ-CERT стремится повысить уровень осведомленности по вопросам ИБ путем выявления и предоставления информации клиентам о мероприятиях, проводимых для улучшения безопасности, и потенциальных угрозах различным системам организации;

3) ***образование/обучение*** – данная услуга включает предоставление информации клиентам по таким темам, как рекомендации по составлению отчетов об инцидентах, соответствующие методы реагирования на них, средства реагирования на инциденты, методы предотвращения инцидентов, а также иную информацию, необходимую для защиты, обнаружения, сообщения и реагирования на инциденты ИБ. Учебные методы включают в себя конференции, семинары, курсы и обучающие программы.

Документ RFC 2350

Работа команд CSIRT подробно описана в стандарте RFC 2350 [15]. Каждая команда CSIRT должна составлять документ на основе RFC 2350 и размещать его на своем веб-сайте. В этом документе указываются информация о документе и контактная информация, описываются устав, услуги, правила CSIRT, формы для доклада об инциденте. В разделе «Устав» определяются виды деятельности, клиентура, спонсоры и вышестоящие организации и полномочия CSIRT. В разделе «Правила» определяются типы нарушений и уровень поддержки, перечисляются организации, с которыми может осуществляться взаимодействие, и определяются политика раскрытия информации, защиты коммуникаций и методы аутентификации. В конце документа RFC 2350 размещается отвод (письменный отказ), предупреждающий пользователей о возможных ограничениях.

Техническая инфраструктура AZ-CERT

Основные элементы технической инфраструктуры CSIRT определяют, исходя из набора услуг, которые команда оказывает или планирует оказывать. В работе [16] на примере CERT.PT (Португалия) анализируется техническая инфраструктура CERT, дается подробное описание компонентов инфраструктуры. Документ [17] также является хорошим источником для выяснения перечня необходимых технических ресурсов.

Телефоны и факс. Прежде всего для коммуникации с клиентами, другими CSIRT, руководством и т.д. требуется телефонная связь. Команда должна быть в состоянии связаться 24x7, определить, кто ответит на звонки в нерабочее время: член команды, другой сотрудник или голосовая почта. Очень важной является регистрация звонков, чтобы проанализировать все как можно скорее.

Некоторые учреждения могут использовать факс в качестве предпочтительного средства коммуникации. Кроме того, факсы можно отправлять или получать, когда сеть или почтовый сервер не работают.

Подключение к Интернету. Естественно, что команда должна быть подключена к Интернету. В идеале команда также должна иметь отдельное интернет-соединение.

Электронная почта. Наиболее используемым средством коммуникации CSIRT является электронная почта. В качестве почтовой системы AZ-CERT использует свободно распространяемый почтовый клиент Mozilla Thunderbird. Установлен простой, легко запоминающийся почтовый адрес info@cert.az, чтобы пользователи сообщили об инцидентах.

Веб-сайт. Веб-сайт, вероятно, самый эффективный способ распространить тревоги и поделиться информацией с клиентами. Учитывая популярность Всемирной паутины, теперь для команды CSIRT обязательно иметь собственный веб-сайт. Команды должны обратить особое внимание на безопасность своих веб-сайтов. Их взлом может вызвать утрату доверия клиентов к команде. Веб-сайт AZ-CERT находится по адресу www.cert.az.

Компьютерное оборудование. В зависимости от размера команды и предоставляемых услуг команде потребуется различное компьютерное оборудование. Оно должно быть выбрано так, чтобы лучше обслуживать нужды клиентов. Для инструментов обработки инцидентов команде потребуются серверы (веб-сервер, сервер баз данных, IDS/Network scanner и т.д.). Для повседневной работы каждый член команды должен быть обеспечен отдельным десктопом или лаптопом, так как они не могут разделять системы с чувствительной информацией.

Сетевая инфраструктура. Команда должна иметь локальную сеть (*LAN*), изолированную от остальной сети организации для минимизации риска подслушивания трафика. Изолирование сетей может быть осуществлено физически (с использованием маршрутизатора или МСЭ) или логически (с помощью *VLAN*).

Для тестирования неизвестного программного обеспечения команде необходимо иметь сеть тестирования. Сеть тестирования тоже следует изолировать от всех сетей (логически или физически). Должна быть также разработана политика, которая определяла бы требования к персоналу CSIRT при тестировании зловредных или других программ на системах CSIRT.

Безопасность коммуникаций. Электронная почта – действенное средство коммуникации; однако она легко может быть сфальсифицирована. Для безопасности коммуникаций AZ-CERT использует GnuPG (*GNU Privacy Guard*). С помощью расширения Enigmail (http://enigmail.mozdev.org) GnuPG работает в почтовом клиенте Mozilla Thunderbird для шифрования и аутентификации сообщений.

Инструменты обработки инцидентов. Для отслеживания процессов обработки инцидентов ИБ используется специализированная программа RTIR (*Request Tracker for Incident Response*) [18]. Свободно распространяемое программное обеспечение RTIR создано командой JANET-CERT (команда безопасности научной и образовательной сети Великобритании - ja.net) и используется многими командами CERT в Европе и в мире. Отметим, что для отслеживания инцидентов существуют также и другие решения: AIRT (*Application for Incident Response Teams, http://www.airt.nl*), OTRS (*Open Ticket Request System*) [19], SIRIOS (*System for Incident Response in Operational Security*, http://sirios.org) и др.

На пилотном сайте Clearinghouse of Incident Handling Tools (CHIHT) [8] можно найти большое количество ссылок на широко распространенные инструменты, используемые CSIRT.

Физическая безопасность CSIRT. Требования физической защиты включают:

- защищенные комнаты для серверов и базы данных;
- защищенные и звуконепроницаемые комнаты для обсуждения действий CSIRT и проведения расследований инцидентов;
- сейф для хранения неэлектронных данных и записей;

- механизмы защищенных коммуникаций, таких как защищенные телефоны, факсы и э-почта;
- физическое изолирование персонала CSIRT от других частей организации.

Резервное копирование данных. Резервное копирование данных считают механизмом безопасности, потому что оно является последней линией защиты против нарушений правил безопасности. Для резервного копирования данных доступны многочисленные инструменты. Например, для пользователей Unix или Linux tar, dump, dd и т.д. Инструмент dd доступен и для Windows. Инструменты типа *Norton Ghost* могут создавать двоичные резервные копии на платформах *Intel.*

Международное сотрудничество AZ-CERT

Для выполнения возложенных обязательств AZ-CERT взаимодействует с другими аналогичными командами, действующими в Азербайджане, с органами государственной власти Азербайджанской Республики, с командами реагирования из зарубежных стран и с другими организациями, работающими в области ИБ.

Как известно, в передовых странах в области информационных технологий уже десятилетия действуют команды CERT, национальные и международные организации, координирующие эти команды, осуществляется обмен опытом и формируется базы знаний. Учитывая, что рост числа кибератак и киберугроз, различных проявлений информационной войны превращается в реальную угрозу, а также происходят конкретные инциденты в информационном пространстве Азербайджана, повлекшие большой ущерб, представление системы реагирования на инциденты ИБ страны в международных организациях становится важной задачей.

В среде глобальной информационной инфраструктуры для предотвращения и реагирования на инциденты ИБ международное сотрудничество имеет особую значимость. По этой причине интеграция команды AZ-CERT в соответствующие международные структуры открывает широкие возможности для эффективного сотрудничества с коллегами из разных стран мира. В 2010 году команда AZ-CERT была зарегистрирована сервисом Trusted Indroducer (TI). Сервис TI (http://www.trusted-introducer.nl/) оказывает услуги в рамках Трансъевропейской ассоциации научно-исследовательских и образовательных сетей (*Trans-European Research and Education Networking Association*, TERENA). Основной задачей TI является создание инфраструктуры доверия между командами CERT европейских стран. TI играет роль доверенной третьей стороны и вводит новые субъекты в инфраструктуру доверия. Сервис TI занимается вопросами регистрации, аккредитации и сертификации команд CERT.

TI оказывает ряд услуг для аккредитованных CERT: доступ к специальным информационным материалам, доступ к системе предупреждения, пользование специальной базой данных и регистрация объектов инцидентов в этой базе данных, участие в мероприятиях, предусмотренных только для членов, инфраструктура шифрования и электронной подписи для обмена информацией во время обработки инцидентов и т.д.

Команда AZ-CERT имеет своей целью оказывать качественные CERT-услуги пользователям и интегрироваться в международные инфраструктуры по CERT-услугам, и ее следующей целью является прохождение аккредитации в TI. Для аккредитации TI предоставляет пригласительный пакет. В пакет входит несколько документов, которые необходимо в течение трех месяцев заполнить и представить в TI. Процедура аккредитации предъявляет командам ряд требований, связанных с качеством предоставляемых ими услуг.

Следующей целью команды AZ-CERT на пути интеграции в международные инфраструктуры является членство в форуме команд реагирования на инциденты безопасности FIRST (*Forum of Incident Response and Security Teams*).

Группы, желающие присоединиться к FIRST, должны найти двух спонсоров – группы, уже являющиеся полноправными членами FIRST. В процессе принятия в членство FIRST, один из спонсоров посещает команду-кандидата и убеждается в том, что она соответствует всем необходимым требованиям к членам FIRST. Также он убеждается в том, что информация и данные, предоставляемые FIRST, будут соответствующим образом обработаны и защищены. Информацию, собранную во время посещения, предоставляют всем членам FIRST для рассмотрения. Требования, предъявляемые к кандидатам в члены FIRST, подробно обсуждаются в документе *Membership Site Visit Requirements V1.0* [14].

Заключение

Функционирование сложной и распределенной информационной системы современной организации неизбежно сопряжено с различными инцидентами информационной безопасности. Создание CSIRT является эффективным средством разрешения инцидентов информационной безопасности, минимизации ущерба от этих инцидентов и уменьшения риска возникновения повторных инцидентов. CSIRT позволяет повысить эффективность работы ИТ-сервисов путем централизации и планирования процессов реагирования на инциденты, а также за счет регламентирования этих процессов.

В этой работе обобщен опыт формирования команды реагирования на инциденты информационной безопасности AZ-CERT. Создание и развитие AZ-CERT производились с учетом рекомендаций международных стандартов в области управления инцидентами, существующей практики и накопленного опыта в других командах по управлению инцидентами.

Принципы создания и развития AZ-CERT могут быть положены в основу построения национальной системы раннего предупреждения и реагирования на инциденты информационной безопасности в информационном пространстве Азербайджана. Создание такой системы – актуальная задача, без решения которой невозможно обеспечение надежной защиты информационных ресурсов страны.

Литература

1. West-Brown M.J., Stikvoort D., Kossakowski K.P. Handbook for computer security incident response teams (CSIRTs). Report: CMU/SEI-98-HB-001. Carnegie Melon University/Software Engineering Institute. 1998, 222 p.
2. Killcrece G., Kosakowsky K., Ruefle R., Zajicek M. State of the practice of Computer Security Incident Response Team (CSIRT‘s). Technical Report No. IA-233, Carnegie Mellon Software Engineering Institute. 2003, 291 p.
3. ISO/IEC TR 18044:2004 – Information technology – Security techniques – Information security incident management. 2004. 50 p.
4. Alberts C., Dorofee A., Ruefle R., Killcrece G., Zajicek M. Defining Incident Management Processes for CSIRTs: A Work in Progress. Technical Report CMU/SEI-2004-TR-015, 2004, 249 p.
5. NIST Special Publication 800-61: Computer security incident handling guide. National Institute of Standards and Technology. January 2004, 148 p.
6. Northcutt S. Computer Security Incident Handling: Step-by-Step (Version 2.3.1). SANS Institute, 2003, 76 p.
7. A step-by-step approach on how to set up a CSIRT. ENISA. 2007. 86 p. http://www.enisa.europa.eu/act/cert/ support/guide.
8. Clearinghouse of Incident Handling Tools (CHIHT) http://www.enisa. europa.eu/act/cert/ support/chiht
9. Killcrece G., Steps for Creating National CSIRTs, Software Engineering Institute, Carnegie Mellon University, Carnegie Mellon University, 2004, 26 p. http://www.cert.org/archive/ pdf/NationalCSIRTs.pdf.

10. Имамвердиев Я.Н. Поэтапный подход к созданию национальной CERT // Материалы республиканской научной конференции «Вопросы применения математики и новые информационные технологии» – Сумгайыт, 26–27 ноября, 2007, стр. 252–254 (на азербайджанском языке).
11. Grobler M., Bryk H. Common challenges faced during the establishment of a CSIRT // Information Security for South Africa (ISSA), 2010, 2-4 August, 2010, Sandton, Johannesburg, pp.1-6.
12. Killcrece G, Kossakowski KP, Ruefle R, Zajicek M. Organizational models for computer incident response teams (CSIRTs). Report: CMU/SEI-2003-HB-001. Carnegie Melon University/Software Engineering Institute. 2003, 158 p.
13. Van Wyk K., Forno R. Incident response. NY: O'Reilly. 2001, 240 p.
14. Mitropoulos S., Patsos D., Douligeris C. On Incident Handling and Response: A state-of-the-art approach / Computers & Security, v.25, no.5, 2006, pp. 351-370.
15. Brownlee N., Guttman E. Expectations for Computer Security Incident Response. – RFC 2350, BCP 21, 1998, 38 p.
16. Penedo D. Technical Infrastructure of a CSIRT // International Conference on Internet Surveillance and Protection – ICISP '06, 26-28 August 2006, Cote d'Azur, France, pp.27-35.
17. Ruefle R., Rajnovic D. FIRST Site Visit Requirements and Assessment, version 1.0, 4/2006, 22 p. http://www.first.org/membership/site-visit-V1.0.pdf.
18. RTIR: Request Tracker for Incident Response. http://www.bestpractical.com/rtir/
19. Kácha P. OTRS: Tool for Security Incident Reports Management. Technical report 12/20074. Praha: CESNET, 2007, 13 p. http://www.cesnet.cz/doc/techzpravy/2007/otrs/.

UOT 004.056

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

Creating CERT-team for scientific computer network AzScienceNet

Incident response is an important aspect of information security management. In this paper the methodology of creating AZ-CERT team for scientific computer network AzScienceNet is described. The review of standard and scientific-methodical documents in the field of incident management is given, the choice of organizational structure and a set of services for AZ-CERT are substantiated, the model of stage-by-stage creation of a CERT-team is proposed. The description of the general process of incident response in network AzScienceNet and technical infrastructure of AZ-CERT is presented as well.

Keywords: *information security, information security incident, incident response, computer emergency response team.*

İmamverdiyev Yadigar N.
AMEA Informasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

AzScienceNet elm kompyuter şəbəkəsi üçün CERT-komandasının yaradılması

İnsidentlərin cavablandırılması informasiya təhlükəsizliyinin idarə edilməsinin vacib aspektlərindən biridir. Bu işdə AzScienceNet elm kompyuter şəbəkəsi üçün AZ-CERT komandasının yaradılması metodologiyası təsvir edilir. İnsidentlərin idarə edilməsi sahəsində normativ və elmi-metodiki sənədlərin icmalı verilir, AZ-CERT komandası üçün təşkilati strukturun və xidmətlərin seçilməsi əsaslandırılır, CERT-komandanın mərhələli yaradılması modeli təklif edilir. AzScienceNet şəbəkəsində insidentləri cavablandırmanın ümumi prosesinin və AZ-CERT-in texniki infrastrukturunun təsviri də verilir.

Açar sözlər: *informasiya təhlükəsizliyi, informasiya təhlükəsizliyi insidenti, insidenti cavablandırma, insidentləri operativ cavablandırma komandası.*