[**RFC 2196 — Справочник по безопасности сетевого узла**](mhtml:file://J:\1\Стандарты%20ИБ\Перевод%20RFC%202196%20—%20Справочник%20по%20безопасности%20сетевого%20узла.mht!/2196.rfc)

Это руководство написано, чтобы создать базовое руководство для разработки системы безопасности для вашего узла. Одним из общих подходов сформулирован Файтесом и др. и включает в себя следующие шаги:

1. Определение того, что вы пытаетесь защитить.
2. Выявление того, от чего вы пытаетесь защититься.
3. Выявление того, откуда и какие исходят угрозы.
4. Осуществление мер, которые должны защитить ваши данные и систему эффективным образом.
5. Постоянное отслеживание процесса и внесение улучшений всякий раз, когда обнаруживаются слабости.
6. **Оценка риска**

**Общее обсуждение**

Анализ риска включает в себя определение того, что вам надо защитить, от чего и как. Это процесс рассмотрения всех рисков, а не аранжировка этих рисков по уровню угрозы. Этот процесс включает в себя принятие эффективных в стоимостном отношении решений, связанных с защитой нужных объектов.

Полный анализ рисков находится за пределами задач данного документа рассмотрели некоторые подходы к данной теме. Однако имеется два пункта анализа риска, которые будут кратко рассмотрены в последующих секциях:

1. Идентификация защищаемых объектов
2. Идентификация угроз

Для каждого из защищаемых объектов, основными целями безопасности являются доступность, конфиденциальность и целостность. Каждая угроза должна рассматриваться с точки зрения ее влияния на эти области.

***Идентификация защищаемых объектов***

Первым шагом при анализе риска является идентификация объектов, которые нужно защитить. Некоторые вещи типа ценной частной информации, интеллектуальной собственности, различное оборудование являются очевидными, но часто упускаются из вида люди, которые используют все это. Существенным пунктом является составление списка объектов, влияющих на проблему безопасности.

Список общих категорий был предложен Пфлегером:

* **Оборудование:**
* CPU, карты, клавиатуры, терминалы, рабочие станции, персональные ЭВМ, принтеры, дисковые драйвы, коммуникационные линии, терминальные серверы, маршрутизаторы.
* **Программы:**
* тексты программ, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы.
* **Данные:**
* во время исполнения, записанные в реальном времени, архивированные off-line, резервные копии, журнальные записи, базы данных, при передаче через транспортную среду.
* **Люди:**
* пользователи, администраторы, группа поддержки оборудования.
* **Документация:**
* на программы, оборудование, системы, локальные административные процедуры.
* **Материалы:**
* бумага, формы, ленты, магнитные носители.

***Идентификация угроз***

Когда список объектов, которые нужно защитить определен, необходимо идентифицировать угрозы. Угрозы могут быть затем рассмотрены с целью определения того, какой потенциал потерь они в себе несут. Это помогает определить, от каких угроз вам следует защищаться. Должны быть рассмотрены следующие классические угрозы. В зависимости от узла, могут существовать и специфические угрозы, которые следует идентифицировать.

1. Неавторизованный доступ к ресурсам и/или информации
2. Непреднамеренное и/или неавторизованное раскрытие информации
3. Отказ в обслуживании (Denial of service)
4. **Политика безопасности**

Политика безопасности является формальным объявлением правил, которым должны подчиняться лица, получившие доступ к технологии и информации организации.

Главной целью политики безопасности является информирование пользователей, персонал и менеджеров об их обязанностях по защите технологии и информации. Политика должна специфицировать механизмы, через которые могут быть реализованы соответствующие требования. Другой целью является обеспечение базиса при конфигурировании и аудите компьютерных систем и сетей в соответствии с политикой. Следовательно, попытка использовать набор средств безопасности в отсутствии определенной политики безопасности является бессмысленным.

Политика использования AUP может также быть частью политики безопасности. Она должна определять, что можно и чего нельзя делать с различными компонентами системы, включая типы трафика, разрешенные в сетях. AUP должна быть максимально прозрачной (заданной явно), чтобы избежать неопределенности и недоразумений. Например, AUP может перечислить какие-то запрещенные группы новостей USENET. (Заметим: AUP для некоторых узлов является приемлемой политикой использования).

Список лиц, которые должны быть вовлечены в создание и подготовку документов по политике безопасности:

1. администратор безопасности узла
2. технический персонал информационной технологии (например, персонал вычислительного центра)
3. администраторы больших групп пользователей организации (например, коммерческие подразделения, отдел компьютерной информатики в университете и т.д.)
4. команда ликвидации инцидентов нарушения безопасности
5. представители групп пользователей, имеющие отношения к политике безопасности
6. ответственные управленцы
7. юрист (если таковой имеется)

Выше в списке приведены представители многих организаций, но перечень не является исчерпывающим. Идея заключается во включении в список ключевых лиц, работающих в сети и имеющих распорядительные функции, лица, определяющие политику, технический персонал, кто знает основные разветвления политического выбора. В некоторых организациях, может быть разумным включить персонал EDP-аудита. Включение этой группы является важным, если результирующие политические заявления должны быть восприняты как можно более широким кругом лиц. Важно также упомянуть, что роль юриста может сильно варьироваться от страны к стране.

Характеристиками хорошей политики безопасности являются:

1. Она должна быть реализуема через процедуры системной администрации, публикацию приемлемых руководств по использованию, или другими приемлемыми способами.
2. Она должна быть, где возможно, внедряема посредством специальных устройств и программ и через санкции, где предотвращение угроз технически невозможно.
3. Она должна ясно определять области ответственности пользователей, администраторов и менеджмента.

Хорошая политика безопасности включает в себя следующие компоненты:

1. Инструкции по технологии приобретения компьютерного оборудования, которые разъясняют требования или предпочтения, связанные с безопасностью. Эта инструкция должна прилагаться к существующим рекомендациям по закупкам и закупочной политике.
2. Политику конфиденциальности, которая определяет разумные требования по обеспечению закрытости частной информации, включая мониторинг электронной почты, контроль операций, выполняемых пользователями и доступ к их файлам.
3. Политику доступа, которая определяет права доступа и привилегии с целью защиты определенных объектов от утраты или раскрытия для пользователей оперативного персонала и менеджмента. Она должна предоставить инструкции для внешнего подключения, передачи данных, устройств подключения к сети и для добавления нового программного обеспечения к системе. Она должна также специфицировать любые необходимые сообщения уведомления (например, сообщения подключения должны предоставлять предупреждения об авторизованном использовании и мониторинге канала, а не просто выдавать строку типа "Welcome").
4. Политику аккаунтинга, которая определяет ответственность пользователей, операционного персонала и менеджмента. Она должна специфицировать возможность аудита и предоставлять инструкции обработки инцидентов (т.e., что делать и с кем связаться, если зарегистрировано вторжение).
5. Политику аутентификации, которая устанавливает эффективную политику паролей и устанавливает инструкции для удаленной аутентификации и использования аутентификационных устройств (например, одноразовых паролей и устройств их генерирующих).
6. Заявление доступности, которое устанавливает пожелания пользователей о доступности определенных ресурсов. Оно должно относиться к избыточности и восстановлению объектов, а также специфицировать часы работы и периоды остановок для обслуживания. Оно должно также включать контактную информацию для информирования о состоянии системы и об отказах.
7. Политику поддержки сети и информационных систем, которая описывает, как персоналу, отвечающему за поддержку внутренней сети и внешних каналов, разрешено использовать технологию доступа. Важный вопрос, который здесь должен быть задан, заключается в том, должен ли быть разрешен внешний доступ и как такой доступ следует контролировать. Другой областью, рассматриваемой здесь, является организация работ с субподрядными фирмами и способ ее управления.
8. Политику сообщений о нарушениях, которая указывает, какой тип нарушений (например, конфиденциальности и безопасности, внутренней или внешней) должен докладываться и кто готовит такие доклады. Доброжелательная атмосфера и возможность анонимного доклада приведет к тому, что вероятность сообщения в случае нарушения будет выше.
9. Поддерживающую информацию, которая предоставляет пользователям, персоналу и менеджменту контактные данные для каждого типа нарушений политики безопасности; инструкции о том, как обрабатывать внешние запросы об инцидентах, сопряженных с нарушением безопасности, или информацию, которая может рассматриваться как конфиденциальная или частная; и перекрестные ссылки на процедуры безопасности и сопряженную с ними данные, такие как политика компании и правительственные законы и постановления.

Для того чтобы политика безопасности была жизнеспособна в долгосрочном плане, она требует большой доли гибкости, основанной на концепции архитектурной безопасности. Политика безопасности должна быть по большей части независимой от специфического оборудования и программного обеспечения. Механизмы актуализации политики должны быть четкими и понятными. Это включает процесс, вовлеченных людей и лиц, кто должен реализовать изменения.

1. **Конфигурация сети и услуг**

***Защита инфраструктуры***

Инфраструктура также нуждается в защите от человеческих ошибок. Когда администратор неверно конфигурирует ЭВМ, сервис, предоставляемый машиной, может деградировать. Это существенно только для пользователей этой ЭВМ, если только эта машине не является первичным сервером, число пострадавших пользователей при этом ограничено. Однако если маршрутизатор некорректно сконфигурирован, все пользователи, кто нуждается в доступе к сети, пострадают. Очевидно, что число пользователей несравненно большее, чем число людей, зависящих от услуг одной ЭВМ.

***Защита сети***

Существует несколько проблем, которые актуальны для сетей. Классической проблемой является атака "denial of service" (отказ в обслуживании). В этом случае, сеть попадает в состояние, при котором она не может более передавать данные пользователя. Существует два способа реализации такого состояния: путем атаки маршрутизаторов и с помощью перегрузки сети избыточным трафиком. Заметим, что термин маршрутизатор в этом разделе используется как активное сетевое устройство самого широкого класса, сюда могут относиться сетевые экраны (firewall), прокси-серверы, и т.д.

Атака на маршрутизатор заключается в блокировке им передачи пакетов или в переадресации их некорректным образом. В первом случае может иметь место не верная конфигурация, произвольная модификация маршрутной таблицы, или "атака перегрузки" (т.e., маршрутизатор забрасывается немаршрутизуемыми пакетами, что вызывает деградацию его рабочих характеристик). Атака перегрузки на сеть аналогична подобной атаке на маршрутизатор, за исключением того, что пакеты являются обычно широковещательными. Идеальной атакой перегрузки являлась бы такая, при которой посылка одного пакета, использующего известную уязвимость, вызывала посылку лавины пакетов.

Другой классической проблемой является фальсификация (spoofing). В этом случае маршрутизатору посылается запрос произвольной модификации маршрутов, заставляя его послать одному или нескольким маршрутизаторам данные, искажающие маршрутизацию пакетов. Это отличается от атаки отказа обслуживания только целью модификации маршрута. При отказе обслуживания, целью является выведение из строя маршрутизатора; что будет быстро замечено пользователями сети. При фальсификации, ложный путь вынудит пакеты двигаться к ЭВМ, где атакер мониторирует передаваемую информацию. Эти пакеты переадресуются затем по их правильному месту назначения. Однако атакер может менять или не менять при этом содержимое пакетов.

Решением большинства этих проблем является предотвращение посылки пакетов модификации маршрутов протоколами маршрутизации (например, RIP-2, OSPF). Существует три уровня защиты: пароль с открытым текстом, криптографическая контрольная сумма и шифрование. Пароли предоставляют минимальную защиту от атакеров, которые не имеют непосредственного физического доступа к сети. Пароли также предлагают некоторую защиту от некорректного конфигурирования маршрутизаторов. Преимуществом паролей является малая избыточность в отношении полосы и ресурсов CPU. Контрольные суммы защищают от присылки ложных пакетов, даже в случае, когда атакер имеет физический доступ к сети. В сочетании с номером по порядку или другим уникальным идентификатором контрольная сумма может защитить также от атак "откликов", когда атакером или «сошедшим с ума» маршрутизатором повторно присылается старое (но корректное) обновление маршрута. Большая безопасность достигается пересылкой закодированной маршрутной информации. Это мешает атакеру определить топологию сети. Недостатком шифрования является избыточность, связанная с обработкой зашифрованных сообщений.

RIP-2 (RFC 1723) и OSPF (RFC 1583) оба поддерживают пароли с открытым текстом в своей основной спецификации. Кроме того, существует расширения этих базовых протоколов, поддерживающие MD5-шифрование.

К сожалению, не существует приемлемой защиты от атак перегрузки (flooding), или некорректного поведения ЭВМ или маршрутизатора, перегружающих сеть. К счастью, этот тип атак является очевидным и по этой причине хорошо диагностируемым и устраняемым.

**Защита услуг**

**Серверы имен (DNS и NIS(+))**

Интернет использует DNS (Domain Name System) для определения адресов ЭВМ и сетевых имен. Службы NIS (Network Information Service) и NIS+ не используются в глобальном Интернет, но являются причиной тех же рисков, что и DNS-сервер. Преобразование имени в адрес является критическим в отношении безопасного функционирования сети. Атакер, который может успешно управлять DNS-сервером, сможет перенаправить трафик, чтобы обойти защиту. Например, трафик для просмотра может быть перенаправлен на скомпрометированную систему; или, пользователи могут быть введены в заблуждения, и они раскроют свои аутентификационные параметры. Организация должна создавать защищенные узлы, работающие в качестве вторичных серверов имен, и защитить свои DNS серверы от DoS-атак, использующих фильтрующие маршрутизаторы.

**Серверы ключей и паролей (NIS(+) и KDC)**

Серверы паролей и ключей защищают жизненно важную информацию (т.e., пароли и ключи) с помощью алгоритмов шифрования. Однако даже пароли с однопроходным шифрованием могут быть раскрыты (здесь зашифрованные слова сравниваются с образцами, которые хранятся в памяти). Следовательно, необходимо гарантировать, что эти серверы недоступны для машин, которые не должны использовать этот вид услуги.

**Серверы аутентификации и прокси (SOCKS, FWTK)**

Прокси сервер предоставляет ряд улучшений безопасности. Он позволяет узлам концентрировать услуги посредством специально выделенной ЭВМ, что допускает мониторирование, сокрытие внутренней структуры и т.д. Такая скрытность услуг является привлекательной мишенью для потенциального атакера. Тип защиты, необходимой для прокси-сервера, сильно зависит от используемого прокси протокола и проксируемых услуг. Общим правилом ограничения доступа является разрешение доступа только машинам, которые действительно нуждаются в услугах. Причем даже для них разрешается доступ только к определенным видам услуг.

**Электронная почта**

Системы электронной почты (e-mail) в течение долгого времени служили источником вторжений, так как почтовые протоколы являются старейшими и наиболее широко используемыми услугами. Кроме того, согласно своей природе, почтовый сервер требует доступа из внешнего мира. Большинство почтовых серверов позволяют доступ от любого субъекта сети. Почтовый сервер обычно состоит из двух частей: агент приема/передачи и агент обработки. Так как почта доставляется всем пользователям и обычно является конфиденциальной, агент обработки требует системных (root) привилегий при доставке. Большинство реализаций e-mail-сервера выполняют обе эти функции, что означает предоставление системных привилегий и принимающему агенту. Это открывает несколько окон уязвимости. Существуют некоторые реализации, которые позволяют разделение этих двух агентов. Такие реализации считаются более безопасными, но все еще нуждаются в тщательной инсталляции, чтобы избежать дополнительных проблем безопасности.

1. **Сетевые экраны (Firewalls)**

Одной из широко используемых мер безопасности является применение сетевых экранов — firewall. Сетевые экраны считаются панацеей от многих, если не от всех проблем безопасности в Интернет. Но это не так. Сетевые экраны являются лишь инструментом системы безопасности. Они предоставляют определенный уровень защиты и являются вообще средством реализации политики безопасности на сетевом уровне. Уровень безопасности, который предоставляет сетевой экран, может варьироваться в зависимости от требований безопасности конкретной машины. Существует традиционный компромисс между безопасностью, простотой использования, стоимостью, сложностью и т.д. Сетевой экран является одним из нескольких механизмов, используемых для управления и наблюдения за доступом к и из сети с целью ее защиты. Сетевой экран действует как шлюз, через который проходит весь входной и выходной трафик защищенной сети. Сетевые экраны помогают установить ограничения на число и тип коммуникаций, которые осуществляются между защищенной сетью и прочими сетями (например, Интернет или другой частью сети узла).

Сетевой экран является способом построения стены между одной частью сети, например, внутренней сетью компании, и глобальным Интернет. Уникальной чертой этой стены является наличие дверей, через которые при тщательном контроле проходит некоторый трафик. Трудной частью такой системы является установление критериев того, какие пакеты разрешить, а каким запретить проход через эти двери. В книгах, написанных о сетевых экранах, используется разная терминология для описания различных форм сетевых экранов. Это может сбивать системных администраторов, которые не знакомы с сетевыми экранами. Следует здесь заметить, что не существует стандартной терминологии для описания сетевых экранов.

Сетевые экраны не обязательно представляют собой отдельную машину. Сетевые экраны скорее представляют собой комбинацию маршрутизаторов, сетевых сегментов, и рабочих станций. Следовательно, в рамках данного обсуждения, термин "сетевой экран" предполагает наличие более одного физического устройства, фильтрующих маршрутизаторов и прокси-серверов.

Фильтрующие маршрутизаторы представляют собой простейший компонент сетевого экрана. Маршрутизатор передает данные в обоих направлениях между двумя (или более) разными сетями. "Нормальный" маршрутизатор принимает пакет из сети A и "переадресует" его к месту назначения в сети B. Фильтрующий маршрутизатор делает то же самое, но решает не только как маршрутизовать пакет, но также следует ли этот пакет посылать куда-либо вообще. Это делается путем установки ряда фильтров, с помощью которых маршрутизатор решает, что делать конкретно с данным пакетом.

Для лучшей безопасности, фильтры обычно ограничивают доступ между двумя связанными сетями к лишь одной ЭВМ. Можно получить доступ к другой сети только через эту защищенную машину. Так как только эта ЭВМ, а не несколько сот машин, может быть атакована, легче поддержать определенный уровень безопасности, так как именно эта машина может быть защищена особенно тщательно. Чтобы сделать доступными через этот сетевой экран ресурсы для легальных пользователей услуги должны переадресовываться соответствующим серверам через эту защищенную машину. Некоторые серверы имеют встроенную переадресацию (например, DNS-серверы или SMTP-серверы), для других услуг (например, Telnet, FTP, и т.д.) могут использоваться прокси серверы, чтобы обеспечить доступ к ресурсам безопасным способом через firewall.

В настоящее время наилучшим вариантом сетевого экрана считается комбинация двух экранирующих маршрутизаторов и одного или более прокси серверов в сети между маршрутизаторами. Такая схема позволяет внешнему маршрутизатору блокировать любые попытки использования нижележащего IP-уровня для разрушения безопасности (IP-фальсификация, маршрутизация отправителя, фрагменты пакетов), в то же время прокси сервер защищает окна уязвимости на уровне верхних протоколов. Целью внутреннего маршрутизатора является блокировка всего трафика кроме направленного на вход прокси сервера. Если реализована эта схема, может быть обеспечен высокий уровень безопасности.

Существуют сетевые экраны в широком диапазоне качества и мощности. Цена коммерческого варианта начинается примерно с $10,000US и достигает $250,000US. "Самодельные" сетевые экраны могут быть построены за меньшую сумму. Следует учитывать, что правильная конфигурация сетевого экрана (коммерческого или самодельного) требует определенного мастерства и знания TCP/IP. Оба типа требуют регулярного обслуживания, установки пакетов обновления и корректировки программ и непрерывного контроля. При оценке бюджета сетевого экрана, эти дополнительные издержки должны также учитываться наряду с аппаратной частью сетевого экрана.

Сетевые экраны могут оказать помощь при обеспечении безопасности узла, они защищают от большого числа атак. Но важно иметь в виду, что они являются лишь частью решения. Они не могут защитить ваш узел от всех типов атак.

1. **Процедуры и услуги безопасности**

***Аутентификация***

В течение многих лет в качестве стандарта применялся метод аутентификации пользователей с помощью многократно используемых паролей. Первоначально, эти пароли использовались клиентами на терминалах для идентификации на центральной ЭВМ. В то время не было сетей (внутри или вне), так что риск раскрытия пароля с открытым текстом был минимальным. Сегодня системы соединяются друг с другом через локальные сети, а эти локальные сети соединяются между собой и с Интернет. Пользователи входят в систему со всего мира; их многократно используемые пароли часто передаются через одни и те же сети открытым текстом, удобным для перехвата по пути кем угодно. И действительно, координационный центр CERT и другие группы реагирования регистрируют огромное число инцидентов, связанных с использование программ типа sniffer, которые перехватывают пароли с открытым текстом.

С появлением новых технологий, типа однократных паролей (например, S/Key), PGP, и устройств символьной аутентификации, базирующейся на признаках (token), люди стали использовать паролеподобные строки в качестве секретных признаков.

* Одноразовые пароли
* Kerberos
* Выбор и защита секретных ключей и PIN

***Конфиденциальность***

Всегда будет существовать информация, которую ваш узел хотел бы защитить от несанкционированного доступа. Операционные системы часто имеют встроенные механизмы защиты файлов, которые позволяют администратору управлять тем, кто в системе может иметь к ним доступ, или "читать" содержимое файла. Более строгим путем обеспечения конфиденциальности является шифрование. Шифрование осуществляется путем скрэмблирования данных так, что очень трудно и долго для неавторизованного клиента добраться до содержимого исходного текста. Авторизованные клиенты и владелец информации обычно владеет соответствующим ключом дешифрования, который позволяет им легко расшифровать текст и преобразовать его в читаемую форму. Мы рекомендуем узлам использовать шифрование для предоставления конфиденциальности и защиты важной информации.

Использование шифрования определяется иногда правительственными и локальными правилами, так что мы рекомендуем администраторам быть информированными относительно законов или политик, которые регламентируют использования этой техники до ее использования.

***Целостность***

Как администратор, вы захотите быть уверены, что информация (например, файлы операционной системы, данные компании и т.д.) не изменялась неавторизованным образом. Это означает, что вы захотите предоставить некоторую гарантию целостности информации в вашей системе. Одним из способов реализации этого является вычисление контрольной суммы исходного файла, запомнив эту контрольную сумму и периодически (или по запросу) проверяя ее, можно убедиться в том, что файл не был модифицирован.

Некоторые операционные системы поставляются с программами контрольного суммирования, например, UNIX-программа суммирования. Однако, они не дают защиты, которая вам на самом деле нужна. Файлы могут быть модифицированы так, что контрольная сумма останется неизменной! Следовательно, мы советуем, чтобы вы использовали криптографически сильную программу, такую как MD5 для вычисления дайджестов, чтобы получить контрольную сумму для контроля целостности.

Существуют другие приложения, где нужно гарантировать целостность, такие как передача почтовых сообщений. Доступны продукты, которые могут предоставить такую возможность.

***Авторизация***

Авторизация относится к процессу предоставления привилегий процессам и в конечном итоге пользователям. Это отличается от аутентификации, которая осуществляет идентификацию пользователя. После надежной идентификации привилегии, права, принадлежности и разрешения определенных действий определяются авторизацией.

Явное перечисление авторизованных действий для каждого пользователя (и процесса пользователя) с учетом всех ресурсов (объектов) в разумной системе невозможно. В реальной системе используются определенные методики для упрощения процесса предоставления и проверки авторизации.

Один подход, популяризованный системами UNIX, заключается в присвоении каждому объекту трех классов пользователей: владелец, группа и прочий мир. Владельцем является либо создатель объекта, либо пользователь, назначенный администратором. Разрешения пользователя (чтение, запись и исполнение) предоставляются только ему. Группой является объединение пользователей, которые совместно владеют объектом. Групповыми разрешениями могут быть чтение, запись и исполнение. К остальному миру относятся все, кроме перечисленных выше. Для них может быть разрешено (или запрещено) чтение, запись и исполнение.

Другим подходом является привязка к объекту списка, в котором перечислены идентификаторы всех разрешенных пользователей (или групп). Это ACL (Access Control List — список управления доступом). Преимущества ACL заключаются в том, что они легко создаются и обслуживаются (один список на объект) и очень легко визуально проверить, кто имеет доступ и к чему. Недостатком является необходимость дополнительных ресурсов, необходимых для запоминания таких списков, для больших систем нужно огромное число списков.

1. **Контрольные проверки**

**Процесс сбора данных**

Процесс сбора должен осуществляться ЭВМ или ресурсом, к которому производится обращение. В зависимости от важности данных и необходимости их иметь под рукой в моменты, когда происходит отказ в обслуживании, информация может храниться локально или передаваться в память после каждого события.

В основном существует три способа запоминания контрольной информации: в файлы чтения/записи на ЭВМ, в устройствах с однократной записью (например, CD-ROM или специально сконфигурированный привод магнитной ленты), или с помощью аппаратуры записи типа строчного принтера. Каждый метод имеет преимущества и недостатки.

Система журнальных файлов является наименее ресурсоемкой из названных методов и наиболее легко конфигурируемой. Она позволяет немедленный доступ к записям для анализа, который может быть важным в момент атаки. Система журнальных файлов является также наименее надежным методом. Если ведущая журнал ЭВМ компрометирована, файловая система является первым объектом, подвергаемым атаке; атакер без труда может скрыть следы своего вторжения.

Сбор контрольных данных с помощью устройства с однократной записью требует несколько больших усилий по конфигурации, чем журнальные файлы, но имеет значительное преимущество большей безопасности, так как атакер не сможет ликвидировать следы своего вторжения. Недостатком этого метода является необходимость поддержания такого устройства и стоимость.

**Нагрузка сбора данных**

Сбор контрольных данных может привести к заметному расходованию ресурсов памяти, так что проблема переполнения и резервирования этих ресурсов должна рассматриваться заранее. Существует много способов уменьшения требуемого объема памяти. Во-первых, данные могут быть архивированы посредством одного из стандартных методов. Или, требуемое место в памяти может быть минимизировано за счет непродолжительного хранения полных данных с последующей записью коротких резюме в долговременный архив. Главный недостаток последнего метода заключается в необходимости немедленного детектирования и реакции на инцидент. Часто инцидент имеет определенную протяженность во времени и это событие может быть замечено персоналом не сразу и потребуется определенное время, чтобы разобраться, что на самом деле происходит. В определенный момент времени оказывается крайне полезным иметь под рукой подробный журнал событий. Если имеются лишь краткие резюме, этого может оказаться недостаточно для полного анализа инцидента.

**Обработка и сохранение контрольных данных**

Контрольные данные узла должны быть одними из наиболее тщательно сохраняемых, для них должны создаваться обязательно контрольные копии. Если бы атакер получил доступ к журналам контрольных данных, самой системы, риск был бы слишком велик.

Контрольные данные могут также стать ключевыми для исследования, понимания и предъявления претензий инициатору инцидента. По этой причине, рекомендуется проконсультироваться с юристом узла при определении решении того, как следует обрабатывать контрольные данные. Это должно быть сделано до того, как произошел инцидент.

Если план обработки данных не определен должным образом до инцидента, может случиться, что после инцидента не окажется средств восстановления из-за некорректной обработки данных.

1. **Контрольное копирование**

Процедура создания контрольных копий (backups) является классической частью операционной системы ЭВМ. В контексте данного документа резервные копии рассматриваются как часть общего плана обеспечения безопасности узла. Существует несколько важных аспектов резервного копирования, существенных в данном случае:

1. Убедитесь, что ваш узел формирует контрольные копии
2. Убедитесь, что ваш узел использует для резервного копирования запоминающее устройство за пределами узла. Расположение устройства записи должно быть тщательно выбрано с точки зрения безопасности и доступности.
3. Рассмотрите возможность шифрования ваших контрольных копий, чтобы иметь дополнительную гарантию защиты на случай, если эти данные выйдут за пределы узла. Однако, проверьте, чтобы ваша схема управления ключами была достаточно хороша для обеспечения возможности восстановления данных в любой момент в будущем. Проверьте также, чтобы вы имели доступ к необходимым программам, в любой момент, когда потребуется дешифрование.
4. Не думайте, что ваши контрольные копии всегда хороши. Часто случается при проблемах с безопасностью, что проходит много времени, прежде чем факт инцидента будет замечен. В таких случаях могут пострадать и контрольные копии.
5. Периодически проверяйте корректность и полноту ваших контрольных копий.
6. **Обработка случаев нарушения безопасности**

Разделы этой главы предоставляют обзор и перечень стартовых мер для формирования политики безопасности вашего узла при проведении работ в случае инцидентов. Это:

1. Подготовка и планирование (каковы цели и предпосылки анализа инцидентов).
2. Уведомление (с кем следует контактировать в случае инцидента).
   * Местные менеджеры и персонал
   * Правовое обеспечение и следственные органы
   * Группы реагирования на инциденты, сопряженные с компьютерной безопасностью
   * Узлы, вовлеченные или пострадавшие от инцидента
   * Внутренние коммуникации
   * Связь с общественностью и пресс-релизы

3. Идентификация инцидента (является ли это инцидентом и насколько он серьезен).

4. Обработка (что следует сделать, когда инцидент произошел).

* + Оповещение (кто должен быть уведомлен об инциденте)
  + Журналы свидетельств и активности (какие записи до, во время инцидента и после него должны быть рассмотрены)
  + Ограничение последствий (как можно минимизировать ущерб)
  + Искоренение (как исключить причины инцидента)
  + Восстановление (как восстановить услуги и системы)
  + Ликвидация последствий (какие действия должны быть предприняты после инцидента)

5. Последствия (каковы последствия последних инцидентов).

6. Административная реакция на инцидент.

**Подготовка и планирование обработки инцидентов**

Обучение эффективному реагированию на вторжение является важным по многим причинам:(

1. Защита объектов, которые могут быть компрометированы
2. Защитные ресурсы, которые могли бы быть использованы с большей пользой, если инцидент не требует их услуг
3. Выполнение регламентаций (правительственных или других)
4. Предотвращение использования ваших систем в атаках против других систем (которые могут навлечь на вас юридическую ответственность)
5. Минимизация потенциала негативных проявлений

При любом наборе предварительно спланированных мер, эти меры могут иметь разные приоритеты в разных узлах. Рассмотрим набор типовых мер, которые должны быть предприняты в связи с инцидентом:

1. Описать, как это произошло.
2. Выяснить, как избежать дальнейшего использование тех же самых уязвимостей.
3. Исключить последствия и будущие инциденты.
4. Оценить воздействие и ущерб от инцидента.
5. Восстановить систему после инцидента.
6. Обновить политику и процедуры, как это требуется.
7. Найти, кто это сделал (если это возможно).

В силу природы инцидента может иметь место конфликт между анализом источника проблемы и восстановлением систем и услуг. Общие задачи (типа обеспечения целостности критических систем) может стать причиной отказа от анализа инцидента. Конечно, это важное управленческое решение, но все вовлеченные лица должны понимать, что без анализа тот же самый инцидент может повториться.

Важно также определить заранее приоритет действий при инциденте. Иногда инцидент может быть настолько сложным, что невозможно, реагируя на него, сделать все сразу; приоритеты в этом случае крайне важны. Хотя приоритеты варьируются от организации к организации, ниже предложенные приоритеты могут служить отправной точкой для определения реакции вашей организации:

* **Приоритет номер один**
* Защитить человеческую жизнь и безопасность людей; человеческая жизнь имеет всегда приоритет перед любыми другими соображениями.
* **Приоритет два**
* Защитить категорированные и/или важные данные. Предотвратить использование категорированных и/или важных систем, сетей или узлов. Информировать подвергшиеся атаке категорированные и/или важные системы, сети или узлы об уже случившемся вторжении. (Ознакомьтесь с регламентациями вашего узла или правительства)
* **Приоритет три**
* Защита остальной информации, включая частную, научную, управленческую и прочую, так как потеря данных стоит дорого с точки зрения ресурсов. Предотвратить использование других систем, сетей или узлов и проинформировать уже затронутые системы, сети или узлы об успешном вторжении.
* **Приоритет четыре**
* Предотвращение разрушения систем (например, потерю или модификацию системных файлов, разрушение драйвов дисков и т.д.). Разрушение систем может вызвать дорогостоящие отказы и длительное восстановление.
* **Приоритет пять**
* Минимизировать урон вычислительных ресурсов (включая процессы). Во многих случаях лучше закрыть систему или отключить ее от сети, чем рисковать данными или системой. Узлы должны будут сопоставить возможности закрытия, отключения и сохранения открытого состояния. Может существовать локальное соглашение обслуживания, которое требует поддержания системы в подключенном состоянии даже с учетом возможности дальнейшего разрушения. Однако ущерб и область воздействия инцидента могут быть настолько значительны, что соглашение обслуживания может быть пересмотрено.

Важным выводом для определения приоритетов является то, что, если затронуты вопросы человеческой жизни и национальная безопасность, более существенным оказывается сохранение данных, чем системное программное обеспечение и оборудование. Хотя в случае инцидента нежелательно иметь любой ущерб или потерю, системы могут быть замещены. Однако, потеря или компрометация данных (особенно категорированных или частных) обычно не может быть приемлемым при любых обстоятельствах.

**Идентификация инцидента**

Существуют определенные указания или "симптомы" инцидента, которые заслуживают особого внимания:

1. Аварии системы
2. Аккаунты новых пользователей (неожиданно создан аккаунт RUMPLESTILTSKIN), или необычно высокая активность на аккаунте, который был обычно мало активен.
3. Новые файлы (обычно с новыми или странными именами, такими как data.xx или k или .xx).
4. Рассогласование аккаунтингов (в системе UNIX вы можете заметить сжатие файлов аккаунтинга, называемого /usr/admin/lastlog, все что вызывает подозрение может быть результатом действия атакера).
5. Changes in file lengths or dates (a user should be suspicious if .EXE files in an MS DOS computer have unexplainedly grown by over 1800 bytes).
6. Попытки записи в системные файлы (системный менеджер заметил, что привилегированный пользователь в системе VMS пытается отредактировать RIGHTSLIST.DAT).
7. Модификация или стирание данных (файлы начинают исчезать).
8. Отказ в обслуживании (системный менеджер и другие пользователи оказываются блокированы в системе UNIX, система перешла в режим с одним пользователем).
9. Необъяснимое, плохое поведение системы
10. Анормальности (на дисплее отображается "GOTCHA" или частые необъяснимые звуковые сигналы).
11. Подозрительные попытки (имеют место множественные неуспешные попытки авторизоваться из другого узла).
12. Подозрительный просмотр (кто-то становится пользователем root системы UNIX и открывает файл за файлом, принадлежащие разным пользователям).
13. Невозможность пользователя авторизоваться из-за модификаций его/ее аккаунта.

Этот список не является исчерпывающим; мы лишь перечислили несколько общих индикаторов. Лучше всего сотрудничать с техническим персоналом и лицами, ответственными за безопасность, чтобы принять совместное решение, произошел инцидент или нет.

***Типы инцидентов***

Для того чтобы идентифицировать область и воздействие надо определить набор критериев, которые соответствуют данному узлу и типу доступных соединений. Ниже представлены некоторые вопросы:

1. Охватывает ли данный инцидент несколько узлов?
2. Инцидент затронул много ЭВМ вашего узла?
3. Вовлечена ли важная (чувствительная) информация?
4. Что является входной точкой атаки (сеть, телефонная линия, локальный терминал и т.д.)?
5. Вовлечена ли пресса?
6. Каков потенциальный ущерб инцидента?
7. Каково ожидаемое время улаживания инцидента?
8. Какие ресурсы нужны на ликвидацию инцидента?
9. Подразумевается ли привлечение юридической поддержки?

***Обработка инцидентов***

**Типы уведомлений и обмен информацией**

Когда вы убедились, что инцидент имел место, должен быть проинформирован соответствующий персонал.

Прежде всего, любое оповещение местного или внешнего персонала должно быть непосредственным. Это требует, чтобы любое заявление (по электронной почте, телефону, факсом, через пейджер или любым другим способом) предоставляло информацию об инциденте ясно, кратко и профессионально.

Если привлекается команда по ликвидации последствий инцидента, может быть нужно, заполнить форму для информационного обмена. Хотя это может показаться дополнительной нагрузкой и приводит к определенным задержкам, это помогает команде действовать с минимальным набором информации. Команда реагирования может быть способна действовать в отношении некоторых аспектов инцидента, о которых местный администратор не проинформирован. Если информация передана кому-то еще, должен быть предоставлен следующий минимум данных:

1. Временная зона журнальных записей, в формате GMT или местное время
2. Информация об удаленной системе, включая имена ЭВМ, IP-адреса и (может быть) ID пользователей
3. Все журнальные записи, связанные с удаленным узлом
4. Тип инцидента (что случилось, почему вы должны принять меры)

Если локальная информация (т.e., ID местного пользователя) включена в журнальные записи, будет необходимо отредактировать записи, чтобы избежать нарушения конфиденциальности. Вообще, вся информация, которая может помочь удаленному узлу решить проблему, связанную с инцидентом, должна быть предоставлена, если только это не противоречит местной политике безопасности.

**Защита улик и журнальные записи активности**

следует записывать:

1. Все системные события (audit records)
2. Все ваши действия (снабженные временными метками)
3. Все внешние переговоры (включая имена лиц, с которыми вы говорите, дата, время и содержание разговора)

Наиболее прямой способ документирования — ведение журнальных файлов. Это позволяет вам получить централизованный, хронологический источник информации, когда вам это нужно, вместо записи данных на листы бумаги. Большая часть этой информации является уликами для будущего судебного процесса. Таким образом, когда возможно последующее юридическое расследование, следует придерживаться определенных процедур и избегать риска юридических процедур при некорректном обращении с уликами. Если приемлемо, могут быть предприняты следующие шаги.

1. Регулярно (например, каждый день) включайте копирование подписанных копий вашего журнала событий (а также среды, которую вы используете для записи системных событий).
2. Хранитель (custodian) должен хранить копии этих страниц в безопасном месте (например, в сейфе).
3. Когда вы предоставляете информацию для записи, вы должны получить подписанный, датированный доклад от хранителя документов.

Нарушение в процессе реализации этих процедур может привести к тому, что любые улики, которые вы получили, будут признаны в суде недействительными.

**Противодействие**

Целью противодействия является ограничение масштабов развития атаки. Существенной частью противодействия является принятие решения (например, определение, следует ли выключить систему, отключить ее от сети, мониторировать систему или сетевую активность, установить ловушки, закрыть функции, такие как удаленная передача файлов и т.д.).

Этот этап должен включать в себя выполнение определенных заранее процедур. Ваша организация или узел должны, например, определить приемлемые риски в ходе преодоления последствий инцидента, и предложить соответствующие действия и стратегии. Это особенно важно, когда необходимо быстрое решение и невозможно при первом контакте заинтересованных сторон обсудить возможное решение. В отсутствии определенных заранее процедур лицо, ответственное за ликвидацию последствий инцидента, не имеет полномочий принимать сложные управленческие решения (вроде потери результатов сложного эксперимента при отключении системы). Данный этап завершается оповещением всех заинтересованных полномочных представителей.

**Подавление**

Помощь в ликвидации причин и последствий инцидента могут оказать специальные программы, такие, например, как антивирусные. Если атакером были созданы какие-либо файлы, архивируйте их прежде чем уничтожать. В случае вирусного заражения важно очистить и повторно отформатировать среду, содержащую инфицированные файлы. Наконец, убедитесь, что все резервные копии не содержат зараженных файлов. Многие системы, инфицированные вирусами, повторно заражаются просто потому, что народ своевременно не удаляет вирусы с контрольных копий. После ликвидации причин и последствий следует сформировать новые контрольные копии (backup).

**Восстановление**

Когда причина инцидента устранена, следующим этапом становится ликвидация последствий и восстановление системы. Целью восстановления является возвращение системы в нормальное состояние. Вообще, восстановление услуг в порядке запросов является оптимальной стратегией и минимизирует неудобства пользователей. Поймите, что правильные процедуры восстановления системы крайне важны и должны быть специфицированы для узла заранее.

**Доработка**

Наиболее важным элементом стадии доводки является выполнение анализа инцидента и его последствий. Что конкретно случилось, и когда? Насколько эффективно действовал персонал во время инцидента? В какой информации персонал нуждается в первую очередь, и как такую информацию получить как можно быстрее? Что следует сделать персоналу по другому в следующий раз?

После инцидента, разумно написать доклад, описывающий точную последовательность событий: метод обнаружения, процедура коррекции, процедура мониторинга и резюме полученного опыта. Это поможет ясно понять проблему. Создание формальной хронологии событий (включая временные метки) важно также по юридическим причинам. Доклад доводки является ценным по многим причинам. Он используется в случае возникновения других сходных инцидентов. Важно также как можно быстрее получить денежную оценку ущерба, вызванного инцидентом. Эта оценка должна включать суммы, связанные с потерей программ и файлов (особенно стоимость частных данных, которые могут быть раскрыты), выхода из строя оборудования и трудозатраты для восстановления измененных файлов, реконфигурации поврежденных систем и пр. Эта оценка может стать основой для последующего преследования виновных. Доклад может помочь руководству составить представление о состоянии сетевой безопасности организации.

***Последствия инцидента***

В связи с инцидентом нужно предпринять ряд действий. Эти действия перечислены ниже:

1. Должна быть проведена инвентаризация всех повреждений (т.e., в результате тщательного осмотра должно быть определено, насколько система пострадала от инцидента).
2. Чтобы исключить возможность такого вторжения, план безопасности должен быть скорректирован с учетом опыта, извлеченного после инцидента.
3. С учетом данного инцидента должен быть произведен новый анализ рисков.
4. Расследование и наказание лиц, виновных в инциденте, если это считается желательным.

**Ответственность**

Одно дело — защитить свою собственную сеть, но совершенно другое, предположить, что нужно защищать другие сети. В процессе разрешения проблемы инцидента становятся очевидными определенные слабости системы. Достаточно легко и даже соблазнительно найти виновника инцидента, но это не всегда оптимальный путь.

Наилучшее правило, когда это касается права собственности, никогда не использовать ни одно из средств удаленного узла, если оно не является общедоступным. Это ясно исключает любой вход в систему (такой как rsh или сессия авторизации), который не разрешен явно. Может показаться очень привлекательно, после того как уязвимость безопасности определена, испытать эту слабость на соседе и проверить, уязвим ли удаленный узел. Не делайте этого! Вместо этого, попытайтесь установить контакт с пострадавшим узлом.