**Задание на 26.01.2022**

МДК 03.02 Программно-аппаратные средства защиты информации

1. **Сделать конспект лекции**
2. **Сделать практическую работу «**DoS-атаки на серверы удаленного доступа. Автоматические программы».

**Вопросы к практической работе**

1. Принцип работы каждой из сетевых атак типа «отказ в обслуживании»?
2. Какие аномалии в сетевом трафике и ресурсах сервера вы заметили в каждой̆ атаке?
3. Что является признаком конкретной атаки?
4. В чем отличие DDoS от DoS?
5. Что такое UDP-флуд?
6. Как защититься от различных атак DoS/DDoS?
7. Что такое SYN-флуд? Укажите решение защиты от SYN-флуда с помощью iptables.
8. Как определить, что осуществляется атака SYN-флуд?
9. Как осуществить защиту от HTTP-флуда?
10. Как работают атаки типа SlowLoris?
11. Как совершить DDoS-атаку на почтовый сервер и в дальнейшем реализовать его защиту?
12. Как работают атаки типа SSL? Как определить, что осуществляется атака?
13. Перечислите Amplification атаки с коэффициентами их усиления.
14. Опишите теоретически возможность расследования DoS/DDoS атак, установление личности атакующего, определение источников атак.
15. **Отчет отправить на почту svebalch@mail.ru**

**Лекция 4**

**ПОНЯТИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ**

**В КОМПЬЮТЕРНЫХ СИСТЕМАХ**

Всеобщая осведомленность в необходимости обеспечения безопасности компьютерных систем растет по мере того, как очень важные вопросы информационной безопасности все больше и больше становятся зависимыми от взаимодействия компьютерных систем. Безопасность является основной заботой бизнеса, который хочет использовать Интернет в коммерческих целях и для поддержания деловых отношений. Увеличение осведомленности в необходимости защиты вылилось в увеличение количества попыток интегрировать защитные механизмы в компьютерные системы. Механизмы защиты операционной системы играют решающую роль в обеспечении безопасности на более высоких уровнях.

Необходимость наличия встроенных средств защиты на уровне операционной системы бесспорна, операционная система обеспечивает защиту механизмов прикладного уровня от неправильного использования, обхода или навязывания ложной информации. Если она не сможет удовлетворить этим требованиям, появятся уязвимости в масштабах всей системы. Потребность в защищенных операционных системах особенно важна в современных компьютерных средах. Для этого и разрабатывается политика безопасности

Политика информационной безопасности в компьютерных системах — это совокупность требований к функциям, архитектуре, составу и регламенту функционирования информационной системы, которые определяют траектории информационных процессов и состояния системы, безопасные для обрабатываемой информации.

**1. Разработка политики информационной безопасности**

Политика информационной безопасности формируется на основе информационного и технического обследования информационной системы, анализа информационных рисков и оценки защищенности информации, в соответствии с требованиями Российских нормативно-руководящих документов, а также рекомендаций международных стандартов в области защиты информации (например, ISO 17799), что особенно важно для предприятий5 осуществляющих взаимодействие с иностранными партнерами.

Аттестация автоматизированной системы по требованиям защищенности информации в соответствии с Российским законодательством является обязательным, условием, позволяющим обрабатывать информацию ограниченного доступа. Сертификация автоматизированной системы по международным требованиям информационной безопасности делает предприятие более привлекательным для зарубежных компаний при выборе деловых партнеров в России.

В крупных организациях в информационные процессы вовлечена масса людей. для большинства из них требования политики безопасности отнюдь не очевидны. Чем сложнее пользователям приспособиться к установленной политике, тем менее вероятна ее работоспособность. На начальном этапе ее требования наверняка будут нарушаться, да и в будущем полностью избежать этого не удастся.

Необходимо осуществлять непрерывный контроль выполнения правил политики безопасности, как на этапе ее внедрения, так и в дальнейшем, фиксировать нарушения, разбираться в их причинах.

Одна из основных форм этого контроля — регулярное проведение как внутреннего, так и внешнего аудита безопасности.

Политику безопасности необходимо совершенствовать, чтобы она оставалась эффективной. Даже если удалось разработать и внедрить эффективную политику безопасности, работа на этом не заканчивается. Обеспечение информационной безопасности — непрерывный процесс. Технологии стремительно изменяются, системы устаревают, а многие процедуры теряют эффективность. Политики безопасности должны непрерывно совершенствоваться, чтобы оставаться эффективными.

Политика безопасности включает в себя 3 уровня защиты (рис. 2.1):



*Рис. 2.1. Три уровня защиты*

— 1-й уровень — защита на уровне аппаратных средств рабочих станций и серверов, активизируемая на каждом компьютере до загрузки ос;

— 2-й уровень создание замкнутого интерфейсного окружения и защита на уровне локальных компьютерных ресурсов;

— 3-й уровень — защита на уровне общих ресурсов компьютерной сети, включая блокирование несанкционированного межсетевого доступа.

Работоспособность и эффективность существующих политик должны регулярно проверяться. Устаревшие Политики должны пересматриваться.

**2. Методология политики безопасности компьютерных систем**

Политика безопасности в компьютерных системах должна включать:

* Предмет политики. Для того чтобы описать политику по данной области, администраторы сначала должны определить саму область с помощью ограничений и условий в понятных всем терминах (или ввести некоторые из терминов). Часто также полезно явно указать цель или причины разработки политики — это может помочь добиться соблюдения политики. Эта политика также может определять, учитываются ли другие аспекты работы, не имеющие отношения к безопасности.
* Описание позиции организации. Как только предмет политики описан, даны определения основных понятий и рассмотрены условия применения политики, надо в явной форме описать позицию организации (то есть решение ее руководства) по данному вопросу.
* Применимость. Проблемные политики требуют включения в них описания применимости. Это означает, что надо уточнить где, как, когда, кем и к чему применяется данная политика.
* Роли и обязанности. Необходимо описать ответственных должностных лиц и их обязанности в отношении разработки и внедрения различных аспектов политики.
* Соблюдение политики. Могут быть явно описаны наказания, которые должны быть увязаны с общими обязанностями Сотрудников в организации. Если к сотрудникам применяются наказания, они должны координироваться с соответствующими должностными лицами и отделами. Также может оказаться полезным поставить задачу конкретному отделу в организации следить за соблюдением политики.
* Консультанты по вопросам безопасности и справочная информация. для любой проблемной политики нужны ответственные консультанты, с кем можно связаться и получить более подробную информацию. Так как должности имеют тенденцию изменяться реже, чем люди, их занимающие, разумно назначить лицо, занимающее конкретную должность как консультанта. Например, по некоторым вопросам консультантом может быть один из менеджеров, по другим — начальник отдела, сотрудник технического отдела, системный администратор или сотрудник службы безопасности

**3. Основные положения политики информационной безопасности**

Стандарт ISO 17799 является обобщением опыта обеспечения информационной безопасности зарубежными предприятиями и организациями по стандартизации. В нем нет детализированных требований по информационной безопасности, однако описан общий подход к организационным и техническим аспектам защиты информации, которые позволяют сформировать адекватную политику информационной безопасности. Реализация рекомендаций по организационным вопросам защиты информации позволяет сделать политику информационной безопасности комплексной, что в сочетании с решением технических вопросов защиты информации в соответствии с Российскими нормативно-руководящими документами, обеспечивает относительно высокий уровень безопасности.

В стандарте ISO 17799 даны рекомендации по классификации объектов защиты и указаны аспекты информационной безопасности, которые должны быть определены в политике безопасности, разрабатываемой для конкретной организации:

— определение информационной безопасности и перечень составляющих ее элементов, положение о целях управления и принципах информационной безопасности;

— разъяснение основных положений политики информационной безопасности, принципов ее построения и стандартов в области защиты информации, соответствие политики безопасности требованиям российского и международного законодательства;

— порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе;

— организация защиты от компьютерных вирусов и других разрушающих программ средств;

— обеспечение непрерывности функционирования информационной системы;

— последствия нарушения политики информационной безопасности;

— порядок изменения политики информационной безопасности при модернизации системы управления или информационной системы;

— должностные обязанности и ответственность за обеспечение информационной безопасности руководителей и сотрудников организации

— организационно-распорядительные документы, которые Должны быть изданы при формировании политики информационной безопасности (положения, инструкции, регламенты и т.п.).

Определение перечня объектов, подлежащих защите в компьютерной системе, сложная, но необходимая задача, решение которой позволяет идентифицировать информационные ресурсы, подлежащие защите и определить классы объектов защиты, которые могут быть созданы при эксплуатации системы, и, следовательно, заранее определить политику безопасности относительно этих объектов. Однако для разработки адекватной политики информационной безопасности, кроме того, требуется построить информационную модель системы, которая позволит выделить объекты, определяющие траектории информационных процессов в системе и провести анализ информационной безопасности в соответствии с реализуемой стратегией разграничения доступа. Разработку информационной модели системы способны выполнить только специалисты по защите информации, имеющие профессиональную подготовку и опыт разработки таких моделей для различных информационных систем.

Соответствие законодательству — важный пункт политики безопасности. Страны мирового сообщества имеют специфичные законы, регламентирующие применение информационных технологий на своих территориях. Такие особенности имеются и в Российском законодательстве. Поэтому при разработке политики безопасности необходимо учесть специфику законодательства страны, где осуществляет деятельность организация. для этого необходимо привлечение юристов, владеющих вопросами права в области информационных технологий, телекоммуникаций и информационной безопасности. Юристы, специализирующиеся в области информационной безопасности и имеющие соответствующий опыт работы могут быть только в организации, предоставляющей консалтинговые услуги по информационной безопасности.

Определение должностных обязанностей и ответственности за обеспечение информационной безопасности руководителей и сотрудников организации, в том числе, за предоставление отчетности об инцидентах по информационной безопасности, позволяет установить персональную ответственность за участки работ, снизить вероятность халатного отношения к вопросам защиты информации.

Организационно-распорядительные документы, издаваемые при формировании политики информационной безопасности, позволяют юридически закрепить порядок обеспечения информационной безопасности и регламентировать порядок защиты информации.

**4. Жизненный цикл политики безопасности**

Разработка политики безопасности — длительный и трудоемкий процесс, требующий профессионализма, отличного знания нормативной базы в области безопасности. Этот процесс обычно занимает многие месяцы и не всегда завершается успешно. Координатором этого процесса является специалист, на которого руководство организации возлагает ответственность за обеспечение информационной безопасности компьютерных систем. Эта ответственность обычно концентрируется на руководителе отдела информационной безопасности, директоре по безопасности или на руководителе отдела внутреннего аудита. Именно он координирует деятельность рабочей группы по разработке и внедрению политики безопасности на протяжении всего жизненного цикла, который состоит из пяти последовательных этапов:

1. Первоначальный аудит безопасности. Аудит безопасности — процесс, которого начинаются любые планомерные действия по обеспечению информационной безопасности в организации. Он включает в себя проведение обследования, идентификацию угроз безопасности, ресурсов, нуждающихся в защите и оценку рисков. В ходе аудита производится анализ текущего состояния информационной безопасности, выявляются существующие уязвимости, наиболее критичные области функционирования и самые чувствительные к угрозам безопасности бизнес процессы.

2. Разработка. Аудит безопасности позволяет собрать и обобщить сведения, необходимые для разработки политики безопасности. На основании результатов аудита определяются основные условия, требования и базовая система мер по обеспечению информационной безопасности в организации, позволяющих уменьшить риски до приемлемой величины, которые оформляются в виде согласованных в рамках рабочей группы решений и утверждаются руководством организации. Разработка политики безопасности с нуля не всегда является хорошей идеей. Во многих случаях можно воспользоваться существующими наработками, ограничившись адаптацией типового комплекта к специфическим условиям своей организации. Этот путь позволяет сэкономить месяцы работы и повысить качество разрабатываемых документов. Кроме того, он является единственно приемлемым в случае отсутствия в организации собственных ресурсов для квалифицированной разработки политики бёзопасности.

3. Внедрение. С наибольшими трудностями приходится сталкиваться на этапе внедрения политики безопасности, которое, как правило, связано с необходимостью решения технических, организационных и дисциплинарных проблем. Часть пользователей могут сознательно либо бессознательно сопротивляться введению новых правил поведения, которым теперь необходимо следовать, а также программно-технических механизмов защиты информации, в той или иной степени неизбежно ограничивающих их свободный доступ к информации. Системных администраторов может раздражать необходимость выполнения требований политик безопасности, усложняющих задачи администрирования. Помимо этого могут возникать и чисто технические проблемы, связанные, например, с отсутствием в используемых программных средствах функций, необходимых для реализации отдельных положений политики безопасности. На этапе внедрения необходимо не просто довести содержание политики до сведения всех сотрудников организации, но также обучить и дать необходимые разъяснения сомневающимся, которые пытаются обойти новые правила и продолжать работать по-старому. Для успешного завершения внедрения должна быть создана специальная проектная группа, действующая по согласованному плану.

4. Аудит и контроль. Соблюдение положений политики безопасности обязательно для всех сотрудников организации и должно непрерывно контролироваться. Проведение планового аудита безопасности является одним из основных методов контроля работоспособности политики безопасности, позволяющего оценить эффективность внедрения. Результаты аудита могут служить основанием для пересмотра некоторых положений политики и внесения в них необходимых корректировок.

5. Пересмотр и корректировка. Первая версия политики безопасности обычно не в полной мере отвечает потребностям организации, однако понимание этого приходит с опытом. Скорее всего, после наблюдения за процессом внедрения и оценки эффективности ее применения потребуется осуществить ряд доработок. В дополнение к этому, используемые технологии и организация бизнес-процессов непрерывно изменяются, что приводит к необходимости корректировать существующие подходы к обеспечению информационной безопасности. Как правило, ежегодный пересмотр политики безопасности — норма, которая устанавливается самой политикой.

**5. Принципы политики безопасности**

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

— невозможность миновать защитные средства;

— усиление самого слабого звена;

— невозможность перехода в небезопасное состояние;

— минимизация привилегий;

— разделение обязанностей;

— эшелонированность обороны;

— разнообразие защитных средств;

— простота и управляемость информационной системы;

— обеспечение всеобщей поддержки мер безопасности.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Применительно к межсетевым экранам данный принцип означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через экран. Не должно быть «тайных» модемных входов или тестовых линий, идущих в обход экрана.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией — управление доступом и, как последний рубеж, протоколирование и аудит. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками.

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (скажем, таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудно управляемой.

Последний принцип — всеобщая поддержка мер безопасности — носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать, заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Анализ рисков — важнейший этап выработки политики безопасности. При оценке рисков, которым подвержены Intranet - системы, нужно учитывать следующие обстоятельства: новые угрозы по отношению к старым сервисам, вытекающие из Возможности пассивного или активного прослушивания сети (пассивное прослушивание означает чтение сетевого трафика, а активное — его изменение (кражу, дублирование или модификацию передаваемых данных): например, аутентификация удаленного клиента с помощью пароля многократного использования не может считаться надежной в сетевой среде, независимо от длины пароля); новые (сетевые) сервисы и ассоциированные с ними угрозы.

Как правило, в Intranet -системах следует придерживаться принципа «все, что не разрешено, запрещено», поскольку «лишний» сетевой сервис может предоставить канал проникновения в корпоративную систему. В принципе, ту же мысль выражает положение «все непонятное опасно».