Профессиональное образовательное частное учреждение среднего профессионального образования
«Высший юридический колледж: экономика, финансы, служба безопасности»
Пушкинская ул., д. 268, 426008, г. Ижевск. Тел.: (3412) 32-02-32. Тел./факс: 43-62-22. E-mail:mveu@mveu.ru, mveu.ru

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

к выполнению практических работ

при изучении учебной дисциплины

ОП.11 Основы информационной безопасности

для специальности

09.02.03 Программирование в компьютерных системах

Ижевск, 2020 г.

Практическая работа – небольшой научный отчет, обобщающий проведенную учащимся работу, которую представляют для защиты преподавателю.

В процессе практического занятия учащиеся выполняют одну или несколько практических работ (заданий) под руководством преподавателя в соответствии с изучаемым содержанием учебного материала.

Ведущей дидактической целью практических занятий является формирование практических умений - профессиональных (умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности) или учебных (умений решать задачи по математике, физике, химии, информатике и др.), необходимых в последующей учебной деятельности по общепрофессиональным и специальным дисциплинам; практические занятия занимают преимущественное место при изучении общепрофессиональных и специальных дисциплин. Состав и содержание практических занятий направлены на реализацию Государственных требований.

На практических занятиях учащиеся овладевают первоначальными профессиональными умениями и навыками, которые в дальнейшем закрепляются и совершенствуются в процессе курсового проектирования и производственной (преддипломной) практики.

Наряду с формированием умений и навыков в процессе практических занятий обобщаются, систематизируются, углубляются и конкретизируются теоретические знания, вырабатывается способность и готовность использовать теоретические знания на практике, развиваются интеллектуальные умения.

К практическим работам предъявляется ряд требований, основным из которых является полное, исчерпывающее описание всей проделанной работы, позволяющее судить о полученных результатах, степени выполнения заданий и профессиональной подготовке учащихся.

Практические работы:

Тема практической работы №1. Уточнение задач информационной безопасности организации.

Объем часов 2

Цель практической работы. Изучить задачи информационной безопасности организации.

Безопасность для предприятия является залогом продуктивной деятельности и процветания. Такое состояние способствует тому, что все сотрудники направляют силы на достижения новых результатов. Однако любой бизнес может подвергаться различным опасностям, таким как:

- утечка конфиденциальной информации;
- финансовые потери или банкротство;
- опасность потерять ценных сотрудников;
- опасность хищения денежных средств или ценных объектов;
- опасность для здоровья и жизни персонала.

Последние два пункта особенно беспокоят множество предпринимателей. Техническая безопасность предприятия — одна из наиболее актуальных тем, когда речь идет об устранении угроз и обеспечении условий для спокойной и эффективной работы. Больше остальных в технической защите нуждаются предприятия, где велик поток посетителей и сосредоточены ценные предметы или значительная сумма денег:

- ювелирные магазины;
- банковские отделения;
- музеи.

К техническим средствам безопасности следует отнести такие меры, которые направлены на контроль и видеонаблюдение за посетителями и на физическую защиту персонала и ценных объектов (денежных средств, музейных экспонатов).

Системы видеонаблюдения и квалифицированные охранники — первостепенная необходимость на предприятии. Эффективным способом защиты имущества и обеспечения безопасности персонала является пультовая охрана с установлением тревожной кнопки.

Когда речь идет об охране, важно не просто ее наличие – необходимо привлекать профессионалов, которые справятся с самыми дерзкими и подготовленными преступлениями злоумышленников.

Различают пассивные и активные технические средства безопасности. В первом случае меры применяются для предупреждения угрозы (видеонаблюдение, решетки на окнах, сигнализация). Активные меры направлены на задержание и нейтрализацию преступника.

Тема практической работы №2. Изучение источников, рисков и форм атак на информации.

Объем часов 2/1

Цель практической работы. Изучить источники, риски и формы атак на информацию.

Существует следующие формы атак:

1. По природе возникновения.

1.1. Естественные угрозы - угрозы, вызванные воздействиями на автоматизированную систему и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.

1.2. Искусственные угрозы - угрозы информационной безопасности автоматизированной системы, исходящие от человека.

2. По степени преднамеренности проявления.

2.1. Угрозы случайного действия или угрозы, вызванные ошибками халатностью персонала.

2.2. Угрозы преднамеренного действия (например, угрозы действий злоумышлиника)

3. По непосредственному источнику угроз.

3.1. Угрозы, непосредственным источником которых является природная среда

3.2. Угрозы, непосредственным источником которых является человек

3.3. Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства

3.4. Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства

4. По положению источника угроз.

4.1. Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС.

4.2. Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС.

4.3. Угрозы, источник которых имеет доступ к периферийным устройствам АС (терминалам).

4.4. Угрозы, источник которых расположен в АС.

5. По степени зависимости от активности АС.

5.1. Угрозы, которые могут проявляться в независимо от активности АС.

5.2. Угрозы, которые могут проявляться только в процессе функционировния автоматизированной обработки данных (например, угрозы выполнения и распространения программных вирусов)..

6. По степени воздействия на АС.

6.1. Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС

6.2. Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС

7. По этапам доступа пользователей или программ к ресурсам АС.
7.1. Угрозы, которые могут проявляться на этапе доступа к ресурсам АС
7.2. Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС
8. По способу доступа к ресурсам АС.
8.1. Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС.
8.2. Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС.
9. По текущему месту расположения информации, хранимой и обрабатываемой в АС.
9.1. Угрозы доступа к информации на внешних запоминающих устройствах
9.2 Угрозы доступа к информации в оперативной памяти.
9.3. Угрозы доступа к информации, циркулирующей в линиях связи.
9.4. Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере (например, угроза записи отображаемой информации на скрытую видеокамеру).

Тема практической работы №3. Изучение источников, рисков и форм атак на информацию в АСОИУ.

Объем часов 2

Цель практической работы. Изучить источники, рисков и форм атак на информацию в АСОИУ.

Безопасность информации – степень (мера) защищенности информации, хранимой и обрабатываемой в автоматизированной системе (АС), от неактивного воздействия на нее с точки зрения нарушения ее физической и логической целостности (уничтожения, искажения) или несанкционированного использования.

Автоматизированная система– организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации в процессе решения определенного круга прикладных задач.

Защищенность информации– поддержание на заданном уровне тех параметров информации, находящейся в автоматизированной системе, которые обеспечивают установленный статус ее хранения, обработки и использования.

Защита информации (ЗИ)– процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус ее защищенности.

Комплексная защита информации– целенаправленное регулярное применение в автоматизированных системах средств и методов защиты информации, а также осуществление комплекса мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся существенно значимыми с точки зрения обеспечения безопасности информации.

Безопасная информационная система– это система, которая, во-первых, защищает данные от несанкционированного доступа, во-вторых, всегда готова предоставить их своим пользователям, в-третьих, надежно хранит информацию и гарантирует неизменность данных. Таким образом, безопасная система по определению обладает свойствами конфиденциальности, доступности и целостности.

Конфиденциальность– гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).

Доступность– гарантия того, что авторизованные пользователи всегда получат доступ к данным.

Целостность – гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Требования безопасности могут меняться в зависимости от назначения системы, характера используемых данных и типа возможных угроз. Трудно представить систему, для которой были бы не важны свойства целостности и доступности, но свойство конфиденциальности не всегда является обязательным.

Понятия конфиденциальности, доступности и целостности могут быть определены не только по отношению к информации, но и к другим ресурсам вычислительной сети, например внешним устройствам или приложениям. Существует множество системных ресурсов, возможность «незаконного» использования которых может привести к нарушению безопасности системы. Например, неограниченный доступ к устройству печати позволяет злоумышленнику получать копии распечатываемых документов, изменять параметры настройки, что может привести к изменению очередности работ и даже к выводу устройства из строя. Свойство конфиденциальности, примененное к устройству печати, можно интерпретировать так: доступ к устройству имеют те и только те пользователи, которым этот доступ разрешен, причем они могут выполнять только те операции с устройством, которые для них определены. Свойство доступности устройства означает его готовность к

использованию всякий раз, когда в этом возникает необходимость, а свойство целостности может быть определено как свойство неизменности параметров настройки данного устройства.

Важным для понимания дальнейших определений являются такие понятия, как объект, субъект, доступ.

Объект– пассивный компонент системы, хранящий, принимающий или передающий информацию.

Субъект – активный компонент системы, обычно представленный в виде пользователя, процесса или устройства, которому может потребоваться обращение к объекту или системе.

Доступ – взаимодействие между субъектом и объектом, обеспечивающее передачу информации между ними, или изменение состояния системы.

Доступ к информации– обеспечение субъекту возможности ознакомления с информацией и ее обработки, в частности, копирования, модификации или уничтожения информации.

Идентификация– присвоение субъектам и объектам доступа уникального идентификатора в виде номера, шифра, кода и т.п. с целью получения доступа к информации.

Аутентификация – проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы.

Угроза – любое действие, направленное на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов информационной системы (ИС).

Уязвимость информации– возможность возникновения на каком-либо этапе жизненного цикла автоматизированной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

Атака– реализованная угроза.

Риск– это вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки. Значение риска тем выше, чем более уязвимой является существующая система безопасности и чем выше вероятность реализации атаки.

Изначально защищенная информационная технология – информационная технология, которая изначально содержит все необходимые механизмы для обеспечения требуемого уровня защиты информации.

Качество информации– совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением.

Тема практической работы №4. Классификация рисков и основные задачи обеспечения безопасности информации в АСОИУ.

Объем часов 2/1

Цель практической работы. Изучить классификацию рисков и основные задачи обеспечения безопасности информации в АСОИУ.

Использование информационных систем и технологий связано с определенной совокупностью рисков. Оценка рисков необходима для контроля эффективности деятельности в области информационной безопасности, принятия целесообразных защитных мер и построения эффективных экономически обоснованных систем защиты. Основу риска образуют возможные уязвимости и угрозы для организации, поэтому выявление потенциальных или реально существующих рисков нарушения конфиденциальности и целостности информации, распространения вредоносного программного обеспечения и финансового мошенничества, классификация угроз информационной безопасности является одной из первичных задач по защите веб-приложения.

Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность. Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл информационной системы. Тогда эффект оказывается наибольшим, а затраты — минимальными. Можно выделить основные этапы жизненного цикла информационной системы:

- инициация, согласно бизнес-процессам компании;
- установка;
- эксплуатация;
- выведение из эксплуатации.

Информационная система и её составляющие

Первым шагом в процессе оценки рисков является определение объекта оценки, то есть границ анализируемой информационной системы, а также ресурсов и информации, образующих ИС. О системе необходимо собрать следующую информацию:

- архитектура ИС;
- используемое аппаратное обеспечение;
- используемое программное обеспечение;
- системные интерфейсы (внутренняя и внешняя связность);
- топология сети;
- присутствующие в системе данные и информация;
- поддерживающий персонал и пользователи;
- миссия системы (то есть процессы, выполняемые ИС);
- критичность системы и данных;

- чувствительность (то есть требуемый уровень защищенности) системы и данных.

Действия: оценка технического задания функционала системы и её фактических составляющих.

Управление рисками

Управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- регламентную оценку рисков;
- выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения уязвимости);
- уменьшение риска (например, за счет использования дополнительных защитных средств или действий);
- принятие риска (и выработка плана действия в соответствующих условиях).

Управление рисками можно подразделить на следующие этапы:

- инвентаризация анализируемых объектов;
- выбор методики оценки рисков;
- идентификация активов;
- анализ угроз и их последствий;
- определение уязвимостей в защите;
- оценка рисков;
- выбор защитных мер;
- реализация и проверка выбранных мер;
- оценка остаточного риска.

Для определения основных рисков можно следовать следующей цепочке: **источник угрозы > фактор (уязвимость) > угроза (действие) > последствия (атака)**.

- Источник угрозы — это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.
- Угроза (действие) — это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.
- Фактор (уязвимость) — это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и

интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

- Последствия (атака) — это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).

Действия: внедрение политики информационной безопасности компании.Источник угрозы

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Методы противодействия напрямую зависят от организаторов защиты информации.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Или, простыми словами — это либо хакер-злоумышленник или их группа, либо персонал компании, мотивированный теми или иными факторами на противоправные или противозаконные деяния. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

- криминальные структуры;
- потенциальные преступники и хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков телематических услуг;
- представители надзорных организаций и аварийных служб;
- представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

- основной персонал (пользователи, программисты, разработчики);
- представители службы защиты информации.

Действия: составление вероятностной шкалы источников угроз. Анализ угроз

Основным источником угроз информационной безопасности веб-приложения являются внешние нарушители.

Внешний нарушитель – лицо, мотивированное, как правило, коммерческим интересом, имеющее возможность доступа к сайту компании, не обладающий знаниями об исследуемой информационной системе, имеющий высокую квалификацию в вопросах обеспечения сетевой безопасности и большой опыт в реализации сетевых атак на

различные типы информационных систем.
Исходя из этого нам необходимо провести мероприятия по выявлению максимально возможного количества уязвимостей для уменьшения потенциальной площади поверхности атаки. Для этого необходимо провести процедуры идентификации технических уязвимостей. Они могут быть как разовыми, так и регламентными и затрагивать различные объекты инфраструктуры.
В контексте веб-приложения они могут быть разделены на следующие этапы:

- Поиск уязвимостей серверных компонентов;
- Поиск уязвимостей в веб-окружении сервера;
- Проверки ресурса на возможность открытого получения конфиденциальной и секретной информации;
- Подбор паролей.

Действия: составление регламента работ по идентификации уязвимостей, патч-менеджмента.

Идентификация технических уязвимостей

Идентификация технических уязвимостей производится для внешнего и внутреннего периметра корпоративной сети. Внешний периметр – это совокупность всех точек входа в сеть. К внутреннему периметру относятся хосты и приложения, доступные изнутри.
Традиционно используются два основных метода тестирования:

- тестирование по методу «черного ящика»;
- тестирование по методу «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак и проверяется устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмитируют действия потенциальных злоумышленников, пытающихся взломать систему защиты.
Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяется наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности. Выводы о наличии уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяются на практике.
Также, существует метод тестирования под названием «серый ящик», который комбинирует вышеописанные методы, когда известна частичная информация об объекте тестирования.
Отдельным пунктом исследования стоит возможность инфраструктуры работать на пиковых нагрузках и противостоять большому объему «мусорного трафика», генерируемого злоумышленниками или вредоносными программами.
Для исследования времени отклика системы на высоких или пиковых нагрузках

производится «стресс-тестирование», при котором создаваемая на систему нагрузка превышает нормальные сценарии её использования. Основная цель нагрузочного тестирования заключается в том, чтобы, создав определённую ожидаемую в системе нагрузку (например, посредством виртуальных пользователей) наблюдать за показателями производительности системы.

Действия: аудит информационной безопасности, в том числе и регламентный (например, согласно требованиям PCI DSS).

Обработка рисков

При объединении ценности активов с угрозами и уязвимостями необходимо рассмотреть возможность создания комбинацией угроза/уязвимость проблем для конфиденциальности, целостности и/или доступности этих активов. В зависимости от результатов этих рассмотрений должны быть выбраны подходящие значения ценности активов, т.е. значения, которые выражают последствия нарушения конфиденциальности, или целостности, или доступности.

Использование этого метода может привести к рассмотрению одного, двух или трех рисков для одного актива, в зависимости от конкретной рассматриваемой комбинации угроза/уязвимость.

При определении актуальных угроз, экспертно-аналитическим методом определяются объекты защиты, подверженные воздействию той или иной угрозы, характерные источники этих угроз и уязвимости, способствующие реализации угроз.

На основании анализа составляется матрица взаимосвязи источников угроз и уязвимостей из которой определяются возможные последствия реализации угроз (атаки) и вычисляется коэффициент опасности этих атак как произведение коэффициентов опасности соответствующих угроз и источников угроз, определенных ранее. При этом предполагается, что атаки, имеющие коэффициент опасности менее 0,1 (предположение экспертов), в дальнейшем могут не рассматриваться из-за малой вероятности их совершения на рассматриваемом объекте.

Действия: compliance management, консолидация и контроль соответствия требованиям ИТ и ИБ политик.

Нейтрализация и контрмеры

Нейтрализация рисков включает определение приоритетов, оценку и реализацию контрмер, уменьшающих риски и рекомендованных по результатам оценки рисков. Поскольку полное устранение рисков невозможно, руководство организации должно следовать принципу минимальной достаточности, реализуя только необходимые, наиболее подходящие регуляторы безопасности с целью уменьшения рисков до приемлемого уровня с минимальным негативным воздействием на бюджет, ресурсы и миссию организации.

Необходимым элементом управления рисками является оценка экономической эффективности, цель которой — продемонстрировать, что затраты на реализацию дополнительных контрмер окупаются за счет снижения рисков. При вычислении затрат на реализацию регуляторов безопасности следует учитывать:

- затраты на приобретение аппаратного и программного обеспечения;

- снижение эксплуатационной эффективности ИС, если производительность или функциональность системы падает в результате усиления мер безопасности;
- затраты на разработку и реализацию дополнительных политик и процедур;
- дополнительные затраты на персонал, вовлеченный в реализацию предложенных регуляторов безопасности;
- затраты на обучение персонала;
- затраты на сопровождение.

В качестве мер обеспечения могут быть внедрены следующие решения (как по отдельности, так и в совокупности), подготовленными штатными специалистами и/или с помощью аутсорсинга информационной безопасности:

- Системы защиты от атак на прикладном уровне (WAF);
- Системы управления инцидентами и событиями ИБ (SIEM);
- Системы управления соответствием требованиям ИБ (Compliance Management);
- Системы управления идентификационными данными и доступом (IAM);
- Системы однократной и многофакторной аутентификации в корпоративных сетях;
- Системы защиты от утечки конфиденциальной информации (DLP);
- Системы управления доступом к информации (IRM);
- Инфраструктуры открытых ключей (PKI);
- Решения по сетевой безопасности;
- Системы антивирусной защиты;
- Системы защиты электронной почты от спама, вирусов и других угроз;
- Системы контентной фильтрации web-трафика;
- Системы контроля доступа к периферийным устройствам и приложениям;
- Системы контроля целостности программных сред;
- Системы криптографической защиты при хранении информации.

Тема практической работы №5. Изучение Российского законодательства по защите информационных технологий.

Объем часов 2/1

Цель практической работы. Изучить Российское законодательство по защите информационных технологий.

Закон "Об информации, информационных технологиях и о защите информации"

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ (принят Государственной Думой 8 июля 2006 года). В нем даются основные определения, намечаются направления, в которых должно развиваться законодательство в данной области, регулируются отношения, возникающие при:

1. осуществлении права на поиск, получение, передачу, производство и распространение информации;
2. применении информационных технологий;
3. обеспечении защиты информации.

Процитируем основные определения:

1. **информация** - сведения (сообщения, данные) независимо от формы их представления;
2. **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
3. **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
4. **информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
5. **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
6. **доступ к информации** - возможность получения информации и ее использования;
7. **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
8. **предоставление информации** - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9. **распространение информации** - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10. **электронное сообщение** - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11. **документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

12. **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Мы, разумеется, не будем обсуждать *качество данных* в Законе определений. Обратим лишь внимание на нетрадиционность определения конфиденциальности информации, приравнивающего конфиденциальность к неразглашению.

В статье 3 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2. установление ограничений доступа к информации только федеральными законами;

3. открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4. равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5. обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6. достоверность информации и своевременность ее предоставления;

7. неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8. недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Отметим, что в этих принципах явным образом фигурируют целостность (достоверность) и доступность (своевременность предоставления) информации.

В статье 9 Закона содержатся следующие положения:

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав

и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

3. Защита информации, составляющей *государственную тайну*, осуществляется в соответствии с законодательством Российской Федерации о*государственной тайне*.

4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим *коммерческую тайну*, *служебную тайну* и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Отметим, что в этой статье упор делается на конфиденциальность информации.

Статья 11 "Документирование информации" содержит следующие важные положения:

3. Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

4. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

Статья 16 целиком посвящена вопросам защиты информации. Процитируем ее полностью.

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2. соблюдение конфиденциальности *информации ограниченного доступа*;

3. реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1. предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2. своевременное обнаружение фактов несанкционированного доступа к информации;

3. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5. возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6. постоянный контроль за обеспечением уровня защищенности информации.

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

В процитированной статье Закона фигурируют все три основных аспекта информационной безопасности: доступность, целостность и конфиденциальность. Кроме того, обязательным является отслеживание нарушений безопасности и постоянный контроль за обеспечением уровня защищенности информации.

Явным образом не упомянуты такие меры, как аккредитация, сертификация и лицензирование, но в пунктах 5 и 6 они, конечно, подразумеваются.

Таковы важнейшие, на наш взгляд, положения Закона "Об информации, информационных технологиях и о защите информации". На следующей странице будут рассмотрены другие законы РФ в области информационной безопасности.

Тема практической работы №6. Изучение нормативно-правовой информации.

Объем часов 2

Цель практической работы. Изучить нормативно-правовую информацию.

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из Федерального закона «Об информации, информационных технологиях и о защите информации» и других регулирующих отношения по использованию информации федеральных законов.

Правовым фундаментом, регулирующим в Российской Федерации отношения в области информации, являются федеральные законы, направленные, на обеспечение защиты.

Становление информационного законодательства является одной из важнейших задач государственной политики в области информационных технологий и основным способом в решении проблем правового обеспечения информационного общества на национальном уровне.

Правовая основа единого информационного пространства призвана регулировать отношения производителей и потребителей информации, обеспечивать координацию действий органов государственной власти в едином информационном пространстве и гарантировать соблюдение конституционных прав и свобод граждан и организаций.

Федеральным Законом от 27 июля 2006 года №149-ФЗ (в ред. Федерального закона от 02.07.2013 года №187-ФЗ) «Об информации, информационных технологиях и защите информации» в статье 12 провозглашен принцип государственного регулирования в сфере применения информационных технологий.

Статьей 15 Федерального закона «Об информации, информационных технологиях и о защите информации» регламентируется использование информационно-телекоммуникационных сетей. В частности, на территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, Федерального закона «Об информации, информационных технологиях и о защите информации» и иных нормативных правовых актов Российской Федерации.

Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных федеральным законодательством.

Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть

ограничена только в порядке и на условиях, которые установлены федеральными законами.

Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

В настоящее время сложились благоприятные условия для совершенствования системы государственного управления, повышения качества предоставления государственных услуг населению и организациям, повышения результативности и прозрачности работы государственного аппарата, последовательного искоренения коррупции на основе широкого применения информационных технологий в деятельности федеральных органов государственной власти.

В целях повышения эффективности управления процессом использования информационных технологий в деятельности федеральных органов государственной власти осуществляется мониторинг использования информационных технологий, в рамках которого обеспечивается контроль эффективности выполнения государственных программ и проектов, проводится анализ текущих и перспективных потребностей в информационных технологиях, формируются предложения по корректировке государственной политики в сфере информационных технологий.

Целью нормативного правового регулирования в сфере использования информационных технологий в деятельности федеральных органов государственной власти является создание эффективной правовой основы для реализации прав граждан, защиты общественных и государственных интересов в сфере использования информационных технологий.

Тема практической работы №7. Изучение симметричных и ассиметричных криптосистем для защиты компьютерной информации в АСОИУ.

Объем часов 2/1

Цель практической работы. Изучить симметричные и ассиметричные криптосистемы.

Симметричные криптосистемы

Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, в основном используется для обеспечения конфиденциальности данных.

Весьма упрощенным примером алгоритма секретного ключа является так называемый шифр Цезаря. Ключом в этом примере являются три буквы.

Совершенно ясно, что если кто-нибудь получит зашифрованное этим способом сообщение и будет знать алгоритм (куда сдвигать буквы – вверх или вниз по алфавиту), он сможет легко раскрыть ключ методом простого перебора, который заключается в том, что человек перебирает все возможные комбинации алгоритма до тех пор, пока не получит в результате расшифрованный текст. **Обычно, чем длиннее ключ и чем сложнее алгоритм, тем труднее решить задачу расшифровки простым перебором вариантов.**

Сегодня широко используются такие алгоритмы секретных ключей, как Data Encryption Standard (DES), 3DES (или «тройной DES») и International Data Encryption Algorithm (IDEA).

Эти алгоритмы шифруют сообщения блоками по 64 бита. Если объем сообщения превышает 64 бита (как это обычно и бывает), необходимо разбить его на блоки по 64 бита в каждом, а затем каким-то образом свести их воедино.

В настоящее время все чаще говорят о неоправданной сложности и невысокой криптостойкости. На практике приходится использовать его модификации.

Более эффективным является отечественный стандарт шифрования данных ГОСТ 28147-89. Он рекомендован к использованию для защиты любых данных, представленных в виде двоичного кода, хотя не исключаются и другие методы шифрования.

Данный стандарт формировался с учетом мирового опыта, и в частности, были приняты во внимание недостатки и нереализованные возможности алгоритма DES, поэтому использование стандарта ГОСТ предпочтительнее.

Шифрование с помощью секретного ключа чаще всего используется для поддержки конфиденциальности данных и очень эффективно реализуется с помощью неизменяемых «вшитых» программ (firmware).

Этот метод можно использовать для аутентификации и поддержания целостности данных, но метод цифровой подписи (о котором мы скажем позже) является более эффективным.

С методом секретных ключей связаны следующие **проблемы**:

1. Необходимо часто менять секретные ключи, поскольку всегда существует риск их случайного раскрытия.

2. Трудно обеспечить безопасное генерирование и распространение секретных ключей.

3. Для получения и безопасного распространения секретных ключей обычно используется алгоритм Диффи-Хеллмана (Diffie-Hellman), который описывается ниже.

Асимметричные криптосистемы

Как бы ни были сложны и надежны криптографические системы - их слабое место при практической реализации - **проблема распределения ключей**. Для того, чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. Т.е. в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены асимметричные криптосистемы (системы с открытым ключом).

Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым (общим), а другой закрытым (частным, секретным). Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст, в принципе, не может быть расшифрован тем же открытым ключом. Дешифрование сообщение возможно только с использованием закрытого ключа, который известен только самому адресату.

Таким образом, асимметричное шифрование часто называют **шифрованием с помощью общего ключа**, при котором используются разные, но взаимно дополняющие друг друга ключи и алгоритмы шифрования и расшифровки.

Асимметричные системы для преобразования ключей (что нужно для необратимости процесса шифрования даже для отправителя сообщения) используют так называемые необратимые или односторонние функции (безопасные **хэш-функции),**которые обладают следующим свойством: при заданном значении x относительно просто вычислить значение f(x), однако если y=f(x), то нет простого пути для вычисления значения x.

Другими словами, безопасной хэш-функцией называется функция, которую легко рассчитать, но обратное восстановление которой требует непропорционально больших усилий. Входящее сообщение пропускается через математическую функцию (хэш-функцию), и в результате на выходе мы получаем некую последовательность битов. Эта последовательность называется «хэш» (или «результат обработки сообщения»). Этот процесс практически невозможно восстановить. Другими словами, имея выходные данные, невозможно получить входные.

Хэш-функцию можно сравнить с кофемолкой. Если сообщение – это кофейные зерна, а хэш на выходе – это размолотый кофе, то, имея такой размолотый кофе, вы не сможете восстановить кофейные зерна.

Хэш-функция принимает сообщение любой длины и выдает на выходе хэш фиксированной длины. Наиболее известные из хэш-функций (поддерживаемые современными операционными системами):

- алгоритм Message Digest 2 (MD2);
- алгоритм Message Digest 4 (MD4);
- алгоритм Message Digest 5 (MD5);
- алгоритм безопасного хэша (Secure Hash Algorithm – SHA).

Чтобы гарантировать надежную защиту информации, **к асимметричным системам** с открытым ключом (СОК) предъявляются**два важных и очевидных требования**:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.

2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Вообще же все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих **типов** необратимых преобразований:

1. Разложение больших чисел на простые множители.

2. Вычисление логарифма в конечном поле.

3. Вычисление корней алгебраических уравнений.

Здесь же следует отметить, что алгоритмы криптосистемы с открытым ключом (СОК) можно использовать **в трех назначениях**.

1. Как самостоятельные средства защиты передаваемых и хранимых данных, в целях обеспечения конфиденциальности данных.

2. Как средства для распределения ключей, обеспечивающее получение общих ключей для совместного использования. Алгоритмы СОК более трудоемки, чем традиционные криптосистемы. Поэтому часто на практике рационально с помощью СОК распределять ключи, объем которых как информации незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками.

3. Средства аутентификации пользователей.

Алгоритмы шифрования с помощью общих ключей редко используются для поддержки конфиденциальности данных из-за ограничений производительности.

Вместо этого их часто используют в приложениях, где аутентификация проводится с помощью цифровой подписи и управления ключами.

Среди наиболее известных алгоритмов общих ключей можно назвать RSA (разработан в 1977 году и получил название в честь его создателей: Рона Ривеста, Ади Шамира и Леонарда Эйдельмана и ElGamal.

Алгоритм RSA стал мировым стандартом де-факто для открытых систем и рекомендован МККТТ.

Разработчики алгоритма воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению. Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой СОК на фоне десятков других схем.

Тема практической работы №8. Изучение стандартных алгоритмов шифрования. Безопасность и быстродействие криптосистем.

Объем часов 2/1

Цель практической работы. Изучить страндартные алгоритмы шифрования.

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифровкой, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-расшифровки. В соответствии со стандартом ГОСТ 28147-89 под **шифром** понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

1. алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
2. алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
3. гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
4. аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифровки осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровке сообщений. В **асимметричных**криптосистемах для шифрования данных используется один (общедоступный) ключ, а для расшифровки – другой (секретный) ключ.

Симметричные криптосистемы

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам:

Н О Н С Б Н Я

Е Е О Я О Е Т

Я С В Е Л П Н

С Т И Щ Е О Ы

Н А Т Е Е Н М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово «ЛУНАТИК», получим следующую таблицу:

Л У Н А Т И К

А И К Л Н Т У

4	7	5	1	6	2	3
Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

1	2	3	4	5	6	7
С	Н	Я	Н	Н	Б	О
Я	Е	Т	Е	О	О	Е
Е	П	Н	Я	В	Л	С
Щ	О	Ы	С	И	Е	Т
Е	Н	М	Н	Т	Е	А

До перестановки После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка: СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА. Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке перестановки проводятся в обратном порядке. Например, сообщение “Приезжаю_шестого” можно зашифровать следующим образом:

2	4	1	3
4	П	Р	И	Е
1	З	Ж	А	Ю

1	2	3	4
4	И	П	Е	Р
1	А	З	Ю	Ж

1	2	3	4
1	А	З	Ю	Ж
2	Е	_	С	Ш

2 _ Ш Е С 2 Е. _ С Ш З Г Т О О

З Т О Г О З Г Т О О 4 И П Е Р

Двойная перестановка столбцов и строк
В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13		О	И	Р	Т
5	10	11	8		З	Ш	Е	Ю
9	6	7	12		_	Ж	А	С
4	15	14	1		Е	Г	О	П

П Р И Е З Ж А Ю _ Ш Е С Т О Г О

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5- 250000.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение: СОВЕРШЕННО СЕКРЕТНО

Ключ: 3143143143143143143

Шифровка: ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит):

АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_

АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_

_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ

Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ

ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ

ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ

БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

Гаммирование

Процесс шифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i=Г(ш)_i+Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифровки сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i=Г(ш)_i+Т(ш)_i$.

Асимметричные криптосистемы

Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем $P > G$.
2. Получатель выбирает секретный ключ - случайное целое число $X < P$.
3. Вычисляется открытый ключ $Y= G^x \bmod P$.
4. Получатель выбирает целое число K, 1< K< P-1.
5. Шифрование сообщения (M): $a= G^K \bmod P$, $b=Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Алгоритм создания открытого и секретного ключей:

1. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $n=p*q$ и функцию Эйлера $\varphi(n)=(p-1)(q-1)$.

2. Получатель выбирает целое число e ($1<e<\varphi(n)$), взаимно простое со значением функции $\varphi(n)$.

Пара чисел **(e,n)** публикуется в качестве **открытого ключа**.

3. Получатель вычисляет целое число d, которое отвечает условию: $e*d=1 \pmod{\varphi(n)}$.

Пара чисел **(d,n)** является **секретным ключом**. Шифрование сообщения с использованием открытого ключа:

Если m – сообщение (сообщениями являются целые числа в интервале от 0 до n-1), то зашифровать это сообщение можно как $\mathbf{c=m^e \bmod(n)}$.

Дешифрование сообщения с использованием секретного ключа:

Получатель расшифровывает, полученное сообщение c: $\mathbf{m=c^d \bmod (n)}$.

Тема практической работы №9. Изучение принципов идентификации и механизмов подтверждения подлинности пользователя.

Объем часов: 2

Цель практической работы. Изучить принципы идентификации и механизмов подтверждения подлинности пользователя.

Идентификация объекта - одна из функций подсистемы защиты. Эта функция выполняется в первую очередь, когда объект делает попытку войти в сеть. Если процедура идентификации завершается успешно, данный объект считается законным для данной сети.

Следующий шаг - **аутентификация объекта** (проверка подлинности объекта). Эта процедура устанавливает, является ли данный объект именно таким, каким он себя объявляет.

После того как объект идентифицирован и подтверждена его подлинность, можно установить сферу его действия и доступные ему ресурсы КС. Такую процедуру называют **предоставлением полномочий (авторизацией).**

Перечисленные три процедуры инициализации являются процедурами защиты и относятся к одному объекту КС.

При защите каналов передачи данных подтверждение подлинности (аутентификация) объектов означает взаимное установление подлинности объектов, связывающихся между собой по линиям связи. Процедура подтверждения подлинности выполняется обычно в начале сеанса в процессе установления соединения абонентов. (Термин "соединение" указывает на логическую связь (потенциально двустороннюю) между двумя объектами сети. Цель данной процедуры - обеспечить уверенность, что соединение установлено с законным объектом и вся информация дойдет до места назначения.

После того как соединение установлено, необходимо обеспечить выполнение требований защиты при обмене сообщениями:

(а) получатель должен быть уверен в подлинности источника данных;

(б) получатель должен быть уверен в подлинности передаваемых данных;

(в) отправитель должен быть уверен в доставке данных получателю;

(г) отправитель должен быть уверен в подлинности доставленных данных.

Для выполнения требований (а) и (б) средством защиты является **цифровая подпись**. Для выполнения требований (в) и (г) отправитель должен получить **уведомление о вручении** с помощью удостоверяющей почты (certified mail). Средством защиты в такой процедуре является цифровая подпись подтверждающего ответного сообщения, которое в свою очередь является доказательством пересылки исходного сообщения.

Если эти четыре требования реализованы в КС, то гарантируется защита данных при их передаче по каналу связи и обеспечивается функция защиты, называемая функцией подтверждения (неоспоримости) передачи. В этом случае отправитель не

может отрицать ни факта посылки сообщения, ни его содержания, а получатель не может отрицать ни факта получения сообщения, ни подлинности его содержания.

1.2 Идентификация и механизмы подтверждения подлинности пользователя

Прежде чем получить доступ к КС, пользователь должен идентифицировать себя, а затем средства защиты сети должны подтвердить подлинность этого пользователя, т.е. проверить, является ли данный пользователь действительно тем, за кого он себя выдает. Компоненты механизма защиты легальных пользователей размещены на рабочей ЭВМ, к которой подключен пользователь через его терминал (или каким-либо иным способом). Поэтому процедуры идентификации, подтверждения подлинности и наделения полномочиями выполняются в начале сеанса на местной рабочей ЭВМ.

Когда пользователь начинает работу в КС, используя терминал, система запрашивает его имя и идентификационный номер. В зависимости от ответов пользователя компьютерная система проводит его идентификацию. Затем система проверяет, является ли пользователь действительно тем, за кого он себя выдает. Для этого она запрашивает у пользователя пароль. Пароль - это лишь один из способов подтверждения подлинности пользователя.Перечислим возможные способы подтверждения подлинности.

- Предопределенная информация, находящаяся в распоряжении пользователя: пароль, персональный идентификационный номер, соглашение об использовании специальных закодированных фраз.
- Элементы аппаратного обеспечения, находящиеся в распоряжении пользователя: ключи, магнитные карточки, микросхемы и т.п.

- Характерные личные особенности пользователя: отпечатки пальцев, рисунок сетчатки глаза, тембр голоса и т.п.

- Характерные приемы и черты поведения пользователя в режиме реального времени: особенности динамики и стиль работы на клавиатуре, приемы работы с манипулятором и т.п.

- Навыки и знания пользователя, обусловленные образованием, культурой, обучением, воспитанием, привычками и т.п.

Применение пароля для подтверждения подлинности пользователя. Традиционно каждый законный пользователь компьютерной системы получает идентификационный номер и/или пароль. В начале сеанса работы на терминале пользователь указывает свой идентификационный номер (идентификатор пользователя) системе, которая затем запрашивает у пользователя пароль.

Простейший метод подтверждения подлинности с использованием пароля основан на сравнении представляемого пользователем пароля с исходным значением хранящимся в компьютерном центре. Поскольку пароль должен храниться в тайне, его следует шифровать перед пересылкой по незащищенному каналу. Если значения пользователя и системы совпадают, то пароль считается подлинным, а пользователь - законным.

Если кто-нибудь, не имеющий полномочий для входа в систему, узнает каким-либо образом пароль и идентификационный номер законного пользователя, он получит доступ в систему.

Иногда получатель не должен раскрывать исходную открытую форму пароля. В этом случае отправитель должен пересылать вместо открытой формы пароля отображение пароля, получаемое с использованием односторонней функции a(*) пароля. Это преобразование должно гарантировать невозможность раскрытия противником пароля по его отображению, так как противник наталкивается на неразрешимую числовую задачу.

Например, функция a(*) может быть определена следующим образом:

a(P)=Ep(ID),

где P - пароль отправителя;

ID - идентификатор отправителя;

Ep - процедура шифрования, выполняемая с использованием пароля P в качестве ключа.

Такие функции особенно удобны, если длина пароля и длина ключа одинаковы. В этом случае подтверждение подлинности с помощью пароля состоит из пересылки получателю отображения a(P) и сравнения его с предварительно вычисленным и хранимым эквивалентом a'(P).

На практике пароли состоят только из нескольких букв, чтобы дать возможность пользователям запомнить их. Короткие пароли уязвимы к атаке полного перебора всех вариантов. Для того чтобы предотвратить такую атаку, функцию a(P) определяют иначе, а именно:

$t(P)=E_{p \text{ xor } k}(ID)$,

где K и ID-соответственно ключ и идентификатор отправителя.

Очевидно,значение a(P) вычисляется заранее и хранится в виде a'(P) в идентификационной таблице у получателя. Подтверждение подлинности состоит из сравнения двух отображений пароля $a(P_A)$ и $a'(P_A)$ и признания пароля p_A, если эти отображения равны. Конечно, любой, кто получит доступ к идентификационной таблице, может незаконно изменить ее содержимое, не опасаясь, что эти действия будут обнаружены.

Тема практической работы №10. Правила формирования электронной цифровой подписи.

Объем часов 2/1

Цель практической работы. Изучить правила и порядок формирования электронной цифровой подписи.

1. Генерация закрытого ключа

Для генерации закрытого ключа выполните в ППО «СЭД» пункт меню Администрирование→Криптозащита→Генерация ключей ЭЦП и запроса на сертификацию. В открывшемся окне Генерация запроса на сертификат и закрытого ключа (см. **Рис.**), в поле Наименование абонента введите название владельца закрытого ключа; в поле Криптографическая библиотека определяется тип используемой СКЗИ (по умолчанию тип уже определён как Ms Crypto API 2.0, что соответствует криптосистеме КриптоПро CSP 2.0). В параметре Удаленный АРМ отображается наименование АРМ клиента СЭД (т. е. наименование вашей организации).

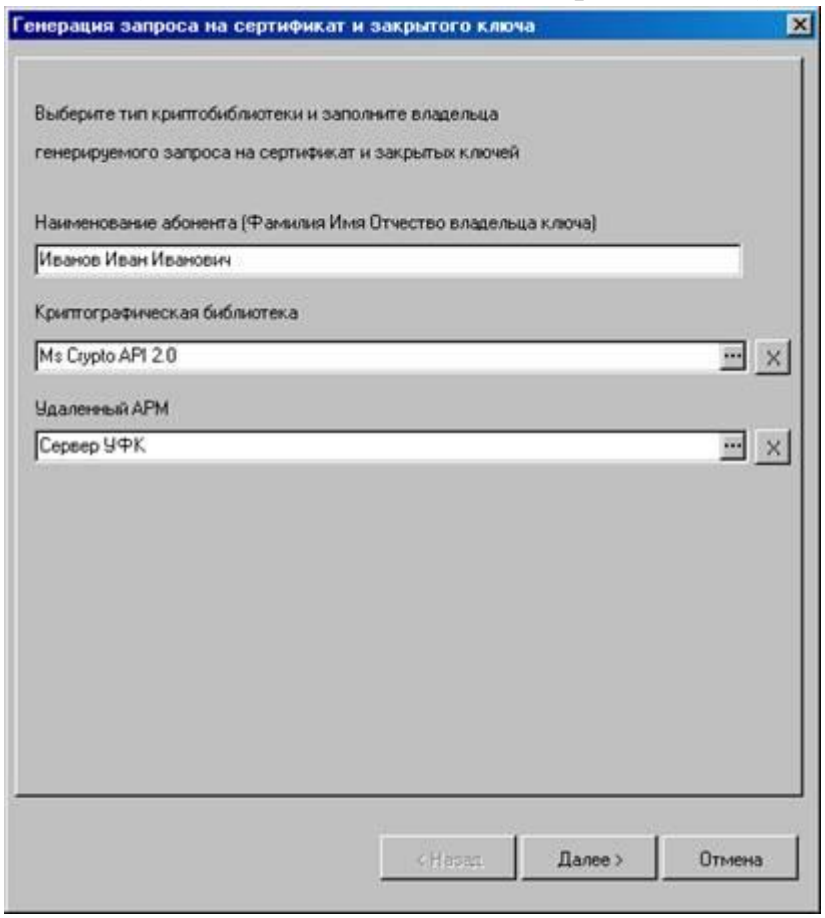


Рис. 1. Генерация запроса на сертификат и закрытого ключа

Убедитесь, что вся информация заполнена верно и нажмите кнопку **Далее>** для перехода на следующий шаг мастера(см. Рис. 2).

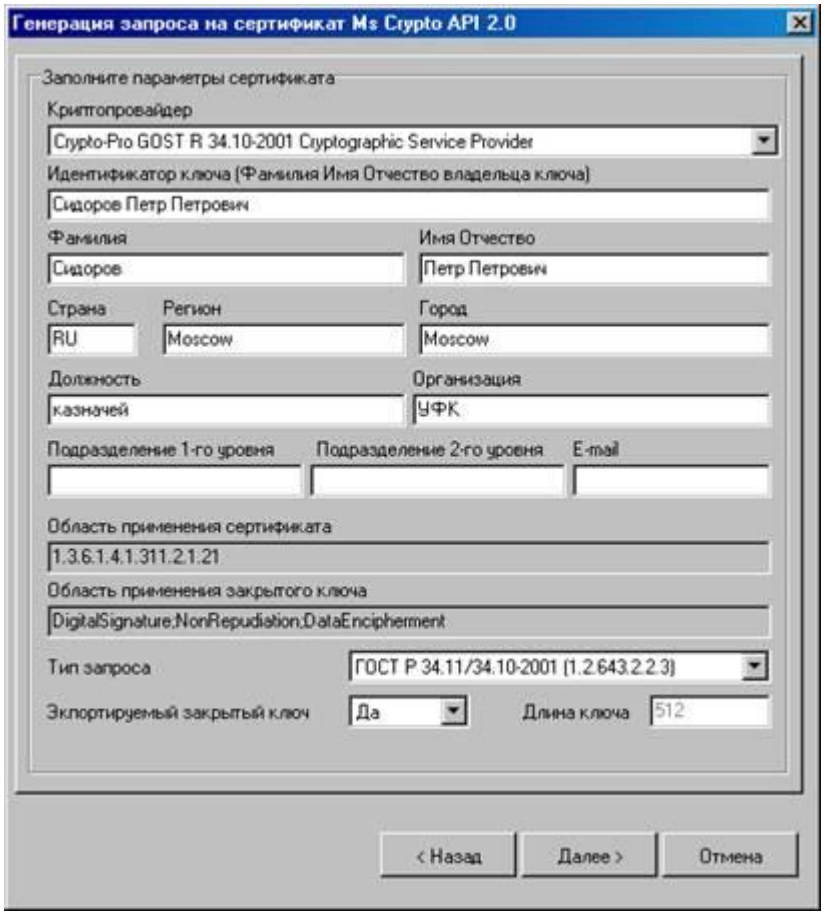


Рис. 2. Генерация запроса на сертификат Ms Crypto API 2.0

В появившемся окне введите значения:

1. Идентификатор ключа (Фамилия Имя Отчество владельца ключа) – вводится фамилия, имя, отчество лица, на которого генерируется закрытый ключ клиента СЭД.

2. Фамилия – заполняется фамилия ответственного лица (поле заполняется автоматически после ввода значение в поле Идентификатор ключа).

3. Имя Отчество – заполняется имя и отчество ответственного лица (поле заполняется автоматически после ввода значение в поле Идентификатор ключа).

4. Страна – заполняется идентификатором страны, в которой зарегистрирована организация (значение определено по умолчанию как RU).

5. Регион – заполняется значением субъекта Российской Федерации, в котором зарегистрирована организация (в нашем случае – **Кемеровская область**).

6. Город – заполняется наименованием города (населённого пункта), в котором зарегистрирована организация (в нашем случае – **Яя либо наименование населенного пункта Яйского района**).

7. Организация – заполняется официальным наименованием организации, в которой работает владелец ЭЦП (т. е. полное наименование вашей организации).

8. Должность – должность лица, на которого генерируется закрытый ключ клиента СЭД.

9. Подразделение 1-го уровня – в поле определяется наименование структурного подразделения (наименование отдела) 1-го уровня, к которому приписано ответственное лицо – владелец подписи (не обязательно для заполнения).

10. Подразделение 2-го уровня – в поле определяется наименование структурного подразделения (наименование группы) 2-го уровня, к которому приписано ответственное лицо – владелец подписи (не обязательно для заполнения).

11. E-mail – заполняется значением электронного адреса e-mail ответственного лица – владельца подписи (не обязательно для заполнения).

Проверив заполненную информацию, нажмите кнопку Далее>(см. Рис.).

В форме «Генерация запроса на сертификат Ms Crypto API 2.0» необходимо установить флаг в поле Распечатать заявку на получение сертификата ключа ЭЦП, так как только с данной распечатанной формой запрос на регистрацию ключей будет приниматься ТОФК. Запрошенный документ будет выведен в форму MS Word, который далее можно распечатать стандартными средствами MS Word.

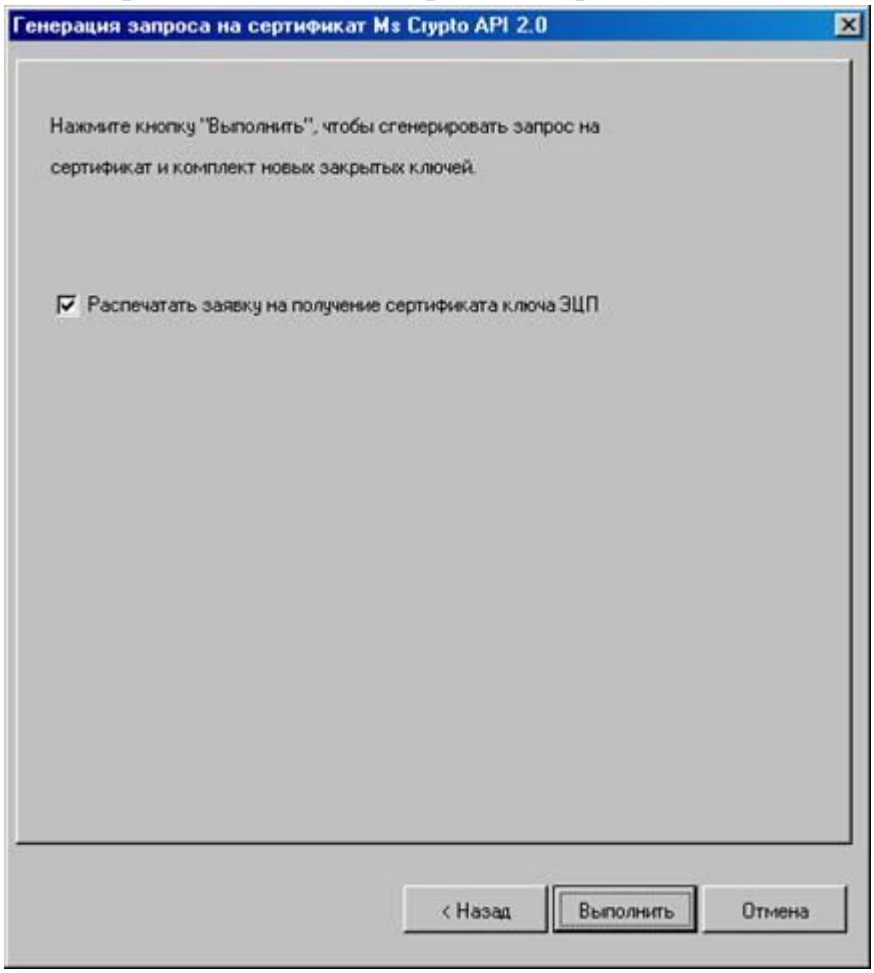
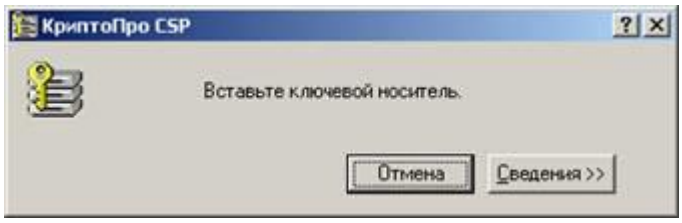


Рис. 3. Генерация запроса на сертификат

Для создания закрытого ключа и формирования запроса на сертификат нажмите кнопку Выполнить.

Внимание!

Если считыватель закрытого ключа у вас определён как дискета 3.5”, то перед нажатием кнопки Выполнить в дисковод необходимо вставить ключевую дискету, на которую будут записаны файлы закрытого ключа (желательно новую). В случае его отсутствия выведется следующее сообщение, и система будет пытаться обратиться к дисководу, пока не будет вставлена дискета.



Далее появится диалог датчика случайных чисел, формирующего комбинацию закрытого ключа. Выйдет окошко с просьбой нажимать клавиши или двигать мышью. Вводите символы до переключения на следующее окошко. Нужно ввести 10 символов (осторожно, не нажимайте лишнее!). Следующее окно - форма запроса пароля на сгенерированный ключ. Перед фразой «Установить новый пароль» в окошечке должна стоять точка.

Примечание: В случае определения пароля для закрытого ключа его ввод будет необходим перед каждой операцией обращения к функциям криптозащиты, если он не был сохранён в системе.

Когда закрытый ключ клиента СЭД будет сгенерирован (при этом на ключевом носителе будет создан контейнер с закрытым ключом, и в него будут помещены файлы закрытого ключа header. key, masks. key masks2.key name. key primary. key primary2.key), система автоматически сгенерирует запрос на сертификат – файл с расширением *.req и отобразит путь, куда он будет помещён (см. Рис.). (Запомните этот путь, чтобы найти этот файл).

Рис. 4. Директория сохранения нового ключа (в этом окне оставьте все без изменений)

После определения каталога с запросом на сертификат мастер генерации запроса на сертификат подтверждаем, нажав **Ok.** На экран будет выведена заявка на получение сертификата, которую нужно сохранить с именем файла, состоящим из фамилии лица – владельца ключа. Данную заявку требуется отредактировать, заверить печатью, подписать лицом, на которое генерировался ключ и руководителем учреждения (организации). Это и есть бумажная копия заявки.

Тема практической работы №11. Изучение средств защиты локальных сетей от несанкционированного доступа.

Объем часов 2

Цель практической работы. Изучить средства защиты локальных сетей от несанкционированного доступа.

Основным средством защиты сети Internet от несанкционированного доступа в настоящее время являются средства firewalls («огненные стены»). Они контролируют информационные потоки между локальными вычислительными сетями (ЛВС), причем уровень контроля определяется в первую очередь сферой интересов компании, структурой ЛВС и целями, ради которых она связана с Internet. В этом случае корпоративную сеть часто сравнивают с крепостью, окруженной глубоким рвом, через который перекинуты два моста. Караулы останавливают всех, кто входит и выходит из крепости, и проверяют пароль. Взломщики часто перехватывали пароль и получали право доступа к корпоративным сетям. Поэтому в настоящее время все чаще применяют одноразовые пароли и схемы проверки полномочий, исключающие использование злоумышленниками любой перехваченной информации.

Система Firewall обеспечивает защиту программного обеспечения сервера от доступа без соответствующей авторизации, но в то же время не препятствует нормальной работе ряда штатных служб (sendmail, ftp, www и так далее). Система Firewall является наиболее распространенным средством усиления традиционных средств защиты от несанкционированного доступа, используемого в семействе UNIX, и используется для обеспечения защиты данных при организации межсетевого взаимодействия. Конкретные реализации Firewall в значительной степени зависят от используемых вычислительных платформ, но тем не менее все системы этого класса используют два механизма, один из которых обеспечивает блокировку сетевого трафика, а второй, наоборот, разрешает обмен данными. При этом некоторые версии Firewall делают упор на блокировании нежелательного трафика, а другие – на регламентировании разрешенного межмашинного обмена.

Большинство организаций и центров обработки данных, использующих сетевые, технологии, к моменту появления Firewall уже имели сложившуюся систему обеспечения безопасности. И в большинстве случаев внедрение новой системы не внесло никаких изменений в традиционные подходы к защите данных. Поскольку основная проблема при работе с Internet состоит именно в обеспечении безопасности локальных данных, появление Firewall оказалось фактором, в значительной мере способствующим росту количества пользователей сети, что, в свою очередь, не замедлило сказаться на развитии и самой технологии защиты данных.

Кроме того, Firewall может использоваться в качестве корпоративной открытой части сети, видимой со стороны Internet. Во многих организациях Firewall-системы используются для хранения данных с открытым доступом, например, информации о продуктах и услугах, файлах из баз FTP, сообщений об ошибках и так далее. Отметим, что некоторые из подобных систем «двойного назначения», например,

uunet.uu.net или gatekeeper.dec.com, играют важную роль в «скелете» Internet и, по словам владельцев систем, справляются с возложенными на них задачами.

Как правило, Firewall предназначены для предотвращения несанкционированной регистрации в системе по телекоммуникационным сетям, то есть из «внешнего мира». Этого в большинстве случаев оказывается достаточно для предотвращения регистрации вандалов в системе или сети. Существуют и более мощные системы защиты, которые блокируют весь трафик, инициированный внешней частью сети, но дают возможность пользователям системы без каких-либо ограничений взаимодействовать с внешним миром, что позволяет, с точки зрения разработчиков, защититься от любой сетевой атаки.

Ряд Firewall-систем разрешает обмен только электронной почтой, что в еще большей степени ограничивает возможности злоумышленника по проникновению в систему. Но, вообще говоря, подобные меры используются исключительно редко, поскольку накладывают слишком сильные ограничения и на самих пользователей системы.

Тема практической работы №12. Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов.

Объем часов 2

Цель практической работы. Изучить функционирование маршрутизаторов,шлюзов сетевого уровня и межсетевых экранов.

МЭ поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный МЭ удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI.

Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели. Соответственно различают такие неделимые МЭ (рис. 9.5), как:

- экранирующий маршрутизатор;
- шлюз сеансового уровня (экранирующий транспорт);
- шлюз прикладного уровня (экранирующий шлюз).

Рис. 9.5. Типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI

Используемые в сетях протоколы (TCP/IP, SPX/IPX) не полностью соответствуют эталонной модели OSI, поэтому экраны перечисленных типов при выполнении своих функций могут охватывать и соседние уровни эталонной модели. Например, прикладной экран может осуществлять автоматическое зашифровывание сообщений при их передаче во внешнюю сеть, а также автоматическое расшифровывание криптографически закрытых принимаемых данных. В этом случае такой экран функционирует не только на прикладном уровне модели OSI, но и на уровне представления.

Шлюз сеансового уровня при своем функционировании охватывает транспортный и сетевой уровни модели OSI. Экранирующий маршрутизатор при анализе пакетов сообщений проверяет их заголовки не только сетевого, но и транспортного уровня.

МЭ указанных типов имеют свои достоинства и недостатки. Многие из используемых МЭ являются либо прикладными шлюзами, либо экранирующими маршрутизаторами, не обеспечивая полную безопасность межсетевого взаимодействия. Надежную защиту обеспечивают только комплексные межсетевые экраны, каждый из которых объединяет экранирующий маршрутизатор, шлюз сеансового уровня, а также прикладной шлюз.

Рассмотрим более детально особенности их функционирования.

Прикладной шлюз

Прикладной шлюз, называемый также экранирующим шлюзом, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает наиболее надежную защиту межсетевых взаимодействий. Защитные функции прикладного шлюза, как и шлюза сеансового уровня, относятся к функциям посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять существенно большее количество функций защиты, к которым относятся следующие:

• идентификация и аутентификация пользователей при попытке установления соединений через МЭ;
• проверка подлинности информации, передаваемой через шлюз;
• разграничение доступа к ресурсам внутренней и внешней сетей;
• фильтрация и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
• регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов;
• кэширование данных, запрашиваемых из внешней сети.

Поскольку функции прикладного шлюза относятся к функциям посредничества, этот шлюз представляет собой универсальный компьютер, на котором функционируют программные посредники (экранирующие агенты) — по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP и др.). Программный посредник (application proxy)каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе.

Прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию, т. е. функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью (рис. 9.6).

Рис. 9.6. Схема функционирования прикладного шлюза

Посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями (программными серверами), во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели OSI.

Прикладные шлюзы используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб TCP/IP — серверы HTTP, FTP, SMTP, NNTP и др. Эти программные серверы функционируют на МЭ в резидентном режиме и реализуют функции защиты, относящиеся к соответствующим службам TCP/IP.

Шлюз прикладного уровня обладает следующими достоинствами:

• обеспечивает высокий уровень защиты локальной сети благодаря возможности выполнения большинства функций посредничества;

• защита на уровне приложений позволяет осуществлять большое число дополнительных проверок, уменьшая тем самым вероятность проведения успешных атак, возможных из-за недостатков программного обеспечения;

• при нарушении его работоспособности блокируется сквозное прохождение пакетов между разделяемыми сетями, в результате чего безопасность защищаемой сети не снижается из-за возникновения отказов.

К недостаткам прикладного шлюза относятся:

• высокие требования к производительности и ресурсоемко-сти компьютерной платформы;

• отсутствие «прозрачности» для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий.

Варианты исполнения МЭ

Существует два основных варианта исполнения МЭ — программный и программно-аппаратный. В свою очередь программно-аппаратный вариант имеет две разновидности — в виде специализированного устройства и в виде модуля в маршрутизаторе или коммутаторе.

В настоящее время чаще используется программное решение, которое на первый взгляд выглядит более привлекательным. Это связано с тем, что для его применения достаточно, казалось бы, только приобрести программное обеспечение (ПО) МЭ и установить на любой компьютер, имеющийся в организации. Однако на практике далеко не всегда в организации находится свободный компьютер, удовлетворяющий достаточно высоким требованиям по системным ресурсам. Поэтому одновременно с приобретением ПО приобретается и компьютер для его установки. Затем следует процесс установки на компьютер операционной системы (ОС) и ее настройка, что также требует времени и оплаты работы установщиков. И только после этого устанавливается и настраивается ПО системы обнаружения атак. Нетрудно заметить, что использование обычного персонального компьютера далеко не так просто, как кажется на первый взгляд.

Поэтому в последние годы значительно возрос интерес к программно-аппаратным решениям, которые постепенно вытесняют «чисто» программные системы. Широкое распространение стали получать специализированные программно-аппаратные решения, называемые security appliance. Программно-аппаратный комплекс межсетевого экранирования обычно состоит из компьютера, а также функционирующих на нем ОС и специального ПО. Следует отметить, что это специальное ПО часто называют firewall. Используемый компьютер должен быть достаточно мощным и физически защищенным,

например находиться в специально отведенном и охраняемом помещении. Кроме того, он должен иметь средства защиты от загрузки ОС с несанкционированного носителя. Программно-аппаратные комплексы используют специализированные или обычные ПО (как правило, на базе FreeBSD, Linux или MicrosoftWindows NT (2000)), «урезанные» для выполнения заданных функций и удовлетворяющие ряду требований:
• иметь средства разграничения доступа к ресурсам системы;
• блокировать доступ к компьютерным ресурсам в обход предоставляемого программного интерфейса;
• запрещать привилегированный доступ к своим ресурсам из локальной сети;
• содержать средства мониторинга/аудита любых административных действий.

Достоинства специализированных программно-аппаратных решений:

• простота внедрения в технологию обработки информации. Такие средства поставляются с заранее установленной и настроенной ОС и защитными механизмами, поэтому необходимо только подключить их к сети, что выполняется в течение нескольких минут;

• простота управления. Данные средства могут управляться с любой рабочей станции Windows 9x, NT, 2000 или Unix. Взаимодействие консоли управления с устройством осуществляется либо по стандартным протоколам, например Telnet или SNMP, либо при помощи специализированных или защищенных протоколов, например SSH или SSL;

• отказоустойчивость и высокая доступность. Исполнение МЭ в виде специализированного программно-аппаратного комплекса позволяет реализовать механизмы обеспечения не только программной, но и аппаратной отказоустойчивости и высокой доступности;

• высокая производительность и надежность. За счет исключения из ОС всех «ненужных» сервисов и подсистем, программно-аппаратный комплекс работает более эффективно с точки зрения производительности и надежности;

• специализация на защите. Решение только задач обеспечения сетевой безопасности не приводит к затратам ресурсов на выполнение других функций, например маршрутизации и т.п.

Тема практической работы №13. Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия **.**

Объем часов 2/1

Цель практической работы. Провести анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия.

Важным моментом при использовании системы ЗИ является обеспечение потенциального невмешательства иных присутствующих в системе программ в процесс обработки информации компьютерной системой, работу системы ЗИ.

С помощью посторонних программ, присутствующих в компьютерной системе, злоумышленник может реализовать опосредованный несанкционированны доступ, то есть НСД, реализуемый злоумышленником не напрямую, а путем запуска в систему постороннего ПО – программных закладок, либо внедрения его на этапе проектирования АС. Можно выделить 3 вида разрушающих программных воздействий (программных воздействий, которые способны нарушить штатное функционирование АС).

Эти программы могут реализовать следующие функции:

1. скрывать признаки своего присутствия в оперативной среде
2. реализуют самодублирование и ассоциирование себя с другими программами. Самодублирование – процесс воспроизведения программой своего кода, который не обязательно совпадает с эталоном, но реализует те же самые функции. Под ассоциированием понимают внедрение программой своего кода в исполнительный код другой программы так, чтобы при неопределенных условиях управление передавалось этому РПВ.
3. способны разрушать код иных программ в оперативной памяти КС
4. способны переносить фрагменты информации из оперативной памяти в некие области внешней памяти, доступной злоумышленнику
5. имеют потенциальную возможность исказить либо подменить выводящуюся во внешнюю память информацию.

РПВ делятся на следующие классы:

1. Вирусы. Особенностью является направленность на самодублирование и деструктивные функции. Задача скрытия своего присутствия в ПА среде часто не ставится
2. Программные «черви» - РПВ, основной функцией которых является самодублирование путем распространения в сетях, используя уязвимости прикладных систем и сетевых сервисов.
3. «Троянские кони». Для этих программ не свойственно деструктивное воздействие. Данный класс РПВ часто относят к вирусам, однако, основной функцией РПВ данного класса, как правило, заключается в краже информации, например, номеров кредитных карт, либо в имитации сбоя ЭВМ, чтобы под видом ремонта злоумышленник мог получить к ней доступ. Основная особенность – ассоциирование либо выдача себя за часто используемое ПО либо сервисы.
4. Логические люки. РПВ, представляющее собой недекларируемую возможность, внедренную на этапе проектирования кода в исходные тексты программного обеспечения.
5. Программные закладки. Как правило, реализуют функции с 3 по 5, их действия могут быть направлены на кражу информации, либо отключение защитных функций.

Для того, чтобы РПВ получило управление, оно должно находится в оперативной памяти и активизироваться по некому общему для этого РПВ и прикладной программы, являющейся целью её воздействия, событию. Подобное событие называется активизирующим.

Если РПВ присутствует в ПА среде и загружено в оперативную память, то при отсутствии для него активизирующего события деструктивные особенности этого РПВ невозможны.

В качестве событий могут выступать прерывания, связанные с выполнением определенных действий, а часто действие, связанное с работой системы защиты, ввод с клавиатуры, прерывания по таймеру, операция с файлами и т.д.

Основные модели работы РПВ

1. Перехват. РПВ внедряется в оперативную среду и осуществляет перехват и дальнейшее копирование требуемой информации в некие скрытые области оперативной памяти. Например, клавиатурные шпионы.
2. «Троянский конь» - РПВ встраивается в постоянно используемое ПО, либо сервис и выполняет кражу информации. Либо сервис при активном событии моделирует сбойную ситуацию.
3. «Наблюдатель» - РПВ встраивается в постоянно используемое ПО или сервис и осуществляет контроль обработки информации, реализует контроль других РПВ. (Trojan Downloader)
4. Искажение либо инициатор ошибок.

РПВ, активируясь в компьютерной системе, искажает потоки выходных данных, подменяет входные данные, а также инициирует или подавляет ошибки, возникающие при работе прикладных программ.

Выделяют 3 основные группы деструктивных функций РПВ:

1. Сохранение фрагментов информации во внешнюю память.
2. Изменение алгоритмов функционирования прикладных программ.
3. Блокировка определенных режимов работы прикладных программ.

Компьютерные вирусы как класс РПВ

Вирусы как класс РПВ обладают следующими функциями:

1. способность к самодублированию
2. способность к ассоциированию с другими программами
3. способность скрывать признаки своего присутствия до определенного момента
4. направлены на деструктивные функции

Компьютерные вирусы делятся на:

- файловые
- загрузочные
- макровирусы

Жизненный цикл вирусов включает 2 фазы: латентную, когда вирус не проявляет своего присутствия, и фазу непосредственного функционирования.

Переход от латентной фазы к фазе исполнения выполняется по методу активизирующего события. Загрузка вируса в оперативную память выполняется одновременно с загрузкой инфицированного объекта. Основные способы загрузки зараженных объектов:

1. автоматическая загрузка при запуске операционной системы
2. внедрение в меню автозагрузки
3. через носители типа flash

Фаза исполнения вируса включает следующие этапы:

1. загрузка вируса в память
2. поиск «жертвы»
3. инфицирование
4. выполнение деструктивных функций
5. передача управления объекту-носителю вируса.

По способу поиска «жертвы» вирусы делятся на:

1. те, которые выполняют активный поиск объектов
2. те, которые ведут пассивный поиск, то есть устанавливают ловушки на заражаемые объекты

Инфицирование объектов может выполняться либо путем простого самокопирования кода вируса в исполнительный код, либо может использовать более сложный алгоритм, осуществляя

мутацию исполнительного кода вируса при его самодублировании. Суть мутации сводится к изменению кода таким образом, чтобы вирус нельзя было обнаружить по фиксированным сигнатурам. Может использоваться шифрование кода на различных ключах.

Суть мутации кода может заключается в изменении порядка независимых инструкций, в замене одних регистров на другие, внедрение в исполнительный код мусорных конструкций, в замене одних инструкций другими.

Вирусы, мутирующие в процессе самокопирования называются полиморфными. Если неполиморфные вирусы могут быть идентифицированы в ПА среде путем их поиска по сигнатурам, то полиморфные вирусы не имеют сигнатуру, по которой бы они однозначно идентифицировались.

Для защиты от вирусов наиболее часто применяют антивирусные мониторы, сканнеры, ПА средства, не допускающие заражение вирусами объектов операционной среды, не допускающие проникновение в КС.

Наиболее часто используемые пути проникновения вируса в КС:

1. носитель информации с зараженным объектом;
2. электронная почта;
3. компьютерная сеть.

Методы борьбы с РПВ

1. Контроль целостности, системных событий, прикладных программ, используемых данных
2. Контроль цепочек прерываний и фильтрация вызовов, критических для безопасности систем прерываний
3. Создание изолированной программной среды
4. Предотвращение результатов воздействия РПВ, например, аппаратная блокировка записи на диск
5. Поиск РПВ по свойственным им или характерным последовательностям – сигнатурам

Сигнатура – уникальная последовательность кода, свойственная вирусу, её присутствие в исполняемом коде говорит об однозначном присутствии РПВ. Можно поступить по-другому: разрешить запускать системе только те модули, которые имеют известную сигнатуру.

6. Поиск критических участков кода, путем его синтаксического анализа, выявление синтаксических характерных конструкций с точки зрения РПВ, например, вирусов.
7. Тестирование программ и компьютерной техники на испытательных стендах, в испытательных лабораториях, идентификация условий, возникающих в ПА среде, при которых она начинает вести себя некорректно.
8. Метод Мельсона – тестирование всех путей переходов программе.

Первый и второй метод действенны, когда сами контрольные элементы не подвержены воздействию закладок. Если этого не обеспечить, закладка может модифицировать алгоритм контроля целостности, подменить контрольную сумму.

Изолированная программная среда

При отсутствии активизирующих событий для программной закладки, её деструктивное воздействие невозможно, даже если она присутствует в ПА среде. Поэтому одним из способов защиты от РПВ можно нейтрализацию всех активных событий ПЗ.

ИПС характеризуется выполнением следующих условий:

1. на ЭВМ с проверенным BIOS-ом установлена проверенная ОС;
2. достоверно установлена неизменность ОС и BIOSa для текущего сеанса работы пользователя;

Эта достоверность должна достигаться только путем использования аппаратных средств, процедура контроля целостности которых прошитая в их ПЗУ, контроль целостности должен выполняться на протяжении всего сеанса работы пользователя, начиная с самых разных этапов загрузки ЭВМ.

3. кроме проверенных программ в ПА среде не запускалась и не запускается никаких иных программ. Проверенная программа перед запуском контролируется на целостность;

4. исключен запуск проверенных программ вне проверенной среды;

5. все вышесказанные требования должны выполняться для всех пользователей, аутентифицированных защищаемыми механизмами.

Идентификацию и аутентификацию пользователя желательно также выполнять на аппаратном блоке.

ИПС при запуске программы пользователя одновременно выполняет проверку условий:

- их принадлежность к списку разрешенных для записи
- их целостность

Тема практической работы №14. Изучение методов борьбы с компьютерными вирусами и средств защиты информации в Internet.

Объем часов 2/1

Цель практической работы. Изучить методы борьбы с компьютерными вирусами и средствами защиты информации в Internet

С помощью антивирусной программы Антивирус Касперского проверим компьютер на наличие вирусов, и при их обнаружении вылечим или удалим зараженные файлы.

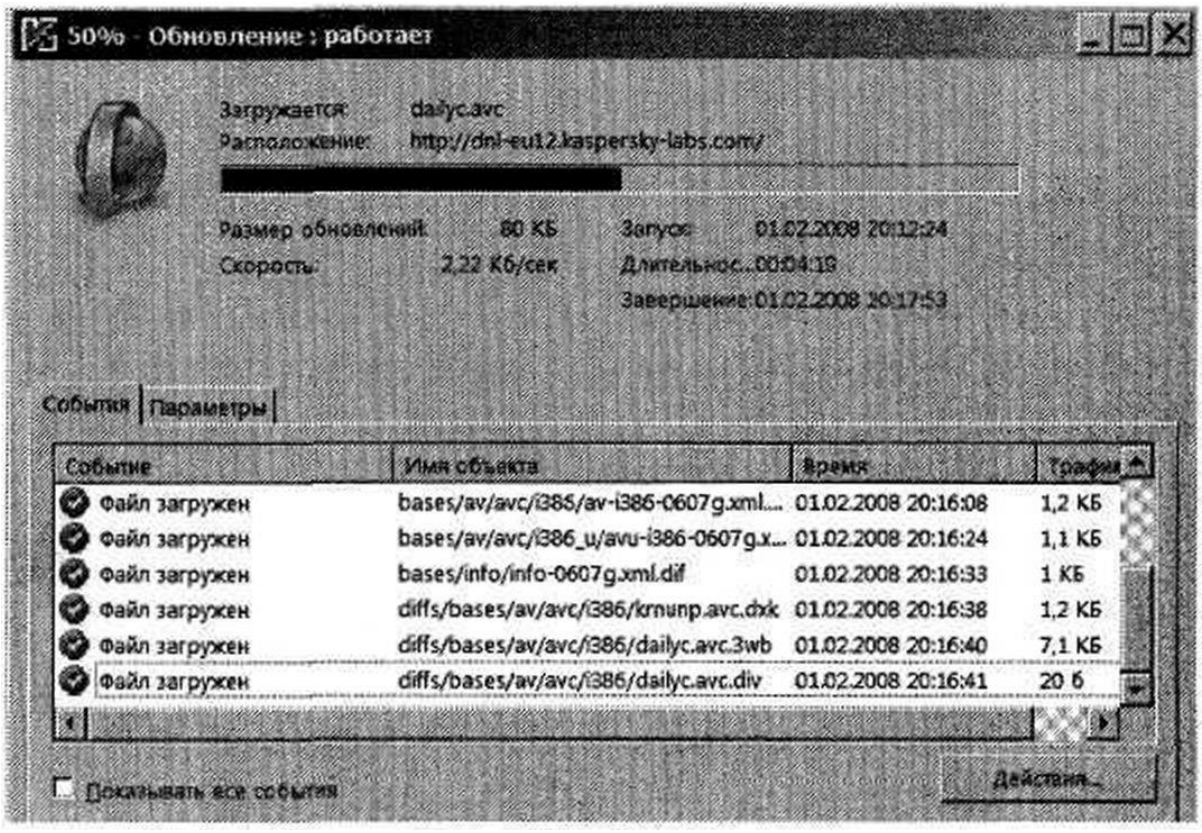
Файловый Антивирус контролирует файловую систему компьютера в реальном времени (файловый монитор). Он проверяет все открываемые, запускаемые и сохраняемые файлы на вашем компьютере и всех присоединенных дисках. Каждое обращение к файлу перехватывается приложением, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен Антивирусом Касперского. Если же файл по каким-либо причинам невозможно вылечить, он будет удален.

Прежде всего, необходимо через Интернет обновить саму антивирусную программу и вирусную базу данных.

1. В операционной системе Windows соединиться с Интернетом.

На Панели задач в контекстном меню значка антивирусной программы Антивирус Касперского выбрать пункт Обновление.

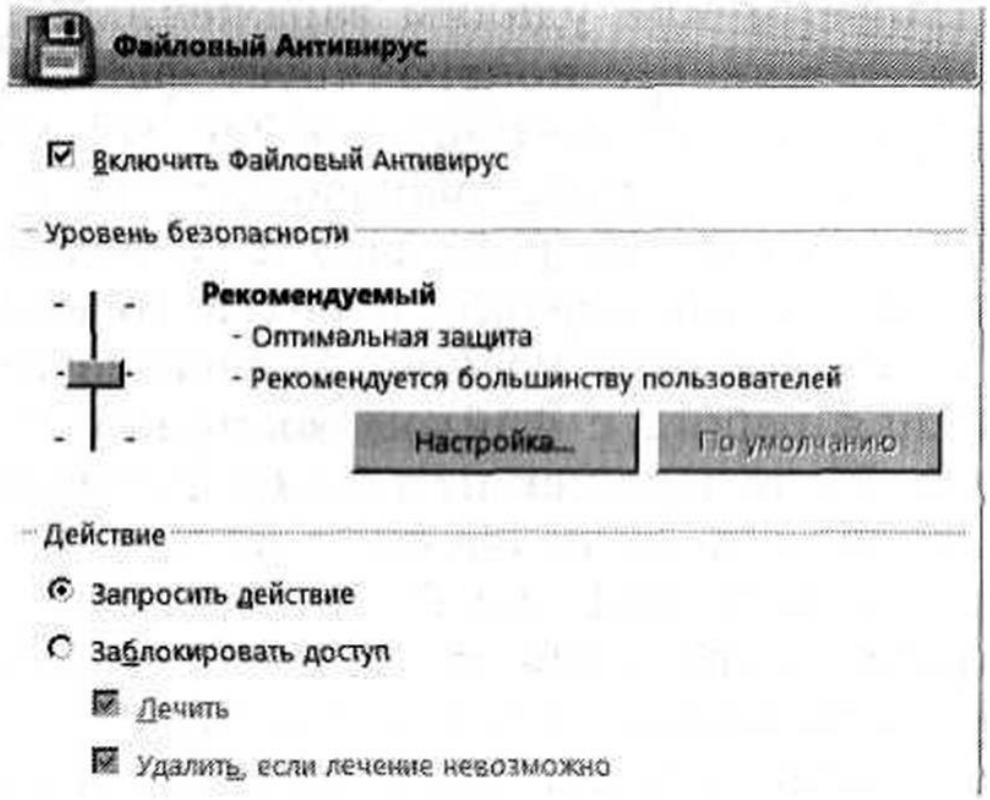
В появившемся диалоговом окне будет отображаться процесс обновления антивирусной программы и вирусной базы данных.



Настроим параметры антивирусного монитора (Файловый Антивирус). 2. В контекстном меню значка антивирусной программы выбрать пункт Настройка....

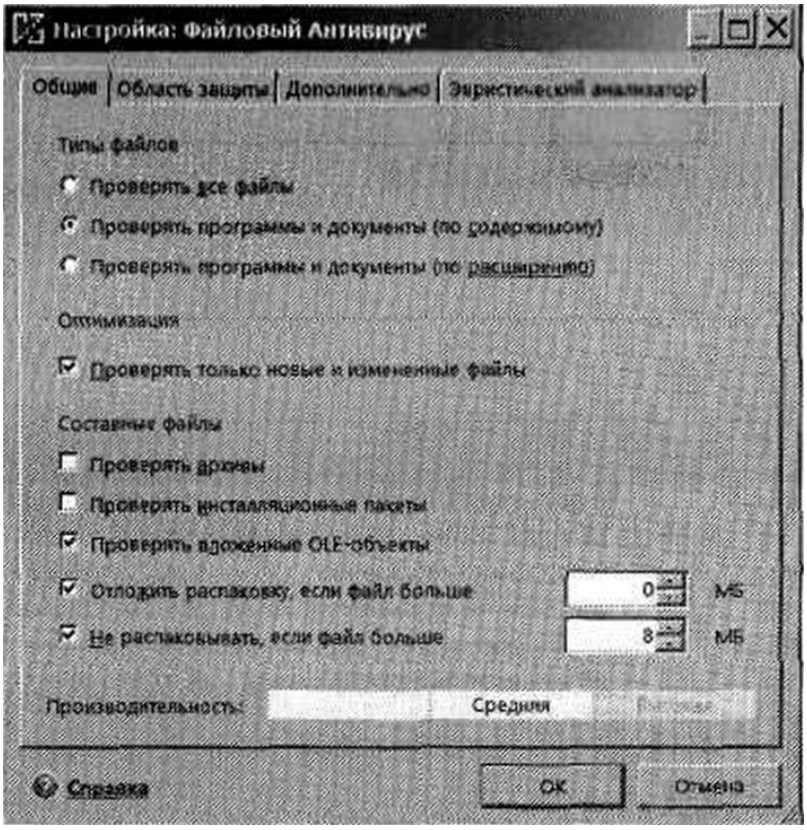
В меню левой части появившегося диалогового окна выбрать Файловый Антивирус.

В правой части окна щелкнуть по кнопке Настройка.



3. В появившемся диалоговом окне на вкладке Общие выбрать типы проверяемых файлов.

На вкладке Область защиты выбрать проверяемые диски. На вкладке Дополнительно выбрать режим проверки. На вкладке Эвристический анализатор выбрать режим его использования и уровень эвристической проверки.



4. Антивирусный монитор (Файловый Антивирус) запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса, проверяя на вредоносность совершаемые другими программами действия.

Активизировать ссылку Открыть отчет. Появится информационное окно с результатами проверки.

Тема практической работы №15. Угрозы исходящие от использования " электронной почты"

Объем часов 2

Цель практической работы. Изучить угрозы исходящие от использования «электронной почты».

Электронная почта как угроза информационной безопасности

Безопасности электронной почты угрожают изнутри и снаружи. Брешь, через которую потекут серьезные убытки, могут пробить мошенники с фишинговыми рассылками и инсайдеры. Аналитический центр Falcongaze рассказывает почему важно контролировать персонал, учить сотрудников грамотно использовать электронную почту и как защитить компанию от спама и вредоносных рассылок.

Внешние угрозы. Фишинг (от английского «рыбалка») — это интернет-мошенничество с помощью спам-рассылки. Пользователь получает письмо, в котором его убеждают перейти на фейковый сайт и ввести конфиденциальные данные. Выделяют два вида «рыбной ловли»: массовым фишингом занимаются браконьеры с массивной потрепанной сетью, целевым — опытные рыбаки со спиннингом и кучей приманок.

Злоумышленники с сетью для массового фишинга засыпают людей сообщениями с мнимыми выигрышами или поддельными уведомлениями от провайдеров и банков. Жертва рассчитывает получить деньги или восстановить утерянные данные, но расстается с ними.

Пользователь попадает в сеть, если переходит на поддельную страницу и отдает конфиденциальную информацию: данные кошелька, пароли доступа и т.д. При нажатии на фишинговую ссылку можно также получить программу-шпиона, кейлоггер или троян.

Массовые рассылки отправляются всем без разбору. Обстоятельства сложатся так, что хотя бы один из сотен тысяч схватит наживку. Целевой, или spear-phishing, — более любопытный вариант.

Целевой фишинг работает направленно. Мошенники выделяют конкретную группу: компанию, отдел, секретаря или руководителя, детально продумывают общение, собирают в соцсетях информацию об образовании, местах работы, интересах и привычках.

Далее в ход идут инструменты социальной инженерии — работа на подсознание. Жертву пробуют напугать, придумывают срочную причину для выдачи информации. Однако угрожать не обязательно, в последнее время мошенники стараются снизить подозрительность пользователя обыденным содержанием.

Простые схемы — эффективны. На законах социальной инженерии и незнании пользователями основ сетевой безопасности сыграть легко. В итоге злоумышленники овладевают учетными данными или запускают вредоносное ПО в корпоративную сеть.

Внутренние нарушители. Инсайдер и растяпа Бесконтрольный трафик входящих и исходящих сообщений внутри компании приведет к серьезным последствиям: навредить могут инсайдеры и невнимательные сотрудники.

Внутренний нарушитель имеет легитимный доступ к информации. Любой может оказаться инсайдером, крадущим закрытые данные для выгоды или мести. Так, сотрудница волгоградского банка продала знакомому мошеннику кодовые слова одиннадцати клиентов, который снял со счетов 4,3 миллиона рублей. Женщина предоставляла незаконные сведения в течение пяти месяцев.

Можно навредить и неумышленно. Утечки чаще всего происходят из-за беспечности и невнимательности. Даже если работник не хочет похитить информацию, он может стать источником утечки, отправляя закрытые данные не тому адресату.

Желает вам зла сотрудник или он просто растяпа, последствия могут быть значительными. Необходимо контролировать электронную почту от потери информации.

Технические меры. Фильтры и DLP-системы

В новые версии браузеров встроен «антифишинг», который оповещает о попадании на подложную страницу. Мошеннические сайты живут от силы дней пять — данные о них попадают в фильтр, а фишерам приходится создавать новые ресурсы снова и снова.
Большинство почтовых сайтов фильтрует и анализирует трафик. Они используют профилактические инструменты: антивирусную проверку всех входящих и исходящих сообщений, антиспам и антифишинг.
Реализовать корпоративную политику ИБ, в том числе для электронной почты, помогут DLP-системы. Такие решения уберегают от инсайдеров. Администраторы могут устанавливать настройки безопасности электронной почты и легко применять их для разных групп сотрудников.

Превентивные меры. Инструктаж и тренинги с имитацией фишинга

Несмотря на эффективность современных технологий, они не дают стопроцентную защиту от невнимательности, лени и любознательности. Обучайте пользователя, какой бы основательной не была система информационной обороны. Мошенники грамотно используют социальную инженерию для несанкционированного доступа в компьютерные сети любого уровня защиты. Технологии совершенствуются, а привычки людей остаются.
Повышайте осведомленность сотрудников о социотехнических атаках. Проводите инструктажи, информационные рассылки. Но лучший способ — обучение на собственных ошибках.
Существуют тренинги с имитацией фишинга. Для занятий можно воспользоваться автоматизированными системами, которые отправляют поддельные письма и собирают статистику откликов, такими как Gophish — фреймворк с открытым исходным кодом. Он позволяет просто и быстро выяснить реакцию сотрудников на мошенничество.
Внимательно относитесь к безопасности электронной почты. Если известные вам сервисы запрашивают персональную информацию, убедитесь, что они те, за кого себя выдают. Не забывайте, что банки не рассылают просьбы сообщить ваш пароль.
Иногда фишеры обещают бонусы или скидки. Не спешите нажимать на ссылку. Внимательно изучите входящее письмо: как выглядит логотип и написаны отдельные буквы. Зайдите на сайт компании и сравните URL-адрес с указанным в сообщении. Если ваш коллега или друг прислал поздравление с подозрительной ссылкой — не кликайте, пока не выясните, что отправитель настоящий.

Тема практической работы №16. Изучение требований по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению АСОИ.

Объем часов 2

Цель практической работы. Изучить требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению АСОИ.

К функционированию системы предъявляются следующие требования:

1) круглосуточная работоспособность системы;

2) наличие обработки исключительных ситуаций;

3) автоматизированный мониторинг действий пользователей;

4) защита информации от несанкционированного доступа;

5) распределенный доступ пользователей к системе (каждый редактирует только «свои данные» и имеет доступ только к тем данным, которые ему настроены);

6) обеспечение сохранности информации при авариях (отказах технических средств, потере питания т.п.);

7) должна быть обеспечена возможность поэтапного наращивания, как производительности, так и функционального состава системы;

8) система должна иметь открытые интерфейсы для развития и интеграции;

9) система должна обеспечить хранение нормативно-справочной, нормативно-методической информации, форм отчетности.

Требования по диагностированию системы

Для своевременного предупреждения возникновения аварийных ситуаций, внештатных ситуаций, вызванных внешними факторами (например, внешняя избыточная нагрузка) должно регулярно проводиться диагностирование и мониторинг системы.

Диагностирование должно выполняться в течение всего штатного режима работы.

Диагностирование системы при первоначальной установке и после модернизации (исправления ошибок) должно проводиться путем проведения серии взаимосвязанных тестов, включающих в себя ввод тестовых данных, проверку правильности их обработки и проверку формируемых системой отчетов.

В режиме промышленной эксплуатации система должна позволять администратору осуществлять диагностику по следующим направлениям:

1) Диагностика информационного хранилища данных. Выполняется программными модулями системы в части проверки структуры данных, сохранности информационного хранилища данных, состояния индексов и триггеров. Может выполняться дополнительная диагностика средствами СУБД.

2) Диагностика OLAP-кубов. Выполняется программными модулями системы в части проверки корректности многомерных моделей. Может выполняться дополнительное диагностирование средствами сервера OLAP.

3) Диагностика функционирования системы выполняется администратором системы с помощью функций Windows-интерфейса системы. Позволяет выявить ошибки при подключении к иным БД для закачки данных и ошибки системы, возникающие при работе пользователей.

Требования к информационной безопасности

Требования к информационной безопасности и защите информации в системе ограничиваются реализацией механизма управления и контроля доступа к данным. Защита от

несанкционированного доступа должна осуществляться с обязательным использованием функций по разграничению полномочий и обеспечению безопасности хранения, предоставляемых программным обеспечением СУБД и операционной системы, на которых функционирует система.

В системе должно обеспечиваться разграничение прав доступа на следующих уровнях:

1) разграничение прав доступа пользователей к объектам системы;

2) разграничение доступа к функциям системы (функции, доступ к которым пользователю запрещен, не должны отображаться на экране);

3) разграничение доступа к данным (информация о данных, доступ к которым пользователю запрещен, не должна отображаться на экране);

4) разделение полномочий на работу с данными (просмотр, редактирование).

В рамках системы должны присутствовать специализированные программные модули администрирования, обеспечивающие выполнение следующих функций:

1) возможность гибкой настройки полномочий пользователей на доступ к системе;

2) ведение протокола доступа к ресурсам системы (с возможностью экспорта в файл) по полям (дата, время, тип события, тип объекта, наименование объекта, идентификатор объекта, имя пользователя, идентификатор пользователя, рабочая станция);

3) ведение протокола ошибок системы для аудита (дата и время, имя пользователя, идентификатор пользователя, имя программы, рабочая станция, текст ошибки);

4) ведение списка пользователей, допущенных к работе с системой;

5) фиксация в протоколе доступа всех действий пользователей: попытки доступа пользователя к любому объекту системы, изменение информационного состояния системы, выполнение каждой операции в Системе.

Для веб-интерфейса системы должны выполняться следующие требования:

1) вход пользователей в систему возможен только после аутентификации пользователя;

2) должна использоваться аутентификация с указанием логина/пароля или по доменной аутентификации пользователя;

3) должна быть обеспечена возможность работы через защищенный канал связи с поддержкой SSL (Secure Sockets Layer);

4) всем пользователям в системе распределяются права на доступ к определенному набору документов;

5) должна быть возможность объединить пользователей в группы и назначить права группам пользователей;

6) для незарегистрированных пользователей должен существовать отдельный пользователь или группа «Гость». Этому пользователю или группе администратор системы также должен настраивать доступ к той части информации, которую можно считать публичной;

7) состав аналитических отчетов системы подразделяется на «открытую» и «закрытую» части. Отчеты «открытой» части доступны для всех пользователей и группы «Гость». Отчеты «закрытой» части доступны согласно индивидуально назначенным правам для отдельных пользователей. Распределение данных аналитических отчетов для отражения в «открытой» и «закрытой» частях системы производится Заказчиком по итогам предпроектного обследования.

Требования к надежности

Состав и количественные значения показателей надежности для системы в целом

Проектные решения должны обеспечивать:

· Сохранение работоспособности системы при отказе или выходе из строя по любым причинам одного из компонентов комплекса технических средств или телекоммуникационной подсистемы;

· Сохранение всей накопленной на момент отказа или выхода из строя информации при отказе двух и более одинаковых по назначению компонентов системы не зависимо от их назначения, с последующим восстановлением после проведения ремонтных и восстановительных работ функционирования системы.

Технические меры по обеспечению надежности должны предусматривать:

1) Резервирование критически важных компонентов и данных системы и отсутствие единой точки отказа;

2) Использование технических средств с избыточными компонентами и возможностью их горячей замены;

3) Конфигурирование используемых средств и применение специализированного ПО, обеспечивающего высокую доступность.

Организационные меры по обеспечению надежности должны быть направлены на минимизацию ошибок персонала (пользователей), а также персонала службы эксплуатации при эксплуатации и проведении работ по обслуживанию комплекса технических средств системы, минимизацию времени ремонта или замены вышедших из строя компонентов за счет:

Квалификации персонала (пользователей);

Квалификации обслуживающего персонала;

Регламентации и нормативного обеспечения выполнения работ персонала (пользователей);

Регламентации проведения работ и процедур по обслуживанию и восстановлению системы;

Своевременного оповещения пользователей о случаях нештатной работы компонентов системы;

Своевременной диагностики неисправностей;

Наличия договоров на сервисное обслуживание и поддержку компонентов комплекса технических средств.

В целом, надежность аппаратно-программного обеспечения должна обеспечивать выполнение задач системы с временем однократного простоя не более 30 мин и суммарным временем простоя не более 24 часов в год.

При работе системы возможны следующие аварийные ситуации, которые влияют на надежность работы системы:

1. Сбои технических средств:

1.1 Сбой в электроснабжении сервера: информация восстанавливается с поддержкой целостности на момент сбоя. Требуется перезагрузка сервера и повторное соединение рабочих станций с сервером. При этом теряются все не сохраненные данные на рабочих станциях. Целостность обеспечивается путем поддержки механизма транзакций сервером БД. В случае невозможности запуска сервера или использования БД, данные системы восстанавливаются из резервной копии.

1.2 Сбой в электроснабжении рабочей станции операторов системы: все, не сохраненные на момент сбоя данные рабочей станции, теряются и восстановлению не подлежат; на сервере обеспечивается целостность информации. Для продолжения работы на рабочей станции требуется перезагрузка операционной системы и повторное подключение к БД. На прочие рабочие станции и сервер сбой одной из рабочих станций не оказывает никакого влияния.

1.3 Сбой в электроснабжении обеспечения локальной сети (поломка сети): система остается неработоспособной до восстановления нормального функционирования сети. После восстановления функционирования сети требуется повторное подключение рабочих станций операторов к серверу.

1.4 Если одна из рабочих станций (или единственная рабочая станция при локальной работе) располагается непосредственно на сервере, то сбой сети не оказывает на нее никакого влияния.

1.5 Поломка сервера (потеря всей информации, хранимой на сервере): все данные теряются, восстановление информации происходит из резервной копии, хранящейся удаленно от сервера.

2. Ошибки программного обеспечения:

2.1 Ошибки системы, не выявленные при отладке и испытании системы, Разработчик обязан устранить в течение гарантийного срока эксплуатации. Срок устранения зависит от сложности выявленных ошибок и составляет от 5 до 30 дней.

2.2 Сбои программного обеспечения сервера: требуется переустановка программного обеспечения сервера. Если потеряна информация, хранимая на сервере, то требуется восстановление данных из резервной копии.

2.3 Сбои программного обеспечения рабочих станций операторов и пользователей: требуется переустановка программного обеспечения рабочей станции.

Общие рекомендации

По всем вопросам, связанным с изучением дисциплины (включая самостоятельную работу), консультироваться с преподавателем.

Контроль и оценка результатов

Оценка за выполнение лабораторной работы выставляется в форме ***по пятибалльной системе*** и учитывается как показатель текущей успеваемости студента.

Качественная оценка индивидуальных образовательных достижений		**Критерии оценки результата**
балл (оценка)	**вербальный аналог**	
5	отлично	Представленные работы высокого качества, уровень выполнения отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, выполнены все предусмотренные лабораторной работой задания.
4	хорошо	Уровень выполнения работы отвечает всем требованиям, теоретическое содержание курса освоено полностью без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные лабораторной работой задания выполнены, некоторые из выполненных заданий, возможно, содержат ошибки.
3	удовлетворительно	Уровень выполнения работы отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных лабораторной работой заданий выполнено, некоторые виды заданий выполнены с ошибками.
2	не удовлетворительно	Теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных лабораторной работой заданий не выполнено.