Министерство образования Республики Беларусь

Учреждение образования

Белорусский Государственный Университет Информатики и Радиоэлектроники

ФЗВиДО

Кафедра РЭС

**Контрольная работа**

по дисциплине «Правовое и нормативное обеспечение защиты информации»

Вариант 30

Путника Антона Денисовича

2010

Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Защита от угрозы нарушения целостности информации. Защита целостности информации в памяти АС. Защита целостности информации в каналах связи.

С позиции обеспечения безопасности информации информационную систему (ИС) целесообразно рассматривать в виде трех связных взаимовлияющих друг на друга компонент:

1) информация;

2) технические и программные средства;

3) обслуживающий персонал и пользователи.

Целью создания любой ИС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности. При этом задача обеспечения информации должна решаться путем защиты от внешних и внутренних неразрешенных (несанкционированных) воздействий.

Под угрозой обычно понимают потенциально возможно событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. В дальнейшем изложении угрозой информационной безопасности автоматизированной системы (АС) будем называть возможность реализации воздействия на информацию, обрабатываемую АС, приводящего к искажению, уничтожению, копированию, блокированию, доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

Утечка информации рассматривается как бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена.

Существует три разновидности угроз.

1. Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин «утечка».

2. Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

Целостность информации – существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Чаще субъектов интересует обеспечение более широкого свойства – достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т.е. ее неискаженности.

3. Угроза отказа служб возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Доступность информации – свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Практически любая АС может выступать в качестве объекта информационной атаки, которая может быть определена как совокупность действий злоумышленника, направленная на нарушение одного из трёх свойств информации – конфиденциальности, целостности или доступности. Рассмотрим эти свойства более подробно. Свойство конфиденциальности позволяет не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам. Характерным примером нарушения конфиденциальности информации является кража из системы секретной информации с целью её дальнейшей перепродажи. Целостность информации подразумевает её способность не подвергаться изменению или уничтожению в результате несанкционированного доступа. В качестве примера нарушения этого свойства можно привести ситуацию, при которой злоумышленник преднамеренно искажает содержимое одного из электронных документов, хранящихся в системе. И, наконец, доступность информации определяется как её свойство быть доступной и используемой по запросу со стороны любого уполномоченного пользователя. Так, например, злоумышленник сможет нарушить доступность Интернет-портала если ни один из легальных пользователей не сможет получить доступ к его содержимому. Таким образом, в результате нарушения конфиденциальности, целостности или доступности информации злоумышленник тем самым может нарушить бизнес-процессы компании, которые базируются на информационных ресурсах, которые являлись объектом атаки.

Для реализации информационной атаки нарушителю необходимо активизировать или, другими словами, использовать определённую уязвимость АС. Под уязвимостью принято понимать слабое место АС, на основе которого возможна успешная реализация атаки. Примерами уязвимостей АС могут являться: некорректная конфигурация сетевых служб АС, наличие ПО без установленных модулей обновления, использование нестойких к угадыванию паролей, отсутствие необходимых средств защиты информации и др. Логическая связь уязвимости, атаки и её возможных последствий показана на рис. 1.

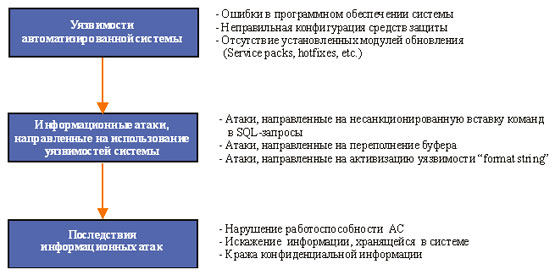


Рис. 1. Связь уязвимости, атаки и её возможных последствий

##### Уязвимости - ахиллесова пята автоматизированных систем

Уязвимости являются основной причиной возникновения информационных атак. Наличие самих слабых мест в АС может быть обусловлено самыми различными факторами, начиная с простой халатности сотрудников, и заканчивая преднамеренными действиями злоумышленников.

Уязвимости могут присутствовать как в программно-аппаратном, так и организационно-правовом обеспечении АС. Основная часть уязвимостей организационно-правового обеспечения обусловлена отсутствием на предприятиях нормативных документов, касающихся вопросов информационной безопасности. Примером уязвимости данного типа является отсутствие в организации утверждённой концепции или политики информационной безопасности, которая бы определяла требования к защите АС, а также конкретные пути их реализации. Уязвимости программно-аппаратного обеспечения могут присутствовать в программных или аппаратных компонентах рабочих станций пользователей АС, серверов, а также коммуникационного оборудования и каналов связи АС.

Уязвимости АС могут быть внесены как на технологическом, так и на эксплуатационном этапах жизненного цикла АС. На технологическом этапе нарушителями могут быть инженерно-технические работники, участвующие в процессе проектирования, разработки, установки и настройки программно-аппаратного обеспечения АС.

Внесение эксплуатационных уязвимостей может иметь место при неправильной настройке и использовании программно-аппаратного обеспечения АС. В отличие от технологических, устранение эксплуатационных уязвимостей требует меньших усилий, поскольку для этого достаточно изменить конфигурацию АС. Характерными примерами уязвимостей этого типа являются:

* наличие слабых, не стойких к угадыванию паролей доступа к ресурсам АС. При активизации этой уязвимости нарушитель может получить несанкционированный доступ к АС путём взлома пароля при помощи метода полного перебора или подбора по словарю;
* наличие в системе незаблокированных встроенных учётных записей пользователей, при помощи которых потенциальный нарушитель может собрать дополнительную информацию, необходимую для проведения атаки. Примерами таких учётных записей являются запись «Guest» в операционных системах или запись «Anonymous» в FTP-серверах;
* неправильным образом установленные права доступа пользователей к информационным ресурсам АС. В случае если в результате ошибки администратора пользователи, работающие с системой, имеют больше прав доступа, чем это необходимо для выполнения их функциональных обязанностей, то это может привести к несанкционированному использованию дополнительных полномочий для проведения атак. Например, если пользователи будут иметь права доступа на чтение содержимого исходных текстов серверных сценариев, выполняемых на стороне Web-сервера, то этим может воспользоваться потенциальный нарушитель для изучения алгоритмов работы механизмов защиты Web-приложений и поиска в них уязвимых мест;
* наличие в АС неиспользуемых, но потенциально опасных сетевых служб и программных компонентов. Так, например, большая часть сетевых серверных служб, таких как Web-серверы и серверы СУБД поставляются вместе с примерами программ, которые демонстрируют функциональные возможности этих продуктов. В некоторых случаях эти программы имеют высокий уровень привилегий в системе или содержат уязвимости, использование которых злоумышленником может привести к нарушению информационной безопасности системы. Примерами таких программ являются образцы CGI-модулей, которые поставляются вместе с Web-приложениями, а также примеры хранимых процедур в серверах СУБД;
* неправильная конфигурация средств защиты, приводящая к возможности проведения сетевых атак. Так, например, ошибки в настройке межсетевого экрана могут привести к тому, что злоумышленник сможет передавать через него пакеты данных.

##### Информационные атаки

Уязвимости могут использоваться злоумышленниками для реализации информационных атак на ресурсы АС. Согласно разработанной классификации любая атака в общем случае может быть разделена на четыре стадии:

* стадия рекогносцировки. На этом этапе нарушитель осуществляет сбор данных об объекте атаки, на основе которых планируются дальнейшие стадии атаки. Примерами такой информации являются: тип и версия операционной системы (ОС), установленной на узлах АС, список пользователей, зарегистрированных в системе, сведения об используемом прикладном ПО и др. При этом в качестве объектов атак могут выступать рабочие станции пользователей, серверы, а также коммуникационное оборудование АС;
* стадия вторжения в АС. На этом этапе нарушитель получает несанкционированный доступ к ресурсам тех узлов АС, по отношению к которым совершается атака;
* стадия атакующего воздействия на АС. Данный этап направлен на достижение нарушителем тех целей, ради которых предпринималась атака. Примерами таких действий могут являться нарушение работоспособности АС, кража конфиденциальной информации, хранимой в системе, удаление или модификация данных системы и др. При этом атакующий может также осуществлять действия, которые могут быть направлены на удаление следов его присутствия в АС;
* стадия дальнейшего развития атаки. На этом этапе выполняются действия, которые направлены на продолжение атаки на ресурсы других узлов АС.

Схематично стадии жизненного цикла информационной атаки изображены на рис. 2.

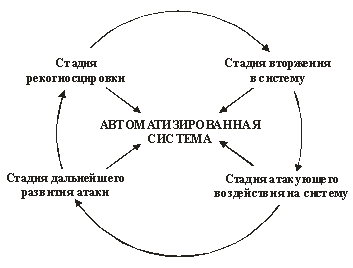


Рис. 2. Жизненный цикл типовой информационной атаки на ресурсы АС

Информационные атаки могут быть классифицированы как внешние или внутренние. Внешние сетевые атаки проводятся извне АС, т.е. с тех узлов, которые не входят в состав системы. Примером внешней сетевой атаки являются вторжение нарушителя в ЛВС из сети Интернет. Внутренние атаки проводятся изнутри АС с одного из её серверов или рабочих станций. В качестве примера такой атаки можно привести действия сотрудника компании, направленные на утечку конфиденциальной информации.

##### Последствия информационных атак

Последствия, к которым могут привести информационные атаки, могут по-разному рассматриваться исходя из той или иной ситуации. Так, например, одно и тоже последствие атаки может сводиться к искажению системного файла на сервере для системного администратора, в то время как для руководителя компании – приостановкой одного из важнейших бизнес-процессов предприятия. Последствия информационных атак могут воздействовать на аппаратное, общесистемное или прикладное программное обеспечение, а также на информацию, которая хранится в АС. Так, например, воздействие на аппаратное обеспечение может быть направлено на несанкционированное изменение памяти микросхемы BIOS, расположенной на материнской плате инфицированного компьютера. В результате такой атаки может быть изменён пароль доступа к настройкам BIOS или полностью искажено содержимое памяти BIOS, что приведёт к блокированию возможности загрузки компьютера. Восстановление работоспособности хоста в этом случае может потребовать перепрограммирования памяти BIOS.

##### Существующие методы и средства защиты от информационных атак

В настоящее время существует большое количество организационных и технических мер защиты, которые могут использоваться для защиты от информационных атак. организационные и технические. Организационные средства связаны с разработкой и внедрением на предприятиях нормативно-правовых документов, определяющих требования к информационной безопасности АС. Примерами таких документов являются политика и концепция обеспечения информационной безопасности, должностные инструкции по работе персонала с АС и т.д. Технические же средства защиты АС реализуются при помощи соответствующих программных, аппаратных или программно-аппаратных комплексов.

На сегодняшний день можно выделить следующие основные виды технических средств защиты:

* средства криптографической защиты информации;
* средства разграничения доступа пользователей к ресурсам АС;
* средства межсетевого экранирования;
* средства анализа защищённости АС;
* средства обнаружения атак;
* средства антивирусной защиты;
* средства контентного анализа;
* средства защиты от спама.

Средства криптографической защиты информации представляют собой средства вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее конфиденциальности и контроля целостности. Защита информации может осуществляться в процессе её передачи по каналам связи или в процессе хранения и обработки информации на узлах АС. Для решения этих задач используются различные типы СКЗИ, описание которых приводится ниже.

Средства разграничения доступа предназначены для защиты от несанкционированного доступа к информационным ресурсам системы. Разграничение доступа реализуется средствами защиты на основе процедур идентификации, аутентификации и авторизации пользователей, претендующих на получение доступа к информационным ресурсам АС.

На этапе собственной идентификации пользователь предоставляет свой идентификатор, в качестве которого, как правило, используется регистрационное имя учётной записи пользователя АС. После представления идентификатора, проводится проверка того, что этот идентификатор действительно принадлежит пользователю, претендующему на получение доступа к информации АС. Для этого выполняется процедура аутентификации, в процессе которой пользователь должен предоставить аутентификационный параметр, при помощи которого подтверждается принадлежность идентификатора пользователю. В качестве параметров аутентификации могут использоваться сетевые адреса, пароли, симметричные секретные ключи, цифровые сертификаты, биометрические данные (отпечатки пальцев, голосовая информация) и т.д. Необходимо отметить, что процедура идентификации и аутентификации пользователей в большинстве случаев проводится одновременно, т.е. пользователь сразу предъявляет идентификационные и аутентификационные параметры доступа.

В случае успешного завершения процедур идентификации и аутентификации проводится авторизация пользователя, в процессе которой определяется множество информационных ресурсов, с которыми может работать пользователь, а также множество операций которые могут быть выполнены с этими информационными ресурсами АС. Присвоение пользователям идентификационных и аутентификационных параметров, а также определение их прав доступа осуществляется на этапе регистрации пользователей в АС (рис. 3).



Рис. 3. Процедура входа пользователя в автоматизированную систему

Межсетевые экраны (МЭ) реализуют методы контроля за информацией, поступающей в АС и/или выходящей из АС, и обеспечения защиты АС посредством фильтрации информации на основе критериев, заданных администратором. Процедура фильтрации включает в себя анализ заголовков каждого пакета, проходящего через МЭ, и передачу его дальше по маршруту следования только в случае, если он удовлетворяет заданным правилам фильтрации. При помощи фильтрования МЭ позволяют обеспечить защиту от сетевых атак путём удаления из информационного потока тех пакетов данных, которые представляют потенциальную опасность для АС.

Средства анализа защищённости выделены в представленной выше классификации в обособленную группу, поскольку предназначены для выявления уязвимостей в программно-аппаратном обеспечении АС. Системы анализа защищённости являются превентивным средством защиты, которое позволяет выявлять уязвимости при помощи анализа исходных текстов ПО АС, анализа исполняемого кода ПО АС или анализа настроек программно-аппаратного обеспечения АС.

Средства антивирусной защиты предназначены для обнаружения и удаления вредоносного ПО, присутствующего в АС. К таким вредоносным программам относятся компьютерные вирусы, а также ПО типа «троянский конь», «spyware» и «adware».

Средства защиты от спама обеспечивают выявление и фильтрацию незапрошенных почтовых сообщений рекламного характера. В ряде случаев для рассылки спама используется вредоносное программное обеспечение, внедряемое на хосты АС и использующее адресные книги, которые хранятся в почтовых клиентах пользователей. Наличие спама в АС может привести к одному из следующих негативных последствий:

* нарушение работоспособности почтовой системы вследствие большого потока входящих сообщений. При этом может быть нарушена доступность как всего почтового сервера, так и отдельных почтовых ящиков вследствие их переполнения. В результате пользователи АС не смогут отправлять или получать сообщения при помощи почтовой системы организации;
* реализация «phishing»-атак, в результате которых пользователю присылается почтовое сообщение от чужого имени с просьбой выполнить определённые действия. В таком сообщении пользователя могут попросить запустить определённую программу, ввести своё регистрационное имя и пароль или выполнить какие-либо другие действия, которые могу помочь злоумышленнику успешно провести атаку на информационные ресурсы АС. Примером атаки этого типа является посылка пользователю сообщения от имени известного банка, в котором содержится запрос о необходимости смены пароля доступа к ресурсам Web-сайта банка. В случае если пользователь обратится по Интернет-адресу, указанному в таком почтовом сообщении, то он будет перенаправлен на ложный Web-сайт злоумышленника, представляющий собой копию реального сайта банка. В результате такой атаки вся парольная информация, введённая пользователем на ложном сайте, будет автоматически передана нарушителю;
* снижение производительности труда персонала вследствие необходимости ежедневного просмотра и ручного удаления спамовских сообщений из почтовых ящиков.

Средства контентного анализа предназначены для мониторинга сетевого трафика с целью выявления нарушений политики безопасности. В настоящее время можно выделить два основных вида средств контентного анализа – системы аудита почтовых сообщений и системы мониторинга Интернет-трафика. Системы аудита почтовых сообщений предполагают сбор информации о SMTP-сообщениях, циркулирующих в АС, и её последующий анализ с целью выявления несанкционированных почтовых сообщений, нарушающих требования безопасности, заданные администратором. Так, например, системы этого типа позволяют выявлять и блокировать возможные каналы утечки конфиденциальной информации через почтовую систему. Системы мониторинга Интернет-трафика предназначены для контроля доступа пользователей к ресурсам сети Интернет. Средства защиты данного типа позволяют заблокировать доступ пользователей к запрещённым Интернет-ресурсам, а также выявить попытку передачи конфиденциальной информации по протоколу HTTP. Системы мониторинга устанавливаются таким образом, чтобы через них проходил весь сетевой трафик, передаваемый в сеть Интернет.

Системы обнаружения атак представляют собой специализированные программные или программно-аппаратные комплексы, предназначенные для выявления информационных атак на ресурсы АС посредством сбора и анализа данных о событиях, регистрируемых в системе. Система обнаружения атак включает в себя следующие компоненты:

* модули-датчики, предназначенные для сбора необходимой информации о функционировании АС. Иногда датчики также называют сенсорами;
* модуль выявления атак, выполняющий анализ данных, собранных датчиками, с целью обнаружения информационных атак;
* модуль реагирования на обнаруженные атаки;
* модуль хранения данных, в котором содержится вся конфигурационная информация, а также результаты работы средств обнаружения атак;
* модуль управления компонентами средств обнаружения атак.

##### Комплексный подход к обеспечению информационной безопасности

Комплексный подход к защите от информационных предусматривает согласованное применение правовых, организационных и программно-технических мер, перекрывающих в совокупности все основные каналы реализации вирусных угроз. В соответствии с этим подходом в организации должен быть реализован следующий комплекс мер:

* меры по выявлению и устранению уязвимостей, на основе которых реализуются угрозы. Это позволит исключить причины возможного возникновения информационных атак;
* меры, направленные на своевременное обнаружение и блокирование информационных атак;
* меры, обеспечивающие выявление и ликвидацию последствий атак. Данный класс мер защиты направлен на минимизацию ущерба, нанесённого в результате реализации угроз безопасности.

Важно понимать, что эффективная реализация вышеперечисленных мер на предприятии возможна только при условии наличия нормативно-методического, технологического и кадрового обеспечения информационной безопасности (рис. 4).



Рис. 4. Основные направления обеспечения информационной безопасности

Нормативно-методическое обеспечение информационной безопасности предполагает создание сбалансированной правовой базы в области защиты от угроз. Для этого в компании должен быть разработан комплекс внутренних нормативных документов и процедур, обеспечивающих процесс эксплуатации системы информационной безопасности. Состав таких документов во многом зависит от размеров самой организации, уровня сложности АС, количества объектов защиты и т.д. Так, например, для крупных организаций основополагающим нормативным документом в области защиты информации должна быть концепция или политика безопасности.

В рамках кадрового обеспечения информационной безопасности в компании должен быть организован процесс обучения сотрудников по вопросам противодействия информационным атакам. В процессе обучения должны рассматриваться как теоретические, так и практические аспекты информационной защиты. При этом программа обучения может составляться в зависимости от должностных обязанностей сотрудника, а также от того к каким информационным ресурсам он имеет доступ.

информационная угроза безопасность

**Литература**

1. Мелик-Гайказян, И.В. «Информационные процессы и реальность»/ И.В. Мелик-Гайказян.-М., 1997.

2. Кураков, Л.П. «Информация как объект правовой защиты»/ Л.П. Кураков, С. Н. Смирнов.- М., 1998.

3. Бриллюэн, Л. “Научная неопределенность и информация” / Л. Бриллюэн. М., 1966.

4. Якушев, М.А. «Интернет и право». М.А. Якушев. «Законодательство»/ 1997, № 1 М.