Д.Ю. Нечаев

ПРИНЦИПЫ СОЗДАНИЯ И ФУНКЦИОНИРОВАНИЯ ЭКОНОМИЧЕСКИХ СИСТЕМ БЕЗОПАСНОСТИ

Угрозы информационной безопасности в экономике и торговле могут возникать в основном в результате совершения компьютерных преступлений, действий профессиональных хакеров, в результате осуществления актов саботажа, а также вследствие ошибок обслуживающего персонала, сбоев в работе оборудования и стихийных бедствий.

Компьютерные преступления (промышленный шпионаж). Промышленный шпионаж представляет собой источник угроз направленных на незаконное овладение коммерческими тайнами предприятий с целью использования содержащейся в них конфиденциальной информации для получения преимуществ в предпринимательской деятельности или организации подрывных действий против конкурента (конкурентов). В качестве субъектов промышленного шпионажа могут выступать:

- фирмы конкуренты;
- кредиторы, опасающиеся вкладывать деньги в неплатежеспособные предприятия;
- фирмы покупатели, стремящиеся приобретать товары по боле низким ценам;
- фирмы продавцы сырья, оборудования и комплектующих изделий, ставящие цель получения максимально возможной прибыли" реализации продукции;
- преступные элементы, готовящие почву для физического завладения собственностью через нападение и вымогательство.

Профессиональные хакеры. Это наиболее квалифицированные злоумышленники, прекрасно знающие вычислительную технику и системы связи. Для вхождения в систему они чаще всего используют некоторую систематику и эксперименты, но рассчитывают также на удачу или догадку. Их цель - выявить и преодолеть систему защиты, изучить возможности вычислительной системы и затем удалиться, утвердившись в возможности достижения цели. Благодаря высокой квалификации эти люди понимают, что степень риска мала, так как отсутствуют мотивы разрушения или хищения. Эту категорию лиц могут использовать преступные группировки для получения информации в целях промышленного шпионажа, наживы, в политических целях и т.п.

Акты саботажа. Акты саботажа могут возникать в результате недовольства работников учреждений и предприятий своим служебным и материальным положением, а также психических расстройств. Недовольный руководителем служащий создает одну из самых больших угроз безопасности информации. Своими действиями он может уничтожить или исказить информацию, нарушить нормальное функционирование компьютер-

ных сетей и т.п.

Ошибки обслуживающего персонала. Угрозы безопасности информации могут возникать из-за ошибок человека в процессе эксплуатации компьютерных сетей, при проведении ремонтных работ и неквалифицированном или небрежном управлении вычислительным процессом. Во время работы программисты, операторы, пользователи, обслуживающий персонал могут допускать следующие ошибки:

- уничтожение запрещенного для удаления файла;
- изменение запрещенного для изменения файла;
- некорректную установку программного обеспечения;
- несоблюдение режима безопасности.

Ошибки могут приводить к блокированию информации, к изменению режима функционирования элементов компьютерной сети, а также к разглашению конфиденциальной информации, идентификаторов и паролей. Использование чужих ошибок является одним из методов несанкционированного доступа к информации.

Сбои оборудования. В процессе функционирования компьютерных сетей могут возникнуть сбои в работе технических и программных средств вычислительной техники и линий связи. Случайные сбои могут повлечь утерю, искажение информации или нерегламентированный доступ к ней, поэтому они рассматриваются как источник угроз безопасности информации. В то же время случайные сбои в работе оборудования могут использоваться для осуществления преднамеренного несанкционированного доступа.

Стихийные бедствия. К этому источнику угроз для компьютерных сетей относятся такие стихийные явления природы, как землетрясения, наводнения, пожары (молния), ураганы и т.п.

Основные источники угроз безопасности информации делятся на умышленные (преднамеренные) и случайные (непреднамеренные).

Умышленные угрозы - это запрещенные законом действия людей, нацеленные на получение доступа к охраняемым сведениям. Источниками данного класса угроз являются промышленный шпионаж и акты саботажа.

Случайные угрозы могут исходить от таких источников угроз, как ошибки в деятельности персонала, сбои в работе оборудования и стихийные бедствия. Этот класс угроз интенсивно используют лица, занимающиеся промышленным шпионажем.

Частота возникновения случайных угроз значительно выше, чем умышленных угроз.

По целям доступа или воздействия источников угроз на информацию выделяются следующие виды угроз:

- перехват (утечка) информации;
- искажение (модификация) информации;
- навязывание ложной (подделка) информации;

- разрушение информации;
- блокирование доступа к информации.

Угрозы утечки информации. Основными источниками данного вида угрозы является промышленный шпионаж. Для достижения доступа к информации могут использоваться как специальные средства, так и ошибки в деятельности персонала или сбои в работе оборудования.

Угрозы искажения информации. Модификация (искажение) информации, обрабатываемой с помощью технических средств - преднамеренный или случайный акт, который приводит к изменению содержания информации. Источниками данного вида угроз могут быть акты саботажа, ошибки в деятельности персонала, сбои в работе оборудования. Характерным проявлением данного вида угроз в последнее время стали компьютерные вирусы.

Навязывание ложной информации. Подделка информации, обрабатываемой с помощью технических средств - это умышленные действия по модификации (созданию ложной) информации, имеющие целью повлиять на решения, принимаемые на основании этой информации. Данный вид угроз характерен для промышленного шпионажа и актов саботажа.

Угрозы разрушения информации. Разрушение информации, обрабатываемой с помощью технических средств, - событие, состоящее в том, что информация перестает физически существовать для собственника информации. Этот вид угроз исходит как от случайных, так и умышленных источников угроз. Характерным проявлением данного вида угроз в последнее время стали компьютерные вирусы.

Блокирование доступа к информации. Блокирование информации, обрабатываемой с помощью технических средств, - действие, в результате которого информация становится недоступной для субъектов, имеющих право доступа к ней. Как правило, этот вид угроз используется в актах саботажа.

По способам реализации угроз выделяются пассивные и активные способы. ***Пассивный способ*** - это способ реализации угроз без нарушения целостности компьютерной сети и какого-либо воздействия на ее элементы. При ***активном*** способе происходит контакт источника угроз с элементами компьютерной сети посредством какого-либо воздействия.

Преимущество пассивных способов состоит в том, что их обычно сложнее обнаружить. Реализация активных способов позволяет добиться результатов, достижение которых при использовании пассивных угроз невозможно. Одной из фаз воздействия на информацию при использовании активных способов может быть восстановление прежнего состояния информации после того, как цель достигнута.

К пассивным способам реализации угроз безопасности информации относятся несанкционированный доступ к информации штатными средствами с использованием:

- ошибок в назначении полномочий пользователям;
- сбоев в оборудовании;
- ошибок в программном обеспечении;
- анализа потока обращений пользователей к информации (даже если информация остается скрытой) для отработки методов доступа.

К активным способам реализации угроз безопасности информации программными средствами относятся способы, основанные на:
- обходе существующих механизмов защиты;
- несанкционированном расширении своих полномочий по доступу к информации;
- модификации программного обеспечения путем добавления новых функций;
- блокировании работы прикладного или общесистемного программного обеспечения;
- скрытой передачи некоторой информации путем размещения ее в разрешенной информации;
- изменении протокола регистрации работ для навязывания ложной информации.

Активные действия злоумышленника могут приводить к разрушению вычислительных средств, а также к навязыванию ложной информации, такой, как:
- отказ от факта формирования (передачи) информации
- утверждение о приеме информации от некоторого пользователя, хотя на самом деле она сформирована нарушителем;
- утверждение о том, что получателю в определенный момент времени была отправлена информация, которая на самом деле не отправлялась (или отправлялась в другой момент времени);
- отказ от факта получения информации, которая на самом деле была получена, или выдача ложных сведений о времени ее получения.

В общем случае план реализации доступа к информации вырабатывается злоумышленником на основании оценки следующих исходных факторов:
- уровень знаний и опыта злоумышленника в области нарушения безопасности информации;
- тематическая направленность интересующей информации;
- сведения о системе охранных мер;
- данные о недостатках средств безопасности информации;
- техническая и программная оснащенность средствами нарушения безопасности информации;
- возможность доступа к техническим средствам и их коммуникациям, являющимся источниками информативного сигнала;
- возможность доступа к программному обеспечению;

- сведения о шаблонах сообщений, типах кодов, используемых в различных технических средствах, но являющихся скрытыми, т.к., они собираются на основе массово-серийной аппаратуры, характеристики которой известны.

Общие принципы обеспечения защиты информационных систем и технологий в экономике и торговле. Безопасность – это состояние, при котором отсутствует возможность причинения ущерба потребностям и интересам субъектов отношений.

Угроза безопасности – это совокупность условий и факторов, создающих опасность жизненно важным интересам.

Обеспечение безопасности – это особым образом организованная деятельность, направленная на сохранение внутренней устойчивости объекта, его способности противостоять разрушительному, агрессивному воздействию различных факторов, а также на активное противодействие существующим видам угроз.

Принципы создания и функционирования систем безопасности можно разбить на три блока: общие принципы обеспечения защиты, организационные принципы, принципы реализации системы защиты.

Общие принципы обеспечения защиты. Принцип неопределенности. Принцип неопределенности обусловлен тем, что при обеспечении защиты неизвестно, кто, когда, где и каким образом попытается нарушить безопасность объекта защиты.

Принцип невозможности создания идеальной системы защиты. Этот принцип следует из принципа неопределенности и ограниченности ресурсов, которыми, как правило, располагает система безопасности.

Принцип минимального риска. Заключается в том, что при создании системы защиты необходимо выбирать минимальную степень риска, исходя из особенностей угроз безопасности, доступных ресурсов и конкретных условий, в которых находится объект защиты в любой момент времени.

Принцип защиты всех от всех. Данный принцип предполагает необходимость защиты всех субъектов отношений против всех видов угроз.

Организационные принципы.

Принцип законности. Важность соблюдения этого очевидного принципа трудно переоценить. Однако с возникновением новых правоотношений в российском законодательстве наряду с хорошо знакомыми объектами права такими, как "государственная собственность", "государственная тайна", появились новые - "частная собственность", "собственность предприятия", "интеллектуальная собственность", "коммерческая тайна", "конфиденциальная информация", "информация с ограниченным доступом". Нормативная правовая база, регламентирующая вопросы обеспечения безопасности, пока несовершенна.

Принцип персональной ответственности. Каждый сотрудник предприятия, фирмы или их клиент несет персональную ответственность за обеспечение режима безопасности в рамках своих полномочий или соответствующих инструкций. Ответственность за нарушение режима безопасности должна быть заранее конкретизирована и персонифицирована.

Принцип разграничения полномочий. Вероятность нарушения коммерческой тайны или нормального функционирования предприятия прямо пропорциональна количеству осведомленных лиц, обладающих информацией. Поэтому никого не следует знакомить с конфиденциальной информацией, если это не требуется для выполнения его должностных обязанностей.

Принцип взаимодействия и сотрудничества. Внутренняя атмосфера безопасности достигается доверительными отношениями между сотрудниками. При этом необходимо добиваться того, чтобы персонал предприятия правильно понимал необходимость выполнения мероприятий, связанных с обеспечением безопасности, и в своих собственных интересах способствовал деятельности службы безопасности.

Принципы реализации системы защиты

Принцип комплексности и индивидуальности. Безопасность объекта защиты не обеспечивается каким-либо одним мероприятием, а лишь совокупностью комплексных, взаимосвязанных и дублирующих друг друга мероприятий, реализуемых с индивидуальной привязкой к конкретным условиям.

Принцип последовательных рубежей. Реализация данного принципа позволяет своевременно обнаружить посягательство на безопасность и организовать последовательное противодействие угрозе в соответствии со степенью опасности.

Принцип защиты средств защиты. Данный принцип является логическим продолжением принципа защиты "всех от всех". Иначе говоря, любое мероприятие по защите само должно быть соответственно защищено. Например, средство защиты от попыток внести изменения в базу данных должно быть защищено программным обеспечением, реализующим разграничение прав доступа. Обеспечение комплексной защиты объектов является в общем случае индивидуальной задачей, что обусловлено экономическими соображениями, состоянием, в котором находится объект защиты, и многими другими обстоятельствами.

Прежде чем приступить к созданию системы безопасности, необходимо определить объекты защиты, уничтожение, модификация или несанкционированное использование которых может привести к нарушению интересов, убыткам и пр. Определив объекты защиты, следует выявить сферы их интересов и проанализировать множество угроз безопасности объектов защиты. Если угрозы безопасности преднамеренные, то необходимо разработать предполагаемую модель злоумышленника. Далее нужно

проанализировать возможные угрозы и источники их возникновения, выбрать адекватные средства и методы защиты и таким образом сформулировать задачи и определить структуру системы обеспечения безопасности.

Литература

1. Основы государственной политики в области безопасности // Проблемы безопасности при чрезвычайных ситуациях. Вып. 2 – М.: ВИНИТИ, 2000.

2. Порфирьев Б.Н. Организация управления в чрезвычайных ситуациях. – М.: Знание, 1989.

3. Нейман Д., Моргенштерн О. Теория игр и экономическое поведение. – М.: Наука, 1970.

4. Новиков Д.А. Институциональное управление организационными системами. – М.: ИПУ РАН, 2003.