Негосударственное образовательное учреждение
Высшего профессионального образования
"Институт государственного администрирования"
Юридический факультет

Реферат

по дисциплине

Информационная безопасность

на тему:

"Информационная безопасность и методы её обеспечения"

Выполнил: Аксенов Валерий Дмитриевич

Казань – 2015

Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Информационная безопасность организации – состояние защищенности информационной среды организации, обеспечивающее её формирование, использование и развитие.

В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т.п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью [2; 22].

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

- Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;
- Целостность – избежание несанкционированной модификации информации;
- Доступность – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

- неотказуемость или апеллируемость – невозможность отказа от авторства;
- подотчётность – обеспечение идентификации субъекта доступа и

регистрации его действий;

- достоверность – свойство соответствия предусмотренному поведению или результату;
- аутентичность или подлинность – свойство, гарантирующее, что субъект или ресурс идентичны заявленным [3; 39].

Действия, которые могут нанести ущерб информационной безопасности организации, можно разделить на несколько категорий:

1. Действия, осуществляемые авторизованными пользователями. В эту категорию попадают: целенаправленная кража или уничтожение данных на рабочей станции или сервере; повреждение данных пользователей в результате неосторожных действий.

2. "Электронные" методы воздействия, осуществляемые хакерами. Под хакерами понимаются люди, занимающиеся компьютерными преступлениями как профессионально (в том числе в рамках конкурентной борьбы), так и просто из любопытства. К таким методам относятся: несанкционированное проникновение в компьютерные сети; DOS-атаки.

Целью несанкционированного проникновения извне в сеть предприятия может быть нанесение вреда (уничтожения данных), кража конфиденциальной информации и использование ее в незаконных целях, использование сетевой инфраструктуры для организации атак на узлы третьих фирм, кража средств со счетов и т.п.

Атака типа DOS (сокр. от Denial of Service – "отказ в обслуживании") − это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работу (файловые, почтовые сервера). Злоумышленники организуют массированную отправку пакетов данных на эти узлы, чтобы вызвать их перегрузку и, в итоге, на какое-то время вывести их из строя. Это, как правило, влечет за собой нарушения в бизнес-процессах компании-жертвы, потерю клиентов, ущерб репутации и т.п.

3. Компьютерные вирусы. Отдельная категория электронных методов воздействия − компьютерные вирусы и другие вредоносные программы. Они

представляют собой реальную опасность для современного бизнеса, широко использующего компьютерные сети, интернет и электронную почту. Проникновение вируса на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств. Вирусная программа, проникшая в корпоративную сеть, может предоставить злоумышленникам частичный или полный контроль над деятельностью компании.

4. Спам. Всего за несколько лет спам из незначительного раздражающего фактора превратился в одну из серьезнейших угроз безопасности: электронная почта в последнее время стала главным каналом распространения вредоносных программ; спам отнимает массу времени на просмотр и последующее удаление сообщений, вызывает у сотрудников чувство психологического дискомфорта; как частные лица, так и организации становятся жертвами мошеннических схем, реализуемых спамерами; вместе со спамом нередко удаляется важная корреспонденция, что может привести к потере клиентов, срыву контрактов и другим неприятным последствиям; опасность потери корреспонденции особенно возрастает при использовании черных списков RBL и других "грубых" методов фильтрации спама.

5. "Естественные" угрозы. На информационную безопасность компании могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства и т.д.

Таким образом, в современных условиях наличие развитой системы информационной безопасности становится одним из важнейших условий конкурентоспособности и даже жизнеспособности любой компании.

Информационная безопасность и Интернет

Общение с использованием новейших средств коммуникации вобрал в себя Интернет. Всемирная информационная сеть развивается большими

темпами, количество участников постоянно растет. По некоторым данным, в сети зарегистрировано около 1,5 миллиарда страниц. Некоторые "живут" до полугода, а некоторые работают на своих владельцев в полную силу и приносят большую прибыль. Информация в сети охватывает все стороны жизнедеятельности человека и общества. Пользователи доверяют этой форме себя и свою деятельность. Однако опыт работы в области компьютерных технологий полон примеров недобросовестного использования ресурсов Интернет.

Специалисты говорят, что главная причина проникновения в компьютерные сети – беспечность и неподготовленность пользователей. Это характерно не только для рядовых пользователей, но и для специалистов в области компьютерной безопасности. Вместе с тем, причина не только в халатности, но и в сравнительно небольшом опыте специалистов по безопасности в сфере информационных технологий. Связано это со стремительным развитием рынка сетевых технологий и самой сети Интернет.

По данным лаборатории Касперского, около 90% от общего числа проникновений на компьютер вредоносных программ используется посредством Интернет, через электронную почту и просмотр Web-страниц. Особое место среди таких программ занимает целый класс – Интернет-червь. Само распространяющиеся, не зависимо от механизма работы выполняют свои основные задачи по изменению настроек компьютера-жертвы, воруют адресную книгу или ценную информацию, вводят в заблуждение самого пользователя, создают рассылку с компьютера по адресам, взятым из записной книжки, делают компьютер чьим-то ресурсом или забирают часть ресурсов для своих целей или в худшем случае самоликвидируются, уничтожая все файлы на всех дисках.

Все эти и другие с ними связанные проблемы можно решить с помощью наличия в организации проработанного документа, отражающего политику информационной безопасности компании. В таком документе должны быть четко прописаны следующие положения:

- как ведется работа с информацией предприятия;
- кто имеет доступ;
- система копирования и хранения данных;
- режим работы на ПК;
- наличие охранных и регистрационных документов на оборудование и программное обеспечение;
- выполнение требований к помещению, где располагается ПК и рабочее место пользователя;
- наличие инструкций и технической документации;
- наличие рабочих журналов и порядок их ведения.

Кроме того, необходимо постоянно отслеживать развитие технических и информационных систем, публикуемых в периодической печати или следить за событиями, обсуждаемыми на подобных семинарах.

Так согласно Указа Президента РФ "О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена", запрещено подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются госорганы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу РФ, в том числе к Интернету.

При необходимости подключения указанных информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств,

прошедших в установленном законодательством РФ порядке сертификацию в Федеральной службе безопасности РФ и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю [1].

Методы обеспечения информационной безопасности

По убеждению экспертов "Лаборатории Касперского", задача обеспечения информационной безопасности должна решаться системно. Это означает, что различные средства защиты (аппаратные, программные, физические, организационные и т.д.) должны применяться одновременно и под централизованным управлением. При этом компоненты системы должны "знать" о существовании друг друга, взаимодействовать и обеспечивать защиту, как от внешних, так и от внутренних угроз.

На сегодняшний день существует большой арсенал методов обеспечения информационной безопасности [6; 275]:

- средства идентификации и аутентификации пользователей (так называемый комплекс 3А);
- средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;
- межсетевые экраны;
- виртуальные частные сети;
- средства контентной фильтрации;
- инструменты проверки целостности содержимого дисков;
- средства антивирусной защиты;
- системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Каждое из перечисленных средств может быть использовано как самостоятельно, так и в интеграции с другими. Это делает возможным создание систем информационной защиты для сетей любой сложности и конфигурации, не зависящих от используемых платформ.

"Комплекс 3А" включает аутентификацию (или идентификацию),

авторизацию и администрирование. Идентификация и авторизация − это ключевые элементы информационной безопасности. При попытке доступа к информационным активам функция идентификации дает ответ на вопрос: "Кто вы?" и "Где вы?" − являетесь ли вы авторизованным пользователем сети. Функция авторизации отвечает за то, к каким ресурсам конкретный пользователь имеет доступ. Функция администрирования заключается в наделении пользователя определенными идентификационными особенностями в рамках данной сети и определении объема допустимых для него действий.

Системы шифрования позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам. Задача данного средства защиты – обеспечение конфиденциальности. Основные требования, предъявляемые к системам шифрования – высокий уровень криптостойкости и легальность использования на территории России (или других государств).

Межсетевой экран представляет собой систему или комбинацию систем, образующую между двумя или более сетями защитный барьер, предохраняющий от несанкционированного попадания в сеть или выхода из нее пакетов данных.

Основной принцип действия межсетевых экранов − проверка каждого пакета данных на соответствие входящего и исходящего IP-адреса базе разрешенных адресов. Таким образом, межсетевые экраны значительно расширяют возможности сегментирования информационных сетей и контроля за циркулированием данных.

Говоря о криптографии и межсетевых экранах, следует упомянуть о защищенных виртуальных частных сетях (Virtual Private Network – VPN). Их использование позволяет решить проблемы конфиденциальности и целостности данных при их передаче по открытым коммуникационным каналам. Использование VPN можно свести к решению трех основных задач:

1. защита информационных потоков между различными офисами компании (шифрование информации производится только на выходе во внешнюю сеть);

2. защищенный доступ удаленных пользователей сети к информационным ресурсам компании, как правило, осуществляемый через интернет;

3. защита информационных потоков между отдельными приложениями внутри корпоративных сетей (этот аспект также очень важен, поскольку большинство атак осуществляется из внутренних сетей).

Эффективное средство защиты от потери конфиденциальной информации − фильтрация содержимого входящей и исходящей электронной почты. Проверка самих почтовых сообщений и вложений в них на основе правил, установленных в организации, позволяет также обезопасить компании от ответственности по судебным искам и защитить их сотрудников от спама. Средства контентной фильтрации позволяют проверять файлы всех распространенных форматов, в том числе сжатые и графические. При этом пропускная способность сети практически не меняется.

Все изменения на рабочей станции или на сервере могут быть отслежены администратором сети или другим авторизованным пользователем благодаря технологии проверки целостности содержимого жесткого диска (integrity checking). Это позволяет обнаруживать любые действия с файлами (изменение, удаление или же просто открытие) и идентифицировать активность вирусов, несанкционированный доступ или кражу данных авторизованными пользователями. Контроль осуществляется на основе анализа контрольных сумм файлов (CRC-сумм).

Современные антивирусные технологии позволяют выявить практически все уже известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе. Кроме того, разработаны технологии моделирования поведения, позволяющие обнаруживать вновь создаваемые вирусные программы.

Обнаруживаемые объекты могут подвергаться лечению, изолироваться (помещаться в карантин) или удаляться. Защита от вирусов может быть установлена на рабочие станции, файловые и почтовые сервера, межсетевые экраны, работающие под практически любой из распространенных операционных систем (Windows, Unix- и Linux-системы, Novell) на процессорах различных типов.

Фильтры спама значительно уменьшают непроизводительные трудозатраты, связанные с разбором спама, снижают трафик и загрузку серверов, улучшают психологический фон в коллективе и уменьшают риск вовлечения сотрудников компании в мошеннические операции. Кроме того, фильтры спама уменьшают риск заражения новыми вирусами, поскольку сообщения, содержащие вирусы (даже еще не вошедшие в базы антивирусных программ) часто имеют признаки спама и отфильтровываются. Правда, положительный эффект от фильтрации спама может быть перечеркнут, если фильтр наряду с мусорными удаляет или маркирует как спам и полезные сообщения, деловые или личные.

Для противодействия естественным угрозам информационной безопасности в компании должен быть разработан и реализован набор процедур по предотвращению чрезвычайных ситуаций (например, по обеспечению физической защиты данных от пожара) и минимизации ущерба в том случае, если такая ситуация всё-таки возникнет. Один из основных методов защиты от потери данных – резервное копирование с четким соблюдением установленных процедур (регулярность, типы носителей, методы хранения копий и т.д.) [5; 382].

Литература

1. Указ Президента РФ "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" от 17.03.2008 №351;
2. Галатенко, В.А. Основы информационной безопасности. Интернет-университет информационных технологий − ИНТУИТ.ру, 2008;
3. Галатенко, В.А. Стандарты информационной безопасности. Интернет-университет информационных технологий − ИНТУИТ.ру, 2005;
4. Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2000. – 428 с;
5. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. − М.: ДМК Пресс, 2008. – 544 с.
6. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. − М.: Книжный мир, 2009. – 352 с.