Реферат

Дисциплина: Информационная безопасность

Выполнила: Афтаева Ксения Васильевна

Содержание

# 1 Введение

За последние годы, компьютерные технологии тесно вошли в нашу жизнь. Людям в наше время довольно сложно представить свой день без компьютеров. С доступностью компьютеров, люди также стали активно пользоваться услугами сети Интернет – электронной почтой, Всемирной паутиной, интернет-банкингом. Теперь каждое утро среднестатистического человека начинается со стандартного просмотра ленты новостей, проверки содержимого личной почты, посещения различных популярных социальных сетей, покупки в интернет-магазинах, оплаты различных услуг и т.п.. Интернет медленно, но верно, стал постоянным помощником в наших повседневных делах.

Но при всех достоинствах компьютерных технологий, существует и масса опасностей. Прежде всего, это угрозы личной и государственной безопасности.

Несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным.

Таким образом, угроза информационной безопасности является одной из важнейших проблем современной жизни человека и нам необходимо знать, откуда она возникает и как нам себя обезопасить.

# 2 Информация и ее виды

Говорить о защите информации нельзя без самого понятия информации.

Информация – это осознанные сведения (знания, выраженные в сигналах, сообщениях, известиях, уведомлениях и т.д.) об окружающем мире, которые являются объектом хранения, преобразования, передачи и использования.

Различают основные виды информации, которые классифицируют по ее форме представления, способам ее кодирования и хранения:

* графическая – один из древнейших видов, с помощью которого хранили информацию об окружающем мире в виде наскальных рисунков, а затем в виде картин, фотографий, схем, чертежей на различных материалах (бумага, холст, мрамор и др.), которые изображают картины реального мира;
* звуковая (акустическая) – для хранения звуковой информации в 1877 г. было изобретено звукозаписывающее устройство, а для музыкальной информации – разработан способ кодирования с использованием специальных символов, который дает возможность хранить ее как графическую информацию;
* текстовая – кодирует речь человека с помощью специальных символов – букв (для каждого народа свои); для хранения используется бумага (записи в тетради, книгопечатание и т.п.);
* числовая – кодирует количественную меру объектов и их свойств в окружающем мире с помощью специальных символов – цифр (для каждой системы кодирования свои); особенно важной стала с развитием торговли, экономики и денежного обмена;
* видеоинформация – способ хранения «живых» картин окружающего мира, который появился с изобретением кино.

Информация, как и любой объект, обладает свойствами, наиболее важными из которых являются: объективность, достоверность, полнота, акутальность и ценность.

# 3 Право собственности на информацию

Информация – это объект права собственности. Владеть информацией могут, как физические, так и юридические лица, а также государство. Она является собственностью организаций, фирм, компаний, органов государственной власти и частных лиц.

Специфическими свойствами информации как объекта собственности являются:

* право информационной собственности имеет материальную основу, т. е. оно является вещным правом;
* информация подлежит использованию, копированию, передаче, восстановлению посредством применения материальных носителей;
* право собственности на информацию обеспечивает владение ею, распоряжение и использование для решения необходимых задач, достижения конкретных целей собственника информации;
* возможна передача прав собственности на информацию ее владельцем, без потери собственных прав на информацию;
* использование информации всегда реализуется в интересах собственника.

Право собственности, распространяемое на защищаемую информацию, подразумевает единство трех прав:

* права владения собственностью;
* права распоряжения ею;
* права ее использования.

Право владения по отношению к информации, точнее, ее содержанию, может означать право знать это содержание.

Право пользования информацией (ее содержанием), может означать право применять информацию в собственной личной деятельности, главным образом для принятия решений и управления.

Право распоряжения информацией в смысле ее гражданского оборота, т.е. с целью реализации исключительного права на это содержание может означать право тиражировать и распространять информацию, прежде всего, в коммерческих целях.

# 4 Ценность информации

Информационные системы требуют защиты именно потому, что обрабатываемая информация бывает ценной не зависимо от происхождения. Реализация любой из угроз может привести к нарушению свойств конфиденциальности, целостности или доступности. При этом собственник информации несет определенные потери, связанные с нарушением этих свойств.

Под ценностью информации понимается ее свойство, характеризующее потери собственника данной информации при реализации определенной угрозы, выраженное в стоимостном, временном либо ином эквиваленте.

Ценность информации меняется во времени. Распространение информации и ее использование приводят к изменению ее ценности.

Ценность большинства видов информации со временем уменьшается - информация стареет. Уменьшается она также и при незаконном распространении.

Только некоторые виды конфиденциальной информации могут сохранять свою потребительскую стоимость на протяжении длительного периода времени. Это информация о состоявшихся фактах, событиях и явлениях, которые остались тайной для многих (например, государственная тайна).

# 5 Угрозы информационной безопасности

Важно отметить, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной (СМИ); однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Итак, угрозы информационной (компьютерной) безопасности — это различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это — потенциально возможные события, процессы или действия, которые могут нанести ущерб информационным и компьютерным системам.

Специалисты выделяют три основных вида угроз в отношении информационных систем:

* угроза нарушения конфиденциальности (в связи с этой угрозой нередко используется термин «утечка»);
* угроза нарушения целостности;
* угроза нарушения доступности.

Угроза, относящаяся к первому виду, возможна в тех случаях, когда информация, которая содержится в информационной системе или передается от одной системы к другой, становится известной в результате несанкционированного доступа лицу, не обладающему правом доступа к ее использованию.

Относящаяся ко второму виду угроза может реализоваться в случае незаконного изменения информации, которая находится в информационной системе или передается из одной системы в другую. Говорить о нарушении целостности информации следует в тех случаях, когда информация преднамеренно изменена злоумышленниками.

В случае допущенной ошибки в программном обеспечении также возможно нарушение целостности информации, если такая ошибка приводит к ее незаконному изменению.

Если корректировка части базы данных проводится уполномоченными на то сотрудниками на законных основаниях, то такие изменения не будут рассматриваться, как незаконные.

Угроза третьего вида может реализоваться в виде блокировки доступа к ресурсу вычислительной системы, предпринятого в результате преднамеренного вмешательства злоумышленником, а возможно другим пользователем.

Если запрашиваемый ресурс перестанет быть доступным, то можно говорить о том, что он блокирован на постоянной основе, в других случаях возможна только задержка в доступе.

Перечисленные выше виды угроз относят к непосредственным, или первичным. Осуществление таких угроз ведет к изменениям в защищаемой информации. В данном случае угроза рассматривается как потенциальная опасность, ведущая к нанесению ущерба информационной системе.

К основным угрозам безопасности относят:

* раскрытие конфиденциальной информации;
* компрометация информации;
* несанкционированное использование информационных ресурсов.

# 6 Причины возникновения информационных угроз

Информационные угрозы можно классифицировать, например, по природе возникновения на естественные (связанные с природными явлениями) и искусственные, то есть те, которые вызваны деятельностью человека.

Угрозы, вызванные деятельностью человека можно разделить на два вида:

* непреднамеренные угрозы, то есть случайные, неумышленные угрозы, связанны с ошибками обслуживающего персонала, а также ошибками в программном обеспечении и ошибками в проектировании компьютерной;
* преднамеренные угрозы, то есть связанные с корыстными намерениями злоумышленников.

Угрозы, носящие случайный, неумышленный характер связаны с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны, для воссоединения с семьей и т.п.) Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные пр01раммы и др.) с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации).

Угрозы, обусловленные умышленными, преднамеренными действиями людей связаны с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий но корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научнотехнических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний информации (например, в связи с получением другого гражданства по корыстным мотивам). Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение носителей информации: дискет, описаний, распечаток и др.).

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы, искажение сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы также подразделяются на внутренние, возникающие внутри управляемой организации, и внешние.

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами

# 7 Выводы

Жизнь современного общества немыслима без современных информационных технологий, но высокая степень автоматизации порождает риск снижения безопасности (личной, информационной, государственной, и т. п.).

Информационные угрозы связаны с их деструктивным влиянием на качественные показатели информации или информационного обслуживания, такие как достоверность, актуальность, целостность, полнота представления, ценность, а также своевременность подачи (получения).

Использование информационных технологий вводит в нашу жизнь новые формы преступной деятельности.

В целях максимальной защиты отдельных граждан и общества в целом необходимо постоянно изучать возникающие проблемы, несущие угрозы принимать действенные меры по обеспечению общественной и государственной безопасности, своевременно выявлять опасные явления в информационных пространствах и оперативно противодействовать им.

# Список литературы