Реферат на тему:

**Обеспечение информационной безопасности на промышленном предприятии**

­Выполнил: студент 402 группы

Батунин М. Е.

**Содержание**

|  |  |
| --- | --- |
| 1. Введение |  |
| 1. Понятие информационной безопасности |  |
| 1. Основные угрозы информационной безопасности |  |
| 1. Методы обеспечения информационной безопасности |  |
| 1. Средства обеспечения информационной безопасности |  |
| 1. Автоматизированная система управления технологическим процессом (АСУ ТП) на промышленном предприятии |  |
| 1. Уязвимости АСУ ТП |  |
| 1. Общий подход к разработке комплексной защиты |  |
| 1. Источники |  |

**Введение**

Конфиденциальная информация представляет огромный интерес для конкурирующих фирм. Именно она становится причиной посягательств со стороны злоумышленников.

Многие проблемы связаны с недооценкой важности угрозы, в результате чего для предприятия это может обернуться крахом и банкротством. Даже единичный случай халатности рабочего персонала может принести компании многомиллионные убытки и потерю доверия клиентов.

Угрозам подвергаются данные о составе, статусе и деятельности компании. Источниками таких угроз являются её конкуренты, коррупционеры и преступники. Особую ценность для них представляет ознакомление с охраняемой информацией, а также ее модификация в целях причинения финансового ущерба.

К такому исходу может привести утечка информации даже на 20%. Иногда потеря секретов компании может произойти случайно, по неопытности персонала или из-за отсутствия систем защиты.

**Понятие информационной безопасности**

В повседневной жизни часто информационная безопасность (ИБ) понимается лишь как необходимость борьбы с утечкой секретной и распространением ложной и враждебной информации. Однако, это понимание очень узкое. Существует много разных определений информационной безопасности, в которых высвечиваются отдельные её свойства.

В утратившем силу ФЗ «Об информации, информатизации и защите информации» под информационной безопасностью понималось *состояние защищённости информационной среды общества, обеспечивающее её формирование и развитие в интересах граждан, организаций и государства*.

В других источниках приводятся следующие определения:

**Информационная безопасность** – это

1) комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с её доступностью для всех авторизованных пользователей;

2) показатель, отражающий статус защищенности информационной системы;

3) состояние защищённости информационной среды;

4) состояние, обеспечивающее защищенность информационных ресурсов и каналов, а также доступа к источникам информации.

В. И. Ярочкин считает, что **информационная безопасность** есть состояние защищённости информационных ресурсов, технологии их формирования и использования, а также прав субъектов информационной деятельности.

Достаточно полное определение дают В. Бетелин и В. Галатенко, которые полагают, что

**Информационная безопасность** –защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.

ИБ не сводится исключительно к защите информации и компьютерной безопасности. Следует различать информационную безопасность от *защиты информации*.

**Защита информации** – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Иногда под защитой информации понимается создание в ЭВМ и вычислительных системах организованной совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации.

Меры по обеспечению информационной безопасности должны осуществляться в разных сферах – политике, экономике, обороне, а также на различных уровнях – государственном, региональном, организационном и личностном. Поэтому задачи информационной безопасности на уровне государства отличаются от задач, стоящих перед информационной безопасностью на уровне организации.

**Основные угрозы информационной безопасности**

Под угрозой информационной безопасности понимается случайная или преднамеренная деятельность людей или физическое явление, которые могут привести к нарушению безопасности информации. Далее рассмотрены основные виды и аспекты угроз информационной безопасности.

Все множество потенциальных угроз информационной безопасности по природе их возникновения можно разделить на два класса естественные (объективные) и искусственные (субъективные).

Угрозы безопасности

Естественные

Искусственные

Непреднамеренные

Преднамеренные

*Естественные угрозы* – это угрозы, вызванные воздействиями на автоматизированную систему и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

*Искусственные угрозы* – это угрозы информационной безопасности, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

1. *Непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками в проектировании автоматизированной системы и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.

2. *Преднамеренные* (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к автоматизированной системе могут быть внешними или внутренними. Внутренние угрозы реализуются компонентами самой информационной системы – аппаратно-программным обеспечением или персоналом.

К основным непреднамеренным искусственным угрозам информационной безопасности относятся действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла:

1. Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.).

2. Неправомерное отключение оборудования или изменение режимов работы устройств и программ.

3. Неумышленная порча носителей информации.

4. Запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.).

5. Нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях).

6. Заражение компьютера вирусами.

7. Неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной.

8. Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков).

9. Проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации.

10. Игнорирование организационных ограничений (установленных правил) при работе в системе.

11. Вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.).

12. Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности.

13. Пересылка данных по ошибочному адресу абонента (устройства).

14. Ввод ошибочных данных.

15. Неумышленное повреждение каналов связи.

К основным преднамеренным искусственным угрозам относятся:

1. Физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.).

2. Отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и др.).

3. Действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.).

4. Внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность).

5. Вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия.

6. Применение подслушивающих устройств, дистанционная фото и видеосъемка и т.п.

7. Перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.).

8. Перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему.

9. Хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ).

10. Несанкционированное копирование носителей информации.

11. Хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.).

12. Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.

13. Чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования.

14. Незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»).

15. Несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.

16. Вскрытие шифров криптозащиты информации.

17. Внедрение аппаратных спец вложений, программных закладок и вирусов, т.е. таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы.

18. Незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений.

19. Незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

**Методы обеспечения информационной безопасности**

Основными методами защиты информации являются следующие.

1. Препятствие — метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

2. Управление доступом — метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы банковской деятельности (элементов баз данных, программных и технических средств). Управление доступом включает следующие функции защиты:

* идентификацию пользователей, персонала и ресурсов системы
* опознание
* проверку полномочий
* разрешение и создание условий работы в пределах установленного регламента
* регистрацию (протоколирование) обращений к защищаемым ресурсам
* реагирование (сигнализация, отключение, задержка работ, отказ в запросе) на попытки несанкционированных действий с информацией

3. Маскировка — метод защиты информации путем ее криптографического закрытия или её сокрытия, т.е. обеспечения невозможности её найти.

4. Регламентация — метод защиты информации, создающий за счёт организации работ такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

5. Принуждение — такой метод защиты, при котором пользователи и персонал системы вынуждены соблюдать регламенты и правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

6. Побуждение — такой метод защиты, который мотивирует пользователя и персонал системы не разрушать установленные регламенты и порядки за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных).

Перечисленные методы обеспечения безопасности реализуются разными средствами, но сущность этих методов остаётся сходной.

**Средства обеспечения информационной безопасности**

Средства обеспечения безопасности – это ресурсы, обеспечивающие безопасность.

К основным средствам защиты, используемым для создания механизма защиты, относятся следующие:

1. *Технические средства* реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические. Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу.

2. *Физические средства* реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

3. *Программные средства* представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

4. *Организационные средства* защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного.

5. *Морально-этические средства* защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в обществе. Эти нормы большей частью не являются обязательными как законодательные меры, однако, несоблюдение их ведет обычно к потере авторитета и престижа человека. Наиболее показательным примером таких норм является Кодекс профессионального поведения членов Ассоциаций пользователей ЭВМ США.

6. *Законодательные средства* защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

**Источники**

1. Гафнер В.В. Информационная безопасность: учеб. пособие / В.В. Гафнер. – Ростов на Дону: Феникс, 2010. - 324 с.
2. Интернет источник. Ссылка: https://studfiles.net/preview/5785046/