**Утверждено**

**Правлением КБ “Event-компания” (ООО)**

**Протокол № XX/2002**

**От " XX " xxxxxxxx 2002 г.**

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В КБ «Event-компания» (ООО)

## Объекты защиты

Понятие информации как объекта правовой защиты регулируется законами и кодексами. Среди них есть закон «Об информации, информационных технологиях и защите информации», Гражданский кодекс, закон «О защите персональных данных» и другие.

В деятельности event-компании образуются следующие объекты информации:

* персональные данные сотрудников компании и клиентов. Эта информация может включать: данные о доходах, данные кредитных карт, номера автомобилей и т.д.;
* данные о месте, времени, продолжительности, стоимости, количестве посетителей, тема события и т.д., которая может быть использована в плохих целях;

Вся эта информация содержится как на бумажных, так и на электронных носителях. Эти данные могут стать объектом противоправного покушения, и использоваться в различных целях. Их сохранность требует принятия серьезных мер безопасности. Несанкционированный доступ к охраняемым законом сведениям является уголовным преступлением.

## 1.2 Виды угроз и их источники

Угроза безопасности - потенциальное нарушение безопасности, любое обстоятельство или событие, которое может стать причиной нанесения ущерба всему предприятию.

Перечень угроз безопасности включает атаки как внешнего, так и внутреннего происхождения. Информационные базы данных, принадлежащие страховым компаниям, часто становятся объектами покушений хакеров. Частыми целями преступных посягательств являются клиентские базы данных, содержащие информацию о номерах телефонов, номерах автомобилей, медицинских историях. В ряде случаев мошенники, используя данные, похищенные у страховщиков, создавали сайты-клоны.

Кроме того, не исключен риск заражения компьютерных систем компании различными вирусами, которые могут причинить существенный ущерб в виде:

* блокировки доступа к важным файлам;
* уничтожения файлов;
* передачи информации третьим лицам.

Не всегда установленный антивирус будет обеспечивать полную защиту от внешних угроз. Кроме внешней угрозы проникновения в компьютерные сети компании существуют и внутренние. Отдельные сотрудники могут намеренно похищать любую информацию с целью ее распространения или передачи конкурентам.

Основные непреднамеренные искусственные угрозы предприятию (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

* 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.);
* неправомерное отключение оборудования или изменение режимов работы устройств и программ;
* неумышленная порча носителей информации;
* 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.);
* 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);
* заражение компьютера вирусами;
* неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
* разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
* проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
* игнорирование организационных ограничений (установленных правил) при работе в системе;
* вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
* некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
* пересылка данных по ошибочному адресу абонента (устройства);
* ввод ошибочных данных;
* неумышленное повреждение каналов связи.

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

* 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.);
* отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
* 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.);
* вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
* применение подслушивающих устройств, дистанционная фото- и видеосъемка, и т.п.;
* 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, сели питания, отопления и т.п.);
* 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;
* хищение носителей информации;
* несанкционированное копирование носителей информации;
* хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
* чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
* чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой зашиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;
* 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»);
* 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.;
* вскрытие шифров криптозащиты информации;
* 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;
* 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.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

## 1.3 Разработка мер защиты

Для предотвращения угроз, связанных с кражей, нападением, взломом, проникновением в отделение компании, нужно предусмотреть:

* наличие охраны;
* наличие системы видеонаблюдения/аудиозаписи;
* наличие пропускной системы с возможностью идентификации;

Для предотвращения технических и аппаратных угроз рекомендуется:

* наличие отдела, отвечающего за ремонт технических средств;
* использовать и регулярно обновлять лицензионное антивирусное программное обеспечение;
* использовать защиту электронного почтового ящика (отключить предварительный просмотр);
* не открывать вложенные данные от сомнительных источников;
* при передаче данных по сети, использовать только защищённые каналы и предварительно проходить аутентификацию (все клиенты канала должны это сделать);
* производить обязательное шифрование данных, при передаче по каналам связи посредством криптографических методов;
* производить контроль за количеством исходящего и входящего трафика, а также ограничивать доступ к неизвестным и сомнительным ресурсам;
* ведение логирования как в плане ОС, так и в сетевом плане;
* поддержание средств защиты и работы с информацией в актуальном состоянии (своевременное обновление);
* правильная настройка и конфигурация сетевых средств (маршрутизаторы и т.д.);

|  |  |  |  |
| --- | --- | --- | --- |
| Атака | Ущерб | Вероятность | Риск |
| Кражи, нападения, взлом, саботаж и проникновение | 4 | 0,1 | 0,4 |
| Отказы и неисправности технических средств | 1 | 0,3 | 0,3 |
| Окончание строка лицензионного соглашения на антивирусные продукты | 1 | 0,2 | 0,2 |
| Вирусная атака на электронную почту | 2 | 0,3 | 0,6 |
| Несанкционированный доступ к каналам связи | 4 | 0,3 | 1.2 |
| Отказ в обслуживании (Denial of Service - DoS) | 2 | 0,3 | 0,6 |
| Взлом метода шифрования | 4 | 0,3 | 1.2 |
| Отсутствие фильтрующих и антивирусных стредств | 4 | 0.3 | 1.2 |

## 1.4 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

Стандарты защиты информации предусмотрены стандартами и нормами. Кроме того, информационная безопасность event-компании должна обеспечиваться целым комплексом мер, среди которых:

* административные;
* организационные;
* технические.

Все они должны применяться совместно. Опираться система защиты должна на управление персоналом компании и контроль над ним. Меры технического характера не менее важны, но не могут существовать в отрыве от организационных мер.

Административные меры безопасности.

Эти способы защиты включают в себя разработку внутренних нормативных документов, обеспечивающих информирование сотрудников о действиях, необходимых для обеспечения информационной безопасности.

Служба безопасности компании разрабатывает и предлагает на утверждение руководства политику защиты конфиденциальной информации. Этот локальный нормативный акт должен содержать:

* основные принципы защиты конфиденциальной информации в компании;
* обязанности каждого сотрудника в части защиты доверенных ему сведений;
* задачи руководства по обеспечению охраны информации;
* регламенты обращения с компьютерной техникой и средствами коммуникации;
* меры ответственности за нарушение положений документа.

Кроме того, приложением ко всем трудовым договорам должен стать перечень информации, носящей характер коммерческой, а в самих договорах должны быть предусмотрены меры ответственности за ее разглашение.

Организационные меры безопасности.

В большей степени они направлены на устранение внутренней угрозы утечки информации и мотивацию сотрудников на соблюдение утвержденных регламентов. Эти меры предпринимаются службой безопасности во взаимодействии с сотрудниками служб управления персоналом.

В числе организационных мер обеспечения информационной безопасности можно назвать следующие:

* установление различных степеней допуска сотрудников к сведениям, содержащим конфиденциальные данные;
* ограничение круга лиц, имеющих допуск к конфиденциальной информации компании;
* привлечение специалистов для проведения тренингов по защите информации;
* внесение в договоры компании с клиентами норм, которые будут ограничивать их в распространении информации;
* привлечение к ответственности лиц, виновных в разглашении информации.

Также следует учитывать, что при проектировании большинства информационных систем уровень защиты от внешнего проникновения был значительно ниже, чем необходим в настоящее время. Среди организационных мер может быть и их аудит, который установит соответствие современным стандартам.

Технические меры.

Эта группа мер рассчитана на использование действенных технических средств защиты. Для ее реализации используются аппаратные, программные и криптографические средства.

Первые предполагают установку систем резервного копирования и защиту от несанкционированного проникновения, вторые отвечают за работу антивирусов и иных защитных программ, третьи обеспечивают шифрование всей хранимой и передаваемой по каналам связи информации. Наиболее часто для защиты информации применяются межсетевые экраны и системы обнаружения вторжений. Технические средства требуют постоянного обновления и модернизации, так как скорость устаревания программных продуктов очень высока.

С каждым днем мошенники разрабатывают новые средства преодоления защитных барьеров, и степень опасности утраты ценных сведений растет, а вместе с ней и риск возможных финансовых потерь. Минимизировать риски можно, пройдя аудит своих систем защиты и получив рекомендации по их модернизации.

Основой защиты технического уровня являются следующие

механизмы безопасности:

* идентификация и аутентификация пользователей;
* управление доступом;
* протоколирование и аудит;
* криптография;
* экранирование;

Таким образом, политика информационной безопасности должна рассматриваться как система, как комплекс инструментов по защите информации.

Комплексное применение современных технических средств в работе службы безопасности Event-компании может обеспечить высокий уровень защиты информации от утечек и несанкционированного доступа. Следует учитывать, что все предпринимаемые действия должны в полной мере соответствовать требованиям белорусского законодательства.