Содержание:

Введение

Использование компьютерной техники и различных компьютерных программ в бизнесе, в производстве, медицине и других областях привело к тому, что появилась новая ветвь информатики - информационная безопасность.

Информационная безопасность представляет собой процесс защиты информации, с помощью совокупности средств, методов и способов человеческой деятельности, которые направлены на обеспечение защиты всех видов информации в предприятиях разного масштаба и разных форм собственности.

То есть, область информационной безопасности отвечает за охрану информации, примем информация может храниться, обрабатываться и передаваться разными способами и средствами.

Целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Информационная безопасность - это состояние защищенности информации среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств. Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.

Данная тема является актуальной, потому, что сегодня все предприятия стремятся к выживанию в современном бизнесе, и одним из факторов успеха является владение информацией, и ее не раглашение конкуренту, поэтому руководители предприятий используют самые современные средства защиты информации.

Цель исследования – изучить теоретические основы угроз информационной безопасности и рассмотреть виды угроз информационной безопасности.

Для достижения данной цели необходимо решение следующих **задач:**

- Дать определение понятия «информационная безопасность»;
- Определить понятия «информационная безопасность» и «конфиденциальная информация»;
- Определить понятия «угроза информационной безопасности»;
- Описать виды угрозы информационной безопасности;
- Описать источники угрозы информационной безопасности;
- Привести классификацию средств защиты информации;
- Описать метода защиты конфиденциальной информации.

Объектом исследования является информационная безопасность. **Предметом** исследования являются виды угроз информационной безопасности.

Работа состоит из введения, трех глав, заключения и списка использованной литературы.

Глава 1. Базовые понятия и определения

1.1. Сущность понятия «информационная безопасность»

Защита информации – это комплекс мер, которые предназначены для безопасного хранения и защиты информации от нежелательных пользователей. Безопасность коммерческих тайн и оборота документов является главной задачей в защите информации. Информацию охраняют методом технического программного управления передачей секретных данных и доступом.

В качестве этих данных могут быть коммерческие документы, государственные тайны и соглашения фирм, данные о планах увеличения производства, идеи, которые могут приносить доход.

Обращение с такой информацией осуществляют в режимной форме.

Информационная безопасность государства — состояние сохранности информационных ресурсов государства и защищенности законных прав общества и личности в информационной области.

Информационная сфера в современном социуме имеет две составляющие: технически-информационную (мир технологий, техники, созданный человеком искусственно и так далее) и психологически-информационную (естественный мир живой природы, который включает и самого человека). Соответственно, в общем случае информационную безопасность государства (общества) можно представить двумя составными: информационно-психологической (психофизической) безопасностью и информационно-технической безопасностью.

Далее раскроем сущность понятия «информационная безопасность».

Следует начать, с того, что данное понятие можно рассмотреть с разных точек зрения, а точнее в зависимости от его применения, может быть рассмотрено с нескольких сторон.

Информационная безопасность — это процесс обеспечения доступности, целостности, конфиденциальности информации. Доступность: Обеспечение доступа к информации и активам авторизованных пользователей, связанным с ней, по мере необходимости. Целостность Информационная безопасность (англ. information security) — все аспекты, которые связаны с поддержанием, определением, достижением целостности, конфиденциальности, неотказуемости, доступности, аутентичности, подотчетности и достоверности информации или средств обработки[1].

В интернет источниках предложено такое определение данного понятия информационная безопасность - понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации[2].

Безопасность информации (данных) (англ. information (data) security) — это состояние защищенности данных (информации), при котором обеспечиваются ее

(их) конфиденциальность, целостность и доступность. Безопасность данных (информации) определяется отсутствием недопустимого риска, который связан с утечкой информации по техническим каналам, непреднамеренными и несанкционированными воздействиями на данные или на другие ресурсы информационной автоматизированной системы, которые используются в автоматизированной системе.

Безопасность информации (при использовании информационных технологий) (англ. IT security) — это состояние защищенности данных (информации), которое обеспечивает безопасность информации, для обработки которой она используется, и информационную безопасность информационной автоматизированной системы, в которой она реализуется. Безопасность автоматизированной информационной системы — это состояние защищенности автоматизированной системы, при котором обеспечиваются доступность, конфиденциальность, подотчетность, целостность и подлинность ее ресурсов.

Информационная безопасность — это защищенность поддерживающей инфраструктуры и информации от преднамеренных или случайных воздействий искусственного или естественного характера, которые могут нанести субъектам информационных отношений неприемлемый ущерб. Поддерживающая инфраструктура — системы тепло-, электро-, газо-, водоснабжения, системы кондиционирования и так далее, обслуживающий персонал. Неприемлемый ущерб — это ущерб, которым невозможно пренебречь[3].

На данный момент сформулировано три базовых задачи, которые должна обеспечивать информационная безопасность:

Целостность данных — защита от сбоев, ведущих к потере информации, а также защита от незаконного создания или уничтожения данных. Примером нарушения целостности данных является повреждение бухгалтерских баз, в дальнейшем это повлечет за собой последствия, которые определенно станут негативными для компании.

Конфиденциальность информации — незаконное разглашение, утечка, повреждение информации;

Доступность информации для всех пользователей — отказ в обслуживании или услугах, которые могут быть вызваны вирусной активностью или действиями злоумышленников.

В результате можно заключить, что под информационной безопасностью понимается отсутствие недопустимого риска, который связанн с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

1.2. «Информационная безопасность » и «конфиденциальная информация»

С понятием «информационная безопасность» тесно связано понятия «конфиденциальная информация». Следует отметить, что это два разных понятия, и первое в некоторых источниках определяется с помощью второго понятия. А именно: информационная безопасность означает защиту данных, которые являются приватными (личными) для пользователя, а также это касается конфиденциальности общения между пользователем и его коллегами по работе, или родственниками[4].

Конфиденциальность – это принцип неразглашения информации, не предназначенной для открытого доступа или пользования всеми желающими. Термин «конфиденциальный» происходит от латинского слова confidentia, что означает – доверие.

Конфиденциальная информация – это устные или документальные сведения, не подлежащие всеобщей огласке, полученные частным лицом в особо доверительной, откровенной или секретной обстановке и представляющие определенную ценность[5].

Конфиденциальная информация определена в п. 7 ст. 2 Закона об информации через требование не передавать такую информацию третьим лицам без согласия ее обладателя. Надо сказать, что ее режим довольно резко критикуется в литературе как весьма неопределенный. Федеральный закон от 27 июля 2006 г. № 149-ФЗ[6] «Об информации, информационных технологиях и о защите информации» использует лишь самые общие нормативные установки, например: «Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также

ответственность за ее разглашение» (ч. 4 ст. 9**)[7].**

Более точное определение можно найти в электронной энциклопедии экономиста, то есть на сайте http://www.grandars.ru/ - «конфиденциальная информация — это документированная информация, то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать, доступ к которой ограничивается в соответствии с законодательством РФ»[8].

Определение конфиденциальной информации, предложенное на сайте http://www.grandars.ru/, более полное. Согласно данному определению понятие «конфиденциальная информация» рассматривается в широком смысле. Но есть одна неточность по мнению автора от кого хранится информация не указано, можно было бы указать, что «… от третьих лиц, передача третьим лицам является грубым нарушением законодательства Российской Федерации».

При разглашении такой информации может быть создана угроза экономической, государственной или личной безопасности. Слово «секрет» было позаимствовано из французского языка secret и означает «тайна».

Конфиденциальной информацией на сегодняшний день считаются:

- сведения, собранные или полученные в результате юридических и этических действий юристами, медицинскими работниками;
- тайна частной жизни гражданина;
- профессиональные, коммерческие, оперативные секреты;
- государственные и военные секретные материалы;
- личные персональные данные физического лица;
- служебная информация, не предназначенная для открытого пользования всеми желающими[9].

То есть, можно заключить, что к конфиденциальной информации относятся документы представленные на рисунке 1:

Рисунок 1. Конфиденциальные документы[10]

А если рассмотреть и проанализировать все виды конфиденциальной информации, то можно получить следующую схему представленную в Приложении 1.

Обобщив все выше изложенные определения понятия «конфиденциальная информация» можно предложить следующее трактование понятия информационная безопасность – это:

- состояние объекта, когда ему путем воздействия на его информационную сферу не может быть нанесен существенный ущерб или вред;
- свойство объекта, характеризующее его способность не наносить существенного ущерба какому-либо объекту путем оказания воздействия на информационную сферу этого объекта[11].
-

1.3. Сущность понятия «угроза информационной безопасности»

Угроза – представляет собой намерение, предполагающее конкурентные (законные), незаконные или криминальные действия, чреватые негативными последствиями (результатами) для персонала и деятельности предприятия[12].

Под угрозой (в общем случае) трактуется как потенциально возможное событие, процесс или явление, которое может (воздействуя на что-либо) привести к нанесению ущерба чьим-либо интересам.

В литературе, термин угроза информационной безопасности определяется как совокупность условий и факторов, создающих опасность нарушения информационной безопасности[13].

Угрозой интересам субъектов информационных отношений называется потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

Исходя из выше представленного определения получаем, что под угрозой информационной безопасности автоматизированной системы - понимается возможность реализации воздействия на информацию, обрабатываемую в АС, которая приводит к нарушению конфиденциальности, целостности или доступности этой информации, а также возможность воздействия на компоненты АС, приводящего к их утрате, уничтожению или сбою функционирования[14].

Нарушением безопасности (нарушением, атакой) называется реализацию угрозы безопасности.

В силу особенностей современных АС, перечисленных выше, существует значительное число различных видов угроз безопасности субъектов информационных отношений.

Чаще всего угроза является следствием наличия уязвимых мест в системе защиты информации. Промежуток времени от момента, когда появляется возможность использовать уязвимое место, и до момента, когда в систему защиты вносятся изменения, ликвидирующие данную уязвимость, называется окном опасности, ассоциированным (связанным) с данным уязвимым местом.

Причины уязвимости системы:

- Особенностями технических средств, используемых в системе электронной обработки данных.

Например, если информация записывается на дискету, то ее целостность может быть легко нарушена вследствие механических повреждений, воздействия температуры и влажности, электромагнитных полей и других факторов.

- Особенностями используемого программного обеспечения.

Например, пароли для доступа в Интернет могут сохраняться в некотором файле на диске. Следовательно, существует угроза, что злоумышленник найдет этот файл и воспользуется чужим паролем для доступа в Интернет.

- Особенностями поведения персонала, работающего с системой электронной обработки данных.

Например, некоторые пользователи записывают свои пароли для доступа к различным ресурсам на отдельных листочках и хранят эти записи прямо на рабочем месте. Естественно, существует угроза, что злоумышленник может найти такой листочек и воспользоваться чужим паролем.

Многие уязвимые места не могут быть ликвидированы и являются постоянной причиной существования угрозы. Что же касается особенностей программного обеспечения, то, как правило, уязвимые места выявляются в процессе эксплуатации и устраняются путем выпуска новых версий и «пакетов обновлений» программ. Именно для таких уязвимых мест чаще всего используется понятие «окно опасности». Оно «открывается» с появлением средств использования данного пробела в защите и ликвидируется при ликвидации данного уязвимого места.

Для большинства уязвимых мест окно опасности существует сравнительно долго, поскольку за это время должны произойти следующие события:

- Должно стать известно о средствах использования данного пробела в защите

- Должны быть найдены способы ликвидации данного пробела

- Должны быть реализованы способы ликвидации данного пробела, то есть внесены соответствующие изменения в программу

- Эти изменения должны быть осуществлены у всех пользователей, использующих данную программу

Угрозы безопасности информации в современных информационных системах обусловлены:

- случайными и преднамеренными разрушающими и искажающими воздействиями внешней среды;

- степенью надежности функционирования средств обработки информации;

- преднамеренными корыстными воздействиями несанкционированных пользователей, целью которых является хищение, разглашение, уничтожение, разрушение, несанкционированная модификация и использование обрабатываемой информации;

- непреднамеренными, случайными действиями обслуживающего персонала и др. [15]

Следует иметь ввиду, что научно-технический прогресс может привести к появлению принципиально новых видов угроз и что изощренный ум злоумышленника способен придумать новые пути и способы преодоления систем безопасности, НСД к данным и дезорганизации работы АС[16].

Угрозы информационной безопасности, несмотря на их негативное влияние, на новые информационные процессы, являются диалектическим порождением последних; новые реалии информационного сообщества (прогресс) вызывают к жизни новые угрозы. Несмотря на то что информационный процесс некоторого активного субъекта остается неизменным и в киберпространства, тому процессу сопутствуют иные (специфические) угрозы, связанные с особенностями существования и передачи информации в повой среде. Таким образом, с точки зрения любой отрасли права (гражданского, административного, уголовного и др.) современные угрозы информационной безопасности не должны быть ограничены известной классификацией, включающей в себя нарушения лишь конфиденциальности, доступности и целостности информации. Новые особенности информационного процесса в современном мире вызывают необходимость обновления содержательного значения термина «угроза информационной безопасности»[17].

Глава 2.Классификация угроз информационной безопасности

2.1 Виды угроз информационной безопасности

Под угрозой (в принципе) обычно подразумевают потенциально возможный процесс (явление, событие или воздействие), которое вероятно приводит к нанесению убытка чьим-либо потребностям. В Последующем под угрозой защиты

АС отделки информации будем принимать возможность влияние на АС, которое косвенно или прямо может нанести убыток ее безопасности.

В настоящий момент известно список угроз информационной безопасности АС, имеющий больше сотни позиций.

Разбор вероятных угроз информационной безопасности делается со смыслом определения полного списка требований к создаваемой системе защиты.

Для предотвращения угроз, существует ряд методов защиты информации.

Список угроз, анализ рисков вероятностей их реализации, а также модель злоумышленника есть основой для разбора и методики оценки рисков, реализации угроз и построению требований к системе зашиты АС. Кроме обнаружения вероятных угроз, целесообразно проводить исследование этих угроз на основе классификации по ряду параметров. Каждый из параметров классификации показывает одно из обобщенных правил к системе защиты. Угрозы, соответствующие любому признаку классификации, разрешают детализировать отражаемое этим параметром требование.

Нужда в классификации угроз информационной защиты АС объясняется тем, что хранимая и обрабатываемая информация в АС склонна к воздействию факторов, из-за чего становится невозможным формализовать проблему описания полного обилие угроз. Поэтому обычно определяют не полный список угроз, а список классов угроз.

Разделение вероятных угроз информационной безопасности АС может быть сделана по следующим основным параметрам.

По рангу преднамеренности выражения:

- угрозы, спровоцированы ошибками или небрежностью сотрудников, например неграмотное использование методов защиты, ввод не венрных данных и т.п.;
- угрозы преднамеренного влияния, например методы мошенников.

По характеру возникновения:

- искусственные угрозы безопасности АС, вызванные руками человека.
- природные угрозы, созданные воздействиями на АС объективных физических действий или стихийных природных явлений;

По непосредственной причине угроз:

- человек, к примеру нанятые путем подкупа сотрудников, выбалтывание конфиденциальной информации и т.п.;
- природный биом, например стихийные напасти, бури и пр.;
- несанкционированные программно-аппаратные фонды, например заражение ПК вирусами с разрушающими функциями;
- санкционированные программно-аппаратные фонды, отказ в работе ОС, к примеру удаление данных.

По степени зависимости от активности АС:

- только в ходе обработки данных, к примеру угрозы реализации и рассылке программных вирусов;
- независимо от активности АС, к примеру вскрытие шифров (поточные шифры или блочное шифрование) криптозащиты информации.

2.2 Источники угроз информационной безопасности

По состоянию источника угроз:

- непосредственно в АС, к примеру неточная реализация ресурсов АС;
- в пределах зоны АС, к примеру использование подслушивающих приборов, записей, хищение распечаток, носителей данных и т.п.;
- вне зоны АС, например захват информации, передаваемых по путям связи, захват побочных акустических, электромагнитных и других излучений устройств.

По степени воздействия на АС:

- активные угрозы, которые при реакции вносят сдвиг в структуру и сущность АС, к примеру ввод вирусов и троянских коней;
- пассивные угрозы, которые при исполнении ничего не изменяют в типе и сущности АС, к примеру угроза копирования секретной информации.

По способу пути к ресурсам АС:

- угрозы, реализуемые с использованием маскированного нестандартного каналу пути к ресурсам АС, к примеру несанкционированный путь к ресурсам АС путем использования каких либо возможностей ОС;
- угрозы, реализуемые с использованием стандартного каналу доступа к ресурсам АС, к примеру незаконное обретение паролей и других параметров разграничения доступа с последующей маскировкой под зарегистрированного сотрудника.

По шагам доступа сотрудников или программ к ресурсам:

- угрозы, реализуемые после согласия доступа к ресурсам АС, к примеру, угрозы некорректного или несанкционированного применение ресурсов АС;
- угрозы, реализуемые на шаге доступа к ресурсам АС, к примеру, угрозы несанкционированного доступа в АС.

По нынешнему месту размещению информации, хранимой и обрабатываемой в АС:

- угрозы проходу к информации, находящейся в ОЗУ, например проход к системной области ОЗУ со стороны прикладных программ, чтение конечной информации из ОЗУ;
- угрозы проходу к информации, расположенной на внешних запоминающих носителях, например несанкционированное копирование конфиденциальной информации с жесткого носителя;
- угрозы проходу к информации, видимой на терминале, например запись отображаемых данных на видеокамеру;
- угрозы проходу к информации, проходящих в каналах связи, например незаконное подсоединение к каналам связи с задачей прямой подмены законного сотрудника с следующим вводом дезинформации и навязыванием ложных данных, незаконное подсоединение к каналам связи с следующим вводом ложных данных или модификацией передаваемых данных.

Как уже говорилось, опасные влияния на АС делят на случайные и преднамеренные. Исследование опыта проектирования, производство и эксплуатации АС демонстрирует, что данные подвергается различным случайным реакциям на всех ступенях цикла и функционирования АС.

Источником случайных реакций при реализации АС могут быть:

- отрешение и сбои аппаратурных устройств;
- упущении в работе обслуживающих сотрудников и других служащих;

- критичные ситуации из-за стихийных несчастий и отключений электрического питания;
- шумы и фон в каналах связи из-за влияния внешних факторов(характеристики проводных линий связи при передачи данных и внутренний фактор — полоса пропускания и пропускная способность) канала;
- огрехи в программном обеспечении.
- спецификация физической среды Ethernet или token ring.

Погрешности в ПО случаются распространенным видом компьютерных повреждений. ПО рабочих станций, серверов, маршрутизаторов и т д. разработано людьми, поэтому оно может содержать ошибки. Если сложность подобного ПО выше, то и больше риск раскрытие в нем ошибок и уязвимых узлов. Некоторые из них могут не представляют никакой угрозы, а некоторые же могут привести к вещественным результатам, таким как неработоспособность серверной платформы, получение похитителем контроля над серверной платформой, несанкционированное эксплуатация ресурсов (использование ПК в качестве площадки для дальнейших атак и т.п.). Принцип похожие погрешности устраняются с помощью паков обновлений, которые регулярно выпускают разработчики ПО. На сегодня своевременное обновление таких паков является необходимым пунктом безопасности информации. Также погрешности в сети могу случатся из-за проблем защиты информации в сети.

Преднамеренные угрозы сплочены с целенаправленными методами преступника. В качестве преступника может быть сотрудник, обычный посетитель, наемники, конкурентные особи и т.д. Методы преступника могут быть объяснены следующими факторами: конкурентной борьбой, любопытством, недовольством сотрудника своей карьерой, материальным интересом (взятка), стремлением самоутвердиться любыми методами и т.п.

Делая вывод из вероятности становление наиболее опасных условий, обусловленной методами злоумышленника, можно прикинуть гипотетическую модель потенциального злоумышленника:

- злоумышленнику известны данные о методах и параметрах работы системы;
- квалификация злоумышленника может позволять делать несанкционированные действия на уровне разработчика;
- Логично, что злоумышленник может выбрать наиболее слабое место в системе защите;

- злоумышленником может быть кто угодно, как и законный пользователь системы, так и постороннее лицо.

Глава 3. Метода и способы защиты конфиденциальной информации

3.1 Классификация средств защиты информации

Если есть угроза — должны быть и методы защиты и противодействия.

Способы — это средства для достижения поставленных задач и порядок методов приемов использования сил по защите конфиденциальной информации.

Принцип действие человека на подсознании рассчитан на достижение положительных результатов. Опыт профессионалов в сфере защите информации достаточно ясно определил совокупность средств, сил и приемов, нацеленных на гарантирование информационной безопасности или информационной надежности.

Обеспечение информационной надежности или информационной безопасности достигается путем следующих действий направленных на:

- Выявление угроз выражается в порядочном анализе и контроле допустимых появлений потенциальных или реальных угроз а также своевременных мерах по их предупреждению;
- предупреждение угроз, достигается путем обеспечения информационной безопасности или информационной надежности в пользу упреждения и их возникновению на обнаружение угроз с анализом рисков;
- Включение мер по уничтожению угрозы или преступных действий и локализацию преступных действий;
- обнаружение угроз, достигается путем определения конкретных преступных действий и реальных угроз;
- ликвидацию последствий относительно угроз и преступных конкретных действий. Восстановление статус-кво.

Их классифицируют на несколько групп:

• Средства аппаратного (или технического) характера;

• Программные меры защиты;

• Средства, которые относят к смешанному виду;

• Меры организационного или административного характера.

К первой группе относятся разные устройства. Они могут быть электронными, механическими или электромеханическими, но специфика их работы предполагает защиту информации посредством аппаратных средств. Применение этих устройств позволит воспрепятствовать физическому проникновению или замаскировать данные, если доступ все же был открыт.

Технические средства надежны, независимы от субъективных факторов и обладают высокой устойчивостью к модификации. Но у них есть и свои недостатки. В первую очередь это достаточно высокая цена. Также они недостаточно гибкие и практически всегда обладают большими массой и объемом.

Второй вид оперирует разнообразными программами, для того чтобы контролировать доступ, проводить идентификацию пользователей, тестировать контроль системы защиты информации. Кроме того, средства, относящиеся к этой группе, могут шифровать данные и удалять рабочую (остаточную) информацию (вроде временных файлов). Если система использует программные средства для защиты, она получает массу преимуществ. Они гибкие и надежные, универсальные и достаточно просты в установке, а еще способны к модификации и предполагают определенное развитие. Однако этот вид средств очень чувствителен к случайным и преднамеренным изменениям. К другим недостаткам программной защиты можно отнести использование части ресурсов файл-сервера и рабочих станций, ограниченную функциональность сети и то, что ее средства могут зависеть от типа компьютера и его аппаратных средств.

Третья группа сочетает е себе свойства первой и второй.

В последний вид входят средства защиты информации организационно-технического и организационно-правового характера. Сюда можно отнести:

• Контроль доступа в помещения, их подготовку и оснащение;

• Разработку стратегий безопасности компании;

• Подборку и изучение национальных законодательств с последующим их применением;

• Учреждение правил работы и контроль их соблюдения.

Полноценная защита информации в может быть достигнута при использовании всех этих средств в комплексе.

3.2 Методы защиты конфиденциальной информации

Наибольшее внимание защите конфиденциальных данных уделяют предприниматели, которые предусматривают следующие способы защиты:

1. Организационная защита. Здесь есть три пути:

- создание специальной структуры, которая берет на себя функции защиты конфиденциальной информации, несет ответственность за предоставления прав доступа и проверку сотрудников, получающих право на допуск к особым данным;

- четкое соблюдение всех установленных в организации правил и контроль их исполнения. Одновременно с этим организовывается строгая система доступа к конфиденциальным данным. Что касается контроля, то он может быть нескольких типов – документальный, визуальный и так далее;

- разделение всех имеющихся в компании данных по типу важности. При этом организовывается ступенчатая система допуска. К примеру, к менее важной информации допускаются рядовые сотрудники, а к конфиденциальным данным особой важности – менеджеры крупного звена и руководители.

2. Законодательная защита. Ее особенность – упор на соблюдение тех прав бизнесмена, которые зафиксированы в законе РФ. Если же права владельца компании (предпринимателя) нарушены, то он может обратиться в соответствующие структуры для защиты своих интересов и возмещения нарушителем убытков компании.

3. Физическая защита – одно из наиболее важных мероприятий, которому уделяется внимание почти на всех предприятиях. Здесь речь идет об организации пропускного режима, создании и выдаче сотрудникам специальных карт (или предоставление таковых посторонним лицам), применение шкафов повышенной надежности, использование закрывающихся сейфов и так далее.

4. Техническая защита. К такому методу можно отнести использование специальных средств защиты и контроля конфиденциальных данных, таких как микрофоны, видеокамеры, сигнализирующие устройства, системы идентификации пользователей и так далее.

5. Работа с персоналом. Одним из самых важных направлений деятельности является выстраивание правильной работы с трудовым коллективом. Здесь подразумевается организация работы по набору персоналу, оптимизация существующих кадровых служб предприятия, дополнительное обучение персонала, его проверка, стимулирование и прочие мероприятия.

Важный момент – регулярное проведение инструктажей о важности соблюдения правил пользования конфиденциальными данными, а также вероятной ответственности за их разглашение. К основным угрозам конфиденциальной информации, которые исходят от персонала, можно отнести:

- вероятное переманивание работника компании конкурирующей организацией;

- обманные предложения о предоставлении новой должности с хорошим заработком исключительно для выведывания конфиденциальной информации;

- постановка вопросов действующим сотрудникам в особой форме, вынуждающей к разглашению секретных данных;

- предложение финансового вознаграждения за предоставление тех или иных данных (подкуп);

- тайное наблюдение за работниками организации;
- направление специальных агентов для работы в структуре с целью дальнейшего «выуживания» интересующей информации.

Для обеспечения максимальной безопасности проверка персонала должна проходить три основных этапа:

1. Предварительный период, когда работник еще не принят на работу. Здесь речь идет о доскональной проверке кандидата и подписания им основных документов – трудового договора и соглашения о неразглашении.

2. Текущий период (деятельность сотрудника). Здесь обязателен испытательный срок, ознакомление с порядком доступа к конфиденциальной информации, обязанностями, существующими ограничениями и так далее.

3. Заключительный период (увольнение). Во избежание утечки важной информации после увольнения сотрудник предупреждается о возможных последствиях своих потенциальных действий (о предоставлени важной информации третьим лицам) и дает подписку о неразглашении.

Заключение

В результате проведенного исследования на тему «Виды и состав угроз информационной безопасности» можно сделать следующие выводы.

Угроза защищаемой информации – совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.

1.Обеспечение информационной надежности или безопасности достигается организационными, техническими и организационно-техническими процедурами, любое из которых обеспечивается своеобразными методами, средствами и мерами, имеющими соответствующими параметрами.

2.Разнообразные действия и условия, способствующие незаконному или неправомерному усвоению конфиденциальными данными, вынуждает использовать не менее разнообразных способов, средств, сил и для обеспечения информационной безопасности или надежности.

3.Основными задачами охраны информации служит гарантирование конфиденциальности, целостности и достаточности информационных ресурсов. А также разработать политику безопасности и внедрить ее в систему.

Однако следует понимать, что обеспечить стопроцентную защиту невозможно. С появлением новых технологий будут появляться и новые угрозы.

Библиография

1. Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [онлайн] - URL:http://naar.ru/acts/zakon_ob_informatsyionnyih_tehnologiyah_zashita_informatsii/

2. Безопасность жизнедеятельности: Учебник для вузов. 2-е изд. / Под ред. Михайлова Л. А. — СПб.: Питер, 2013. — 461 с: ил. ISBN 978-5-496-00054-3
3. Букин С. О. Безопасность банковской деятельности: Учебное пособие. — СПб.: Питер, 2011 —288 с: ил. ISBN 978-5-459-00569-1
4. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010.
5. Семененко В.Л. Информационная безопасность: Учебное пособие. 4-е изд., стереотип. -М.: МГИУ. 2010.-277 с. ISBN 978-5-2760-1876-8
6. Защита информации. [онлайн] URL: https://biznes-prost.ru/zashhita-informacii.html
7. Иванов, Д.В. Конфиденциальная информация в трудовых отношениях. 1.1. Понятие конфиденциальной информации. [онлайн] URL: https://law.wikireading.ru/7623
8. Информационная безопасность. [онлайн] URL: http://protect.htmlweb.ru/p01.htm
9. Коммерческая тайна и конфиденциальная информация [олнлайн] - URL: http://www.grandars.ru/college/biznes/kommercheskaya-informaciya.html
10. Конфиденциальная информация. [онлайн] URL: https://utmagazine.ru/posts/9997-konfidencialnaya-informaciya
11. КОНФИДЕНЦИАЛЬНОСТЬ — ЭТО ЧТО ТАКОЕ? [онлайн] URL: http://ctoetotakoe.ru/privacy-policy.html
12. Курс «Безопасность Информационных Технологий».Тема 5: Угрозы информационной безопасности в АС. [онлайн] URL: http://asher.ru/security/book/its/05
13. Лекция 3. Угрозы информационной безопасности. [онлайн] URL: https://studopedia.ru/3_71428_lektsiya--ugrozi-informatsionnoy-bezopasnosti.html
14. Основные категории информационной безопасности [онлайн] - URL:http://centerpolit.ru/content.php?id=59
15. Что такое информационная безопасность. [онлайн] URL: http://pro-spo.ru/antivir/3307-informaczionnaya-bezopasnost

Приложение 1

Рисунок 1. Сведение, которые, составляют конфиденциальную информацию[18]

1. Защита информации. [онлайн] URL: https://biznes-prost.ru/zashhita-informacii.html ↑

2. Информационная безопасность. [онлайн] URL: http://protect.htmlweb.ru/p01.htm/ ↑

3. Защита информации. [онлайн] URL: https://biznes-prost.ru/zashhita-informacii.html ↑

4. Что такое информационная безопасность. [онлайн] URL: http://pro-spo.ru/antivir/3307-informaczionnaya-bezopasnost ↑

5. КОНФИДЕНЦИАЛЬНОСТЬ — ЭТО ЧТО ТАКОЕ? [онлайн] URL: http://ctoetotakoe.ru/privacy-policy.html ↑

6. Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [онлайн] - URL:http://naar.ru/acts/zakon_ob_informatsyionnyih_tehnologiyah_zashita_informatsii/ ↑

7. Иванов, Д.В. Конфиденциальная информация в трудовых отношениях. 1.1. Понятие конфиденциальной информации. [онлайн] URL: https://law.wikireading.ru/7623 ↑

8. Коммерческая тайна и конфиденциальная информация [олнлайн] - URL: http://www.grandars.ru/college/biznes/kommercheskaya-informaciya.html ↑

9. КОНФИДЕНЦИАЛЬНОСТЬ — ЭТО ЧТО ТАКОЕ? [онлайн] URL: http://ctoetotakoe.ru/privacy-policy.html ↑

10. Конфиденциальная информация. [онлайн] URL: https://utmagazine.ru/posts/9997-konfidencialnaya-informaciya* ↑

11. Основные категории информационной безопасности [онлайн] - URL:http://centerpolit.ru/content.php?id=59 ↑

12. Букин С. О. Безопасность банковской деятельности: Учебное пособие. — СПб.: Питер, 2011 — с. 25. ↑

13. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. – с. 98 ↑

14. Семененко В.Л. Информационная безопасность: Учебное пособие. 4-е изд., стереотип. -М.: МГИУ. 2010.-с. 31. ↑

15. Лекция 3. Угрозы информационной безопасности. [онлайн] URL: https://studopedia.ru/3_71428_lektsiya--ugrozi-informatsionnoy-bezopasnosti.html ↑

16. Курс «Безопасность Информационных Технологий».Тема 5: Угрозы информационной безопасности в АС. [онлайн] URL: http://asher.ru/security/book/its/05 ↑

17. Безопасность жизнедеятельности: Учебник для вузов. 2-е изд. / Под ред. Михайлова Л. А. — СПб.: Питер, 2013. — с. 328 ↑

18. Конфиденциальная информация. [онлайн] URL: https://utmagazine.ru/posts/9997-konfidencialnaya-informaciya ↑