**Источники возникновения и последствия реализации угроз информационной безопасности**

Курсовая работа по дисциплине «Теория информационной безопасности и методология защиты информации»

Студент Д.Д. Кирьянов

Московский государственный индустриальный университет (ГОУ МГИУ)

Москва 2008

Введение

В современном мире информация стала важнейшим ресурсом общества. Традиционные материальные ресурсы постепенно утрачивают свое первоначальное значение, а им на смену приходят информационные ресурсы, которые со временем не убывают, а неуклонно растут. Информация как предмет труда становится всё в большей степени стратегическим ресурсом общества, его движущей производительной силой.

Широкое использование информационных технологий во всех сферах жизни современного общества делает вполне закономерной и весьма актуальной проблему защиты информации, или иначе, проблему обеспечения информационной безопасности. В условиях интенсивного развития рынка информационных продуктов и услуг, информация становиться полноценным товаром. Подобно другим товаром, информация нуждается в сохранности, и следовательно в надежной защите.

В данной работе мы рассмотрим источники возникновения и последствия реализации угроз информационной безопасности, классифицируем источники угроз, рассмотрим человеческий фактор как источник угроз информационной безопасности, а так же опишем последствия воздействия угроз и виды угрожающих воздействий и классифицируем угрозы степени тяжести последствий и возможного ущерба.

2. Источники возникновения и последствия реализации угроз информационной безопасности.

2.1 Классификация источников угроз

Носителями угроз безопасности информации являются источники угроз. Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации) Кроме того, возможно не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред. В качестве источников угроз могут выступать как субъекты (личность) так и объективные проявления. Причем, источники угроз могут находиться как внутри защищаемой организации - внутренние источники, так и вне ее - внешние источники.

Деление источников на субъективные и объективные оправдано исходя из того, что Субъективные уязвимости зависят от действий сотрудников и, в основном, устраняются организационными и программно-аппаратными методами. А Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации.

А деление на внутренние и внешние источники оправдано потому, что для одной и той же угрозы методы парирования для внешних и внутренних источников могу быть разными.

Все источники угроз безопасности информации можно разделить на три основные группы:

1) Обусловленные действиями субъекта (антропогенные источники угроз).

2) Обусловленные техническими средствами (техногенные источники угрозы).

3) Обусловленные стихийными источниками.

2.1.1 Антропогенные источники угроз.

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорит о причинении ущерба. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты информации.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

1) криминальные структуры;

2) потенциальные преступники и хакеры;

3) недобросовестные партнеры;

4) технический персонал поставщиков телематических услуг;

5) представители надзорных организаций и аварийных служб;

6) представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

1) основной персонал (пользователи, программисты, разработчики);

2) представители службы защиты информации;

3) вспомогательный персонал (уборщики, охрана);

4) технический персонал (жизнеобеспечение, эксплуатация).

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты, которые могут быть из числа основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угрозам для этой группы могут иметь свои отличия.

Квалификация антропогенных источников информации играют важную роль в оценке их влияния и учитывается при ранжировании источников угроз.

2.1.2 Техногенные источники угроз.

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако, последствия, вызванные такой деятельностью вышли из под контроля человека и существуют сами по себе. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.

Технические средства, являющиеся источниками потенциальных угроз безопасности информации так же могут быть внешними:

1) средства связи;

2) сети инженерных коммуникации (водоснабжения, канализации);

3) некачественные технические средства обработки информации;

4) некачественные программные средства обработки информации;

5 )вспомогательные средства (охраны, сигнализации, телефонии);

6) другие технические средства, применяемые в учреждении.

2.1.3 Стихийные источники угроз.

Третья группа источников угроз объединяет, обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз информационной безопасности как правило являются внешними по отношению к защищаемому объекту и под ними понимаются прежде всего природные катаклизмы:

1) пожары;

2) землетрясения;

3) наводнения;

4) ураганы;

5) различные непредвиденные обстоятельства;

6) необъяснимые явления;

7) другие форс-мажорные обстоятельства.

2.2 Человеческий фактор как антропогенный источник угроз.

Чаще всего к возникновению значительного ущерба приводят злонамеренные или ошибочные действия людей, а техногенные источники, как правило, выступают в качестве предпосылки.

2.2.1 Внешние источники угроз

Хакеры и криминальные структуры.

Популярность такого источника угроз, как хакеры, к сожалению, активно поддерживается средствами массовой информации.

Личный опыт общения с хакерами показывает, что многие из них испытывают проблемы в создании полноценных межличностных отношений, и их деструктивную деятельность частично можно объяснить потребностью в их компенсации.

Важный мотив действий хакера - материальная выгода. Особенно часто совершаются попытки кражи номеров кредитных карт, либо конфиденциальной информации с последующим шантажом с целью вымогательства. Сюда же можно отнести случаи взлома финансовых систем или мошенничества.

Распространённым мотивом действий хакеров являются межнациональные конфликты. В качестве примеров можно привести хакерские "войны" между Арменией и Азербайджаном, атаки российских сайтов представителями исламских стран, массированные нападения китайских хакеров на сервера Японии, Тайваня, США.

Реальная квалификация большинства хакеров ниже, чем у профессиональных программистов. Иногда попытки злоупотреблений совершаются лицами с преступными наклонностями, совсем не обладающими специальными знаниями. Но даже если вас очень впечатлили навыки компьютерного преступника, не рекомендуем принимать его на работу ввиду наличия деструктивных наклонностей. Взлом и построение информационных систем - далеко не одно и тоже, а "бомба" внутри организации гораздо опаснее, чем снаружи. Это утверждение подтверждено личным знакомством с домашними компьютерами преступников, на которых оказывалась конфиденциальная информация приютивших их компаний.

Практика показывает, что в большинстве случаев хакеры, представляющие реальную опасность, работают по заказу и под контролем организованных криминальных структур.

Время от времени появляются сообщения о том, как в качестве заказчиков компьютерных преступлений выступают спецслужбы различных стран.

Недобросовестные партнёры и конкуренты.

В течении последних лет наряду с пособиями для хакеров на полках магазинов в изобилии появились книги по промышленному шпионажу, и некоторые из них уже являются рекордсменами продаж. В списках услуг охранно-сыскных структур присутствует получение информации и наблюдение за конкурентами и партнёрами, подобные функции выполняют и собственные службы безопасности многих компаний. Ещё одним инструментом добычи сведений являются недобросовестные служащие государственных структур.

В качестве источника информации недобросовестные партнёры и конкуренты используют Web-сайты, СМИ, материалы публичных выступлений. Для сбора информации в глобальной сети всё чаще привлекаются хакеры.

Но самым опасным для компании источником утечки конфиденциальной информации являются ее собственные сотрудники.

Конкуренты могут получать информацию в ходе беседы после выступлений и на специально организованных переговорах. При соответствующей подготовке недоброжелатели могут эффективно использовать современные психотехнологии, эксплуатировать желание субъекта показать себя влиятельным, осведомлённым, компетентным, использовать вредные привычки и скрытые потребности.

В первую очередь объектом воздействия становятся менеджеры и высококвалифицированные специалисты, так как именно они осведомлены в наибольшей степени.

Особенно полезными для недобросовестных конкурентов могут оказаться уволенные сотрудники, а также сотрудники, получившие приглашение, в том числе мнимое, на работу. Находящиеся в штате работники также не всегда следуют интересам организации.

Не менее опасным для компании может оказаться воздействие заведомо ложной и модифицированной информации, которая передаётся по "доверенным" каналам, распространяется через СМИ, Web-сайты, публичные выступления.

2.2.2 Внутренние источники угроз.

Менеджеры.

Как лица, обладающие большими организационными полномочиями, наибольшую потенциальную угрозу для информационных ресурсов компании представляют менеджеры. Например, к потерям могут привести распоряжения предоставить пользователю неоправданно высокие права, реализовать в информационной системе небезопасный, но удобный функционал. Иногда информационные угрозы возникают вследствие неудовлетворительного выполнения руководителями контролирующих функций. Известны случаи, когда продавалось оборудование, с дисков которого не удалялась конфиденциальная информация компании и партнёров.

Во избежание возникновения ущерба целесообразно обязать менеджеров согласовывать решение вопросов, связанных с информационными рисками, с руководителем службы информационной безопасности.

Сотрудники.

Значительной угрозой информационной безопасности компании является низкая квалификация персонала, недостаточная для корректной работы с корпоративной информационной системой. Особо опасными являются некомпетентные сотрудники, выдающие себя за грамотных пользователей, или считающие себя таковыми.

Во многих компаниях отсутствует контроль над установкой на рабочих станциях программного обеспечения. Не понимая возможных последствий, сотрудник может установить на своём рабочем месте заинтересовавшую его программу или "патч", существенно снизив эффективность усилий по обеспечению корпоративной сетевой безопасности. Подобная угроза возникает и в случае подключения находящейся в локальной сети рабочей станции к Интернет через модем или мобильный телефон, оснащённый функцией цифровой связи.

Конечно, не будет лишним ещё раз упомянуть об угрозах, исходящих от приклеенных к мониторам стикеров с паролями и практики обмена паролями между работниками, выполняющими сходные функции.

В ряде случаев проблемы безопасности связаны с тем, что легальные пользователи используют необходимую для работы информацию не по назначению. Причиной может быть злой умысел, халатность, непонимание последствий распространения доступных им сведений. Очевидно, что данная проблема неразрешима только технологическими мерами.

Наибольшую опасность представляют сотрудники, обиженные на организацию и её руководителей. Поэтому случаи возникновения явных и скрытых конфликтов, несоответствия сложившейся ситуации ожиданиям сотрудников, могут рассматриваться как потенциальные предпосылки нарушений информационной безопасности. Особого внимания требуют связанные с такими ситуациями случаи увольнения. Как отмечалось выше, сотрудник, уволившийся из компании с чувством обиды, легко может стать источником информации для недоброжелателей.

IT-специалисты, администраторы и лица, выполняющие критичные операции.

Хочется обратить внимание на отбор кандидатов, которым предполагается доверить выполнение операций, требующих больших прав в информационной системе. Не меньшее значение, чем профессиональные навыки, имеют лояльность кандидата и способность сохранять приверженность интересам компании даже в сложных ситуациях. По этой причине лица, на вершине системы ценностей которых находится материальное вознаграждение, скорее всего, получат отказ. С особой осторожностью следует относиться к кандидатам, слишком часто меняющим работу, предоставившим недостоверные сведения, привлекавшимся к административной и уголовной ответственности, имевшим психические или невротические расстройства.

Желательно, чтобы кроме собеседования со своим руководителем, кандидат встретился с профессиональным психологом. Часто психолог проводит тестирование, которое выявляет особенности характера и потенциальные возможности кандидата. Также важно провести беседу, в ходе которой будут выявлены система ценностей и особенности поведения. Это позволит убедиться в том, что кандидат гладко "впишется" в корпоративную культуру, понять, какая система мотивации будет для него наиболее подходящей.

Особое внимание следует уделить тому, чтобы работа сотрудника в организации соответствовала его ожиданиям. В частности руководителю следует воздержаться от необоснованных обещаний. Психологический контракт важен так же, как формальный.

Традиционной проблемой, связанной с IT-сотрудниками, является контроль и оценка результатов деятельности. Немногие руководители способны воспринимать "птичий" язык и вникать в сущность их работы, в том числе в вопросы защиты данных. И немногие владеющие глубокими знаниями в IT, компетентны в вопросах управления.

Например, в IТ-подразделениях часто отсутствуют должностные инструкции и не проводятся аттестации. Иногда IТ-специалистов рассматривают как обслуживающий персонал, пытаются нагрузить дополнительной работой, не определённой должностной инструкцией. Это ухудшает выполнение прямых обязанностей, вызывает недовольство, отрицательно сказывается на лояльности, приводит к высокой текучке кадров. Наверняка многим известны случаи, когда увольняющийся администратор блокирует пароли сервера.

2.3 Последствия воздействия угроз и виды угрожающих воздействий.

Последствием воздействия угроз является нарушение безопасности системы. Рассмотрим эти последствия угроз, а также перечень и сущность различных видов угрожающих воздействий, которые являются причинами дискредитации системы защиты информационно-вычислительной сети или системы. (Угрожающие действия, являющиеся следствием случайных (природных) событий обозначены "\*".)

2.3.1 (Несанкционированное) Вскрытие.

Обстоятельство или событие, посредством которого субъект получил доступ к охраняемым данным (например, конфиденциальным), не имеющий на самом деле прав доступа к ним. Следующие угрожающие действия могут стать причиной несанкционированного вскрытия:

1.1. "Разоблачение": Угрожающее действие, посредством которого охраняемые данные стали доступны непосредственно субъекту, не имеющему на это право. Оно включает:

1.1.1. "Преднамеренное разоблачение": Умышленный допуск к охраняемым данным субъекта, не имеющему на это право.

1.1.2. "Просмотр остатка данных": Исследование доступных данных, оставшихся в системе, с целью получения несанкционированного знания охраняемых данных.

1.1.3.\* "Ошибка человека": Действие или бездействие человека, которое неумышленно повлекло за собой несанкционированное знание субъектом охраняемых данных.

1.1.4.\* "Аппаратно-программная ошибка": Ошибка системы, которая повлекла за собой несанкционированное знание субъектом охраняемых данных.

1.2. "Перехват": Угрожающее действие, посредством которого субъект имеет непосредственный несанкционированный доступ к охраняемым данным, циркулирующим между полномочными источниками и получателями. Оно включает:

1.2.1. "Кража": Получение доступа к охраняемым данным путем воровства различных накопителей информации независимо от их физической сущности (например, кассеты с магнитной лентой или магнитные диски и др.).

1.2.2. "Прослушивание (пассивное)": Обнаружение и запись данных, циркулирующих между двумя терминалами в системе связи.

1.2.3. "Анализ излучений": Непосредственное получение содержания передаваемых в системе связи сообщений путем обнаружения и обработки сигнала, излучаемого системой и "переносящего" данные, но не предназначенного для передачи сообщений.

1.3. "Умозаключение": Угрожающее действие, посредством которого субъект получает несанкционированный, но не прямой, доступ к охраняемым данным (но не обязательно к данным, содержащимся в передаваемых сообщениях) путем осмысления характеристик или "побочных продуктов" систем связи. Оно включает:

1.3.1. "Анализ трафика": Получение знания охраняемых данных путем наблюдения за изменением характеристик системы связи, которая транспортирует данные.

1.3.2. "Анализ сигналов": Не прямое получение знания охраняемых данных, передаваемых в системе связи, путем обнаружения и анализа сигнала, излучаемого системой и "переносящего" данные, но не предназначенного для передачи сообщений.

1.4. "Вторжение": Угрожающее действие, посредством которого субъект обеспечивает несанкционированный доступ к охраняемым данным путем обмана средств обеспечения безопасности системы. Оно включает:

1.4.1. "Посягательство": Получение несанкционированного физического доступа к охраняемым данным путем обмана системных средств защиты информации.

1.4.2. "Проникновение": Получение несанкционированного логического доступа к охраняемым данным путем обмана системных средств защиты информации.

1.4.3. "Реконструкция": Добыча охраняемых данных путем декомпозиции и анализа конструкции системного компонента.

1.4.4. "Криптоанализ": Преобразование зашифрованных данных в открытый текст (дешифрование) без априорных знаний о параметрах и алгоритме процедуры зашифрования.

2.3.2 Обман.

Обстоятельство или событие, которое может повлечь за собой получение полномочным субъектом искаженных данных, но воспринимаемых им как верные. Следующие угрожающие действия могут повлечь за собой обман:

2.1. "Маскарад": Угрожающее действие, посредством которого субъект получает несанкционированный доступ к системе или осуществляет злонамеренное действие, выступая в роли полномочного субъекта.

2.1.1. "Мистификация": Попытка субъекта осуществить несанкционированный доступ в систему под видом полномочного пользователя.

2.1.2. "Устройство для злонамеренных действий": С точки зрения "маскарада", любое аппаратно-программное устройство или программное обеспечение (например, "троянский конь"), которое якобы предназначено для поддержания эффективного и устойчивого функционирования системы, но на самом деле обеспечивает несанкционированный доступ к системным ресурсам или обманывает пользователя путем выполнения другого злонамеренного акта.

2.2. "Фальсификация": Угрожающее действие, посредством которого искаженные данные вводят в заблуждения полномочного субъекта.

2.2.1. "Подмена": Внесение изменений или замена истинных данных на искаженные, которые служат для обмана полномочного субъекта.

2.2.2. "Вставка": Добавление искаженных данных, которые служат для обмана полномочного субъекта.

2.3. "Отказ": Угрожающее действие, посредством которого субъект обманывает другого путем ложного отрицания ответственности за какое-либо собственное действие.

2.3.1. "Ложный отказ источника": Действие, посредством которого автор ("держатель") данных отрицает свою ответственность за авторство (генерирование) этих данных.

2.3.2. "Ложный отказ получаеля": Действие, посредством которого получатель данных отказывается от получения этих данных и обладания ими.

2.3.3 Разрушение.

Обстоятельство или событие, которое препятствует или прерывает корректное функционирование системных служб и реализацию необходимых действий. Следующие угрожающие действия могут вызвать разрушение:

3.1. "Вредительство": Угрожающее действие, которое препятствует или прерывает функционирование системы путем вывода из строя ее компонентов.

3.1.1. "Устройство для злонамеренных действий": С точки зрения "вредительства", любое аппаратно-программное устройство или программное обеспечение (например, "логическая бомба"), умышленно встраиваемое в систему для нарушения ее работоспособности или уничтожения ее ресурсов.

3.1.2. "Физическое разрушение": Умышленной разрушение системного компонента с целью препятствия нормальному функционированию системы или его прерывание.

3.1.3.\* "Ошибка человека": Действие или бездействие человека, которое неумышленно повлекло за собой выход из строя компонента системы.

3.1.3.\* "Аппаратно-программная ошибка": Ошибка, которая либо повлекла за собой повреждение системного компонента, либо привела к прекращению нормального (или полному прекращению) функционирования системы.

3.1.4.\* "Природный катаклизм": Любое природное явление (например, пожар, наводнение, землетрясение, молния или смерч), повлекшее за собой выход из строя компонента системы.

3.2. "Порча": Угрожающее действие, которое вносит нежелательное изменение в функционирование системы путем вредительского изменения алгоритмов функционирования или данных ситемы.

3.2.1. "Подделка": С точки зрения "порчи", умышленное искажение программного обеспечения, данных или управляющей информации системы с целью прерывания или препятствования корректному выполнению системных функций.

3.2.2. "Устройство для злонамеренных действий": С точки зрения "порчи", любое аппаратно-программное устройство или программное обеспечение (например, "компьютерный вирус"), преднамеренно встроенное в систему с целью изменения алгоритмов и процедур функционирования системы или ее данных.

3.2.3.\* "Ошибка человека": Действие или бездействие человека, которое неумышленно повлекло за собой искажение алгоритмов и процедур функционирования системы или ее данных.

3.2.4.\* "Аппаратно-программная ошибка": Ошибка, которая повлекла за собой изменение алгоритмов и процедур функционирования системы или ее данных.

3.2.5.\* "Природный катаклизм": Любое природное явление (например, мощный электромагнитный импульс, вызванный молнией), повлекшее за собой искажение алгоритмов и процедур функционирования системы или ее данных.

2.3.4 Захват (узурпация).

Обстоятельство или событие, в результате которого управление службами системы и ее функционирование перешло к незаконному субъекту. Следующие угрожающие действия могут повлечь за собой "захват":

4.1. "Незаконное присвоение": Угрожающее действие, посредством которого субъект присваивает себе функции несанкционированного логического или физического управления системным ресурсом.

4.1.1. "Кража службы": Несанкционированное использование службы субъектом.

4.1.2. "Кража функциональных возможностей": Незаконное приобретение действующих аппаратно-программных средств и программного обеспечения компонентов сети.

4.1.3. "Кража данных": Незаконное приобретение и использование данных.

4.2. "Злоупотребление": Угрожающее действие, которое повлекло за собой выполнение системным компонентом каких-либо функций или процедур обслуживания, подрывающих безопасность системы.

4.2.1. "Подделка": С точки зрения "злоупотребления", умышленное искажение программного обеспечения, данных или управляющей информации системы с целью принуждения системы выполнять несанкционированные функции или процедуры обслуживания.

4.2.2. "Устройство для злонамеренных действий": С точки зрения "злоупотребления", любое аппаратно-программное устройство или программное обеспечение, преднамеренно встроенное в систему с целью выполнения или управления несанкционированными функцией или процедурой обслуживания.

4.2.3. "Нарушение дозволенности": Действие субъекта, которое обеспечивает для него превышение дозволенных системных полномочий путем выполнения несанкционированной функции.

Анализ представленных угроз и последствий их воздействия показывает, что конечными их целями являются: информация пользователей, циркулирующая в информационно-вычислительной сети или системе - чтение и искажение (разрушение) информации и/или нарушение процедур информационного обмена; работоспособность самой информационно-вычислительной сети или системы - чтение и искажение (разрушение) управляющей информации и/или нарушение процедур управления сетевыми (системными) компонентами или всей сетью (системой).

2.4 Классификация угроз по степени тяжести последствий и возможного ущерба.

По степени тяжести последствий угрозы бывают: угрозы с высокой, значительной, средней и низкой тяжестью последствий.

Высокая тяжесть означает, что эти угрозы могут привести к резкому ухудшению всех финансово-экономических показателей деятельности субъекта предпринимательства, что вызывает немедленное прекращение его деятельности либо наносят такой непоправимый вред, который приведет к этим же последствиям позднее. В этом случае происходит ликвидация фирмы.

Значительная степень тяжести последствий реализации угроз предполагает возможность нанесения фирме таких финансовых потерь, которые окажут негативное воздействие на основные финансово-экономические показатели фирмы, на ее деятельность в будущем и преодолеваются в течение длительных сроков времени.

Средняя степень тяжести означает, что преодоление последствий осуществления этих угроз требует затрат (наносит потери), сопоставимые с текущими затратами фирмы и не требует значительного времени.

Последствия реализации угроз с низкой степенью последствий не оказывают какого-либо существенного воздействия ни на стратегические позиции фирмы, ни даже на ее текущую деятельность.

Проявления возможного ущерба могут быть различны:

1) моральный и материальный ущерб деловой репутации организации;

2) моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;

3) материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;

4) материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

5) материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;

6) моральный и материальный ущерб от дезорганизации деятельности организации;

7) материальный и моральный ущерб от нарушения международных отношений.

Ущерб может быть причинен каким-либо субъектом и в этом случае имеется на лицо правонарушение, а также явиться следствием независящим от субъекта проявлений (например, стихийных случаев или иных воздействий, таких как проявления техногенных свойств цивилизации). В первом случае налицо вина субъекта, которая определяет причиненный вред как состав преступления, совершенное по злому умыслу (умышленно, то есть деяние совершенное с прямым или косвенным умыслом) или по неосторожности (деяние, совершенное по легкомыслию, небрежности, в результате невиновного причинения вреда) и причиненный ущерб должен квалифицироваться как состав преступления, оговоренный уголовным правом.

Во втором случае ущерб носит вероятностный характер и должен быть сопоставлен, как минимум с тем риском, который оговаривается гражданским, административным или арбитражным правом, как предмет рассмотрения.

В теории права под ущербом понимается невыгодные для собственника имущественные последствия, возникшие в результате правонарушения. Ущерб выражается в уменьшении имущества, либо в недополучении дохода, который был бы получен при отсутствии правонарушения (упущенная выгода).

При рассмотрении в качестве субъекта, причинившего ущерб какую-либо личность, категория "ущерб" справедлива только в том случае, когда можно доказать, что он причинен, то есть деяния личности необходимо квалифицировать в терминах правовых актов, как состав преступления. Поэтому, при классификации угроз безопасности информации в этом случае целесообразно учитывать требования действующего уголовного права, определяющего состав преступления.

3 Заключение.

Внешние лица имеют меньше возможностей доступа к ресурсам корпоративной информационной системы, чем внутренние пользователи, и представляют из себя меньшую угрозу. В то же время, на них очень сложно или почти невозможно влиять, поэтому для эффективной защиты от внешних угроз необходимо в первую очередь использовать внутренние технические и организационные меры.

Степень надёжности средств информационной безопасности должна соответствовать потенциальным потерям компании. Критичность информации желательно оценивать также с точки зрения цены этой информации на рынке.

Реализация злоупотребления внешним лицом должна требовать от него больших затрат, чем потенциальная выгода преступника.

Желательно, чтобы ваша информационная система компании была защищена не хуже, чем системы конкурентов.

Доступ к серверам, хранящим информацию, должен быть ограничен не только технологически и организационно, но и физически. Вход в помещения ограниченного доступа должен контролироваться наиболее жёстко.

Информация в компании должна быть разделена на несколько уровней доступа. Сотрудник должен получать доступ только к тем сведениям, которые необходимы ему для работы. Принцип минимальных полномочий должен действовать как для электронных, так и для иных данных. Необходимо утвердить список наиболее критичной информации, отнесённой к разряду конфиденциальной, сотрудники должны быть ознакомлены с ним под роспись. Доступ к конфиденциальной информации возможен только после внесения сотрудника в соответствующий список, утверждаемый руководством.

При принятии решения о предоставлении доступа к информации целесообразно учитывать психологические особенности и компетентность сотрудника.

Изменения в поведении сотрудника, свидетельствующие о недовольстве и разочаровании в связи с происходящими в компании событиями, могут рассматриваться как причина ограничения его прав доступа к информации. Особого внимания требует процесс увольнения сотрудника. Разумным решением будет ограничить доступ сотрудника к информации на время прохождения испытательного срока.

Работа и оценка деятельности персонала должна производиться в соответствии с требованиями положений о подразделениях, должностных инструкций и регламентов. Критичные действия с информацией должны быть максимально определены, сотрудник не должен в таких случаях принимать решений. Он должен точно знать, к кому обязан обратиться в случае возникновения специально определённой или не описанной инструкцией ситуации.

Желательно, чтобы выполнение требований информационной безопасности рассматривалось в качестве одного из критериев оценки работы, и нарушение этих требований должно приводить к наказанию, определённому внутренними нормативными документами. Наряду с рядовыми сотрудниками ответственность за соблюдение правил информационной безопасности должны нести менеджеры.

Выполнение внутренних регулирующих документов в части, касающейся информационной безопасности, должно контролироваться службой информационной безопасности. При этом сотрудникам необходимо объяснить, что контролируются не люди, а производственные процессы, и что такой контроль соответствует их личным интересам, так как защищает от давления на них и близких им людей со стороны криминальных структур.

Руководитель службы информационной безопасности не должен подчиняться IT-директору ввиду различия решаемых ими задач.

Желательно, чтобы наряду с подготовкой по защите данных, руководитель службы информационной безопасности прошёл специальную подготовку в области практической психологии.

Корпоративная культура должна поддерживать лояльность сотрудников. Желательно, чтобы система мотивации сотрудника соответствовала его психологическим особенностям.

Если в компании принят кодекс поведения, целесообразно включить в него пункты, определяющие ожидания компании относительно обращения сотрудника с доступной ему служебной информацией.

Сотрудники должны быть проинструктированы о том, как себя вести с партнёрами, клиентами, ранее неизвестными лицами, пытающимися получить после выступлений, в ходе переговоров, при иных обращениях, сведения, составляющие коммерческую тайну. Особо аккуратно следует общаться с прямыми и косвенными конкурентами, компаниями, проводящими на рынке агрессивную политику.

При передаче партнёрам сведений, не являющихся общедоступными, должно быть подписано соглашение о неразглашении информации.

Одним из способов снижения информационных рисков компании является аутсорсинг информационных ресурсов у специализированной организации, способной нанять высококвалифицированный IT-персонал и обеспечить его эффективную работу. Желательно, чтобы такая организация обладала репутацией, подтверждённой многолетним опытом успешной работы. Дополнительным преимуществом является наличие заключения о результатах проверки в этой организации состояния информационной безопасности, проведённой внешним авторитетным аудитором.

**Список литературы**

Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. – М.: МЦНМО, 2002.

Е.Б. Белов, В.П. Лось Основы информационной безопасности. / Москва, Горячая линия – Телеком, 2006

Федеральный закон РФ "О персональных данных"

Вихорев С.В. Информационная Безопасность Предприятий. Москва, 2006.

В.А. Семененко Информационная безопасность. Москва, 2004