5. Лекция: Юридические вопросы информационной безопасности

В лекции рассмотрены юридические вопросы информационной безопасности. Рассмотрено законодательство в данной области ряда стран (США, Австралия, Китай и ряд других). А также вопросы судебного преследования, конфиденциальности личной информации.

Существует множество юридических проблем, связанных с информационной безопасностью. Очевидно, что взлом компьютеров является противозаконным действием. В разных странах мирового содружества определения компьютерного преступления отличаются друг от друга, и наказание за участие в такого рода деятельности также различно. Независимо от способа совершения компьютерного преступления его исполнители должны быть наказаны, и профессионалы, работающие в сфере информационной безопасности, должны уметь собирать информацию, необходимую правоохранительным органам при задержании и вынесении приговора лицам, несущим ответственность за это преступление.

Использование компьютера в преступных целях - это не единственная проблема, с которой сталкиваются IT-профессионалы. Существуют вопросы гражданской ответственности и неприкосновенности личной информации, которые тоже нуждаются в исследовании. Следует понять, что при слабой внутренней защите возникает опасность, исходящая от служащих и сторонних организаций, подключенных к сетевому окружению вашей организации. В новом законодательстве нашли отражение вопросы безопасности финансовой информации о клиентах и конфиденциальности сведений медицинского характера. Нарушение этих законов представляет собой серьезную проблему для организации и может привести к уголовному наказанию. Все эти проблемы требуют понимания и изучения профессионалами, работающими в сфере информационной безопасности, в тесном взаимодействии с юрисконсультами организации.

Уголовное право США

Уголовное право США представляет собой основу для расследования компьютерных преступлений федеральными властями (Федеральным Бюро Расследований и Секретной Службой). Закон 1030 США является главным законом, посвященным компьютерным преступлениям, другие законы могут быть взяты за основу при проведении расследований. В следующих разделах мы рассмотрим те законы, которые наиболее широко используются на практике. Узнать об их применении в конкретной ситуации или в определенной организации следует у главного юрисконсульта вашей компании.

Компьютерное мошенничество и злоупотребление (Закон 1030 Свода законов США)

Как уже говорилось выше, на базе закона 1030 США осуществляется расследование компьютерных преступлений на федеральном уровне. В этом законе имеется несколько важных моментов, понимание которых необходимо профессионалам, работающим в области безопасности, например, определение типов компьютерных преступлений. Так, в разделе "a" приведено определение компьютерного преступления как преднамеренного несанкционированного доступа в компьютер. Во вторую часть закона внесена поправка, что лицо, получившее доступ к защищенному компьютеру, должно завладеть информацией, хранящейся на этом компьютере. Понятие "защищенные компьютеры" включает в себе компьютеры, используемые правительством США, финансовыми учреждениями и организациями внутренней или внешней торговли и связи.

Основываясь на этом определении, большинство компьютеров, подключенных к интернету, классифицируются как "используемые во внутренней или внешней торговле и связи". Следует отметить еще один важный момент. В законе 1030 вводится понятие величины минимального ущерба, нанесенного при совершении преступления, позволяющее применить этот закон. Размер минимального ущерба составляет 5 000 долларов, сюда входит также стоимость проведения расследования и исправление повреждений от взлома. Обратите внимание, что в сумму ущерба не включен ущерб от взлома конфиденциальных данных, несмотря на то, что в разделе "a" обсуждалось разглашение сведений, которые находятся под защитой правительства.

В законе, таким образом, не предусмотрено наказание за взлом компьютера, если причиненный ущерб составляет менее 5 000 долларов. К примеру, в соответствии с решением суда Джорджии установлено, что сканирование системы не приводит к ее повреждению и, следовательно, не попадает под действие федерального закона или закона штата Джорджия.

Мошенничество с кредитными картами (Закон 1029 Свода законов США)

Множество компьютерных преступлений связано с кражей номеров кредитных карт. В этом случае закон 1029 позволяет вынести лицу обвинение в совершении федерального преступления. Обвинение выносится при подделке пятнадцати или больше номеров кредитных карт.

Атака на компьютерную систему, в результате которой злоумышленник получает несанкционированный доступ к номерам кредитных карт, является нарушением закона 1029. Эта атака считается преступлением, даже если величина нанесенного ущерба составляет менее 5 000 долларов, но при этом

злоумышленник завладеет номерами кредитных карт в количестве 15 и выше.

Авторские права (Закон 2319 Свода законов США)

Закон 2319 Свода законов США определяет наказание за нарушение авторских прав в случае, если обвиняемый занимался воспроизведением и распространением материалов, защищенных авторскими правами, изготовил 10 (или больше) копий, и общий доход от этого составил 1000 долларов (или 2500 долларов в более серьезных случаях). Если компьютерная система была вскрыта и использовалась как место для распространения защищенного авторским правом программного обеспечения (warez-сайт), то лицо, совершившее это деяние, подвергается наказанию по статье 2319, даже если величина ущерба не превысила 5000 долларов.

Примечание

Жертвой такого преступления считается не владелец вскрытой компьютерной системы, а владелец авторских прав.

Перехват (Закон 2511 Свода законов США)

Закон 2511 определяет ответственность за прослушивание телефонных переговоров. Считается незаконным прослушивание телефонных переговоров и перехват других типов электронных сообщений, что запрещает правоохранительным органам использовать прослушивающие устройства без наличия соответствующего ордера. Взломщик компьютерной системы, занимающийся снифингом, попадает под действие этого закона.

При чтении закона складывается такое впечатление, что некоторые типы мониторинга, выполняемые организациями, являются незаконными. Считается ли нарушением закона ситуация, когда организация размещает в своей сети контрольную аппаратуру для изучения электронной почты или отслеживания попыток выполнения атак? Оказывается, что для поставщиков службы связи (провайдеров) сделано исключение. Если организация является поставщиком службы связи, любой служащий организации может контролировать связь для "защиты прав или имущества поставщика данной службы". Если организация контролирует свои собственные сети и компьютерные системы с целью их защиты, то такая деятельность не является противозаконной.

Совет

Удостоверьтесь, что внутренняя политика вашей организации и процедуры включают в себя мониторинг сети. Политика и процедуры должны определять, какие служащие уполномочены выполнять такой мониторинг, а

также информировать остальных работников, что такой мониторинг имеет место.

Доступ к электронной информации (Закон 2701 Свода законов США)

Закон 2701 запрещает незаконный доступ к хранилищам систем связи, но в то же время запрещает ограничивать доступ авторизованных пользователей в такие системы. Этот закон содержит исключение для владельцев служб - для них разрешен доступ к файлам системы. Это означает, что любой файл в системе доступен для авторизованных служащих организации.

Другие уголовные законы

При совершении преступления с использованием компьютера для обвинения правонарушителя можно использовать не только уголовные законы, связанные именно с компьютерными преступлениями. Существуют другие правоохранительные акты, например, связанные с мошенничеством на почте или с мошенничеством с использованием электронных средств коммуникации. Помните о том, что с помощью компьютера можно совершить преступление, не имеющее отношения к компьютерным преступлениям. Компьютер или информация, хранящаяся на нем, могут составить доказательство во вполне определенном случае или помочь в расследовании.

Акт Патриота

Акт Патриота США от 2001 г. (официальное название акта "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" - "Сплачивающий и укрепляющий Америку надлежащими орудиями, требуемыми для пресечения терроризма и воспрепятствования ему") был принят в ответ на атаку террористов 11 сентября 2001 г. Некоторые разделы акта имеют непосредственное влияние на федеральные законы о компьютерных преступлениях.

Изменения в законе 1030

Акт Патриота увеличил максимальное наказание за нарушение закона 1030 до десяти лет за первое правонарушение и до двадцати лет - за последующие. В соответствии с новым законом, преступления, совершенные в Штатах, будут учитываться при вынесении приговора.

Одной из самых больших проблем в первоначальном варианте закона 1030 было требование выявления ущерба в размере 5 000 долларов. Акт Патриота модифицировал формулировку этого раздела закона, определив ущерб как "любое повреждение целостности или доступности данных, программ, систем или информации". Такое простое изменение позволяет гораздо проще

достичь искомой цифры в 5 000 долларов. Новая версия закона учитывает объединение нескольких видов ущерба для разных систем, если атаки злоумышленника происходили в течение одного года.

Понятие "ущерб" было расширено и включило любые оправданные потери жертвы. Сюда вошла стоимость возмещения убытков, стоимость определения величины ущерба и затраты на восстановление систем до рабочего состояния, ущерб, связанный с уменьшением дохода, и прочие издержки, возникшие из-за остановки служб.

В закон 1030 добавлен новый вид правонарушения. Считается, что лицо нарушило государственный закон, если его действия нанесли ущерб компьютерным системам, используемым правительством для целей правосудия, государственной обороны и государственной безопасности, независимо от суммы ущерба. Внесение этой поправки аннулирует констатацию факта наличия повреждений в случае атак, направленных против компьютерных систем Министерства обороны США.

И, наконец, если лицо, находящееся в Соединенных Штатах Америки, произвело атаку на компьютеры, расположенные вне страны, оно подлежит преследованию по федеральному закону - закон 1030 был дополнен определением такого вида атак.

Изменения в системе перехвата и отслеживания информации

До выхода в свет Акта Патриота закон 3127 об автоматической регистрации телефонных звонков (Pen Register Statute) разрешал правоохранительным органам осуществлять доступ к телефонным номерам, на которые выполнялись звонки с определенного телефона. Он разрешал доступ только к номерам, а не к содержимому телефонных разговоров. Закон был изложен специфическим техническим языком и ограничивал возможность получения информации.

Акт Патриота внес поправки в закон, включив в него любые устройства или процессы, с помощью которых записывается информация о дозвоне, маршрутизации, адресации и передаче сигналов. Акт не отменил запрета на запись содержимого разговоров. Используя нововведения в законе, стал возможен сбор следующей информации:

- заголовки электронной почты;
- IP-адреса отправителя и получателя;
- номера портов TCP и UDP отправителя и получателя.

Закон по-прежнему запрещает собирать следующую информацию:

- тема письма электронной почты;

- содержимое письма электронной почты;
- содержимое вложенных файлов.

В закон внесено еще одно изменение, которое облегчает правоохранительным органам расследование преступлений: перехват и отслеживание информации теперь может осуществляться локально с помощью устройств, установленных в других округах. Например, для расследования в Нью-Йорке вначале следует получить приказ на месте, и этот приказ будет иметь силу для сбора информации в Калифорнии. Единственным ограничением является то, что суд, выпускающий это постановление, должен иметь полномочия на рассмотрение такого рода правонарушений.

Исключения в законе, касающиеся нарушения владения

До выхода в свет Акта Патриота правоохранительные органы имели затруднения при отслеживании действий злоумышленника. Они должны были получить распоряжение на прослушивание телефонных разговоров, если жертва давала на это согласие. Акт Патриота внес поправки в законы 2511 и 2701. В изменении к закону 2511 отмечено, что лицо, получившее несанкционированный доступ в систему, лишается права на конфиденциальность. Согласно новым законам, для осуществления электронного перехвата необходимо следующее:

- согласие владельца;
- электронный перехват должен иметь отношение к расследованию;
- перехват не может использовать иные средства связи, кроме как ведущие к/от лицу, осуществляющему сбор данных.

Поправка к закону о кабельных коммуникациях

С тех пор как компании кабельной связи открыли доступ в интернет, возник серьезный конфликт между потребностями правоохранительных органов при расследовании компьютерных преступлений и существующим законодательством относительно раскрытия того, что провайдеры услуг связи отслеживают и/или делают в сети. Акт Патриота разрешает правоохранительным органам собирать информацию с помощью подслушивающей аппаратуры, методов перехвата и отслеживания (закон 3127, о котором говорилось выше).

Акт о национальной безопасности

Акт о национальной безопасности от 2002 г. (особенно Акт о расширенных мерах по обеспечению кибербезопасности, содержащийся в разделе 225) решает вопросы, касающиеся информационной безопасности. В основном Акт направлен на создание Министерства национальной безопасности, а

раздел 225 модифицирует закон 1030, увеличивая размер наказаний за криминальные действия. Он также предписывает Пенитенциарной комиссии США (United States Sentencing Commission) принимать во внимание серьезность компьютерных преступлений при вынесении приговора.

Законодательство штатов

В дополнение к статьям федерального законодательства, касающихся использования компьютера в преступных целях, в каждом штате разработаны свои законы. Эти законы отличаются от федеральных в отношении состава преступления (многие из них не имеют определения величины нанесенного ущерба) и наказания за преступление. В зависимости от того, где произошло преступление, местные правоохранительные органы могут быть больше заинтересованы в расследовании, чем федеральные службы. Поговорите с представителями местных правоохранительных органов и убедитесь в их заинтересованности и способности к расследованию компьютерных преступлений.

Помните о том, что федеральное законодательство часто меняется, и законы, связанные с компьютерными преступлениями, находятся в состоянии постоянного развития. Если у вас возникли вопросы по отдельным статьям законодательства, проконсультируйтесь с главным юрисконсультом вашей организации или представителями местных правоохранительных органов.

Концепция состава преступления зависит от штата. Некоторые штаты регламентируют цель компьютерного преступления - полное лишение владельца доступа к информации в результате ее кражи. Другие штаты требуют, чтобы информация на самом деле была утеряна, так что восстановление информации из архивной копии аннулирует факт нарушения закона.

Существуют различия и в определении способа доступа преступника к системе. В одних случаях рассматривается только факт реального взлома системы, в других принимаются во внимание именно попытки несанкционированного доступа. А в штате Юта, например, организациям разрешается атаковать компьютеры, с которых был выполнен взлом их компьютерных систем.

И, наконец, в отдельных штатах изменение или подделка заголовка электронной почты считается преступлением. Законы этих штатов направлены на борьбу с массовыми рассылками электронной почты (спамом).

Вне зависимости от того, в каком штате расположена ваша фирма, проконсультируйтесь с представителями местных правоохранительных органов и с главным юрисконсультом вашей организации и убедитесь, что вы

понимаете особенности законодательства вашего штата. Вы непосредственно столкнетесь с этим, когда будете заявлять в правоохранительные органы о компьютерном преступлении.

Вопросы для самопроверки

1. Как называется основный федеральный закон США в области компьютерных преступлений?
2. Какие изменения в законы США о компьютерных преступлениях внес Акт Патриота для облегчения процедуры вынесения обвинений в федеральном суде?

Законодательство других стран

В США законы, относящиеся к компьютерным преступлениям, различаются для каждого штата. В рамках мирового содружества это законодательство различается для каждой страны. Многие страны вообще не имеют соответствующих законов. Например, когда был установлен факт проживания хакера, написавшего вирус ILOVEYOU, в Филиппинах, выяснилось, что осудить его нельзя, поскольку в этой стране отсутствует закон, согласно которому написание и распространение компьютерного вируса является преступлением (позже такой закон был введен).

Законодательство в области компьютерных преступлений в других странах может оказывать влияние на расследование этих преступлений в США. Предположим, что в результате расследования установлено, что компьютерная атака выполнена с территории другой страны. В этом случае ФБР обращается к правоохранительным органам этой страны через официального представителя посольства США. Если в этой стране отсутствует законодательство в области компьютерных преступлений, то вряд ли она будет принимать участие в расследовании.

В следующих разделах приведен краткий обзор законодательства других стран. Дополнительную информацию вы можете получить от представителей иностранных государств (в посольстве или консульстве) или в ФБР.

Австралия

В федеральном законе Австралии определено, что несанкционированный доступ к данным в компьютерах является уголовным преступлением, наказание за которое - до шести месяцев лишения свободы (см. Законы Содружества наций, уголовный закон 1914). Наказание увеличивается до двух лет, если целью преступления было мошенничество, или если информация классифицируется как секретная правительственная, финансовая или являющаяся коммерческой тайной. Также считается незаконным, если злоумышленник получил несанкционированный доступ к

компьютерам, обслуживающим системы связи или транспортные коммуникации. Понятие величины минимального ущерба не определено, наказание в основном зависит от типа вскрытой информации.

Бразилия

В Бразилии определено два вида компьютерных преступлений: ввод ложных данных в информационные системы и несанкционированная модификация этих данных. Соответствующие законы направлены на служащих организаций, злоупотребляющих своими правами. Наказание за эти преступления составляет от 3-х месяцев до 12-ти лет лишения свободы, а также включает штрафы.

Индия

Хакинг компьютерных систем считается в Индии преступлением. Лицо признается виновным в совершении преступления, если в результате его действий в компьютерной системе произошло повреждение, удаление или изменение информации, и она утратила свою ценность. Хакер при осуществлении преступных действий стремится причинить ущерб или, по крайне мере, знает об этом. При вынесении обвинительного приговора наказание составляет от двух до трех лет тюремного заключения. На степень наказания не влияет величина ущерба, причиненного системе, или тип информации, к которой обращался злоумышленник.

Китай

Декрет 147 Государственного совета Народной Республики Китай от 18 февраля 1994 г. определяет два вида компьютерных преступлений. Первый - преднамеренный ввод компьютерного вируса в компьютерную систему. Второй - продажа нелицензионных программных продуктов. В любом случае наказанием является штраф, возможна и конфискация дохода, полученного незаконным путем.

В Гонконге также имеется ряд законов, направленных против компьютерных преступлений. В "Постановлении о средствах телекоммуникации", раздел 27А определено, что несанкционированный доступ к компьютеру через телекоммуникационную систему является преступлением. Осуждение влечет за собой большой штраф. Преступлением считается взлом компьютера со злоумышленным или нечестным намерением - это может быть получение незаконной выгоды или причинение ущерба. Наказанием является тюремное заключение сроком до пяти лет.

Примечание

В Гонконге сохранились многие законы, действующие еще до его присоединения к Китаю. Однако эти законы со временем могут измениться.

Великобритания

Несанкционированный доступ к материалам, содержащимся на компьютере, расценивается как преступление. Доступ выполняется с определенной целью, и лицо, осуществляющее это действие, не может не знать, что у него нет полномочий для его выполнения. Преступлением является несанкционированное изменение данных или действие, повлекшее за собой отказ в обслуживании компьютера. Наказание за эти преступления не зависит от того, выполнялась ли атака один раз или происходила в течение долгого времени.

При вынесении обвинительного приговора наказанием является штраф или лишение свободы сроком до шести месяцев. Срок тюремного заключения не может превышать пять лет.

Вопросы судебного преследования

Если ваша организация стала жертвой компьютерного преступления, то вы можете обратиться за помощью к правоохранительным органам, чтобы наказать обидчиков. Это решение не следует принимать в приступе гнева. Скорее всего, детальное рассмотрение всех параметров и процессуальных мероприятий нужно обсудить при выполнении ответных действий на инцидент. Во время этой процедуры ваша организация должна привлечь юристов и получить консультации от местных правоохранительных органов. Совместное обсуждение даст информацию относительно их возможностей, интереса в раскрытии преступления и о нанесенном ущербе (эту оценку нужно сделать заранее, до совершения реального взлома).

Примечание

После выявления инцидента проконсультируйтесь с главным юрисконсультом вашей организации, перед тем как обращаться к правоохранительным органам.

Сбор доказательств

Независимо от ваших намерений касательно судебного преследования нужно выполнить множество мероприятий в ходе расследования преступления и возвращения систем в рабочее состояние. Сначала мы рассеем один миф, широко распространенный в сфере безопасности. Миф заключается в том, что якобы требуются специальные меры предосторожности для сохранения доказательств, если вы решили преследовать преступника по суду, и если информация будет использоваться при вынесении приговора.

Давайте внесем ясность в этот вопрос. Во-первых, во время проведения стандартных деловых процедур в качестве доказательства может использоваться любая информация. Если вы обычно делаете резервные копии своих систем, то в них содержится информация о том, где произошла атака и что было при этом сделано, которая пригодится при расследовании. В этом случае не нужны никакие специальные предосторожности для сохранения информации как доказательства. Создание системным администратором резервных копий перед внесением в систему каких-либо изменений, чтобы зафиксировать состояние системы, - хорошая идея, однако это не является необходимым.

Примечание

Формально информация не является доказательством до тех пор, пока вы не передадите ее представителю правоохранительных органов. Поэтому то, что вы делаете, является сохранением целостности информации, а не защитой вещественных доказательств.

Второй пункт немного сложнее. Если организация обращается к внешнему консультанту для выполнения судебной экспертизы систем, то эти действия обычно не входят в практику стандартных деловых процедур. В этом случае необходимо соблюдать соответствующие предосторожности.

- Создать по крайней мере две копии образа жестких дисков компьютера.
- Ограничить доступ к одной из копий и надежно ее упаковать, чтобы идентифицировать любые попытки фальсификации.
- Создать защищенные контрольные суммы информации на дисках, чтобы идентифицировать изменение информации.

В любом случае процедура, которой следует придерживаться, должна быть разработана до инцидента, и при ее создании необходимо предварительно проконсультироваться с адвокатом организации и с представителями правоохранительных органов.

Следует принять во внимание и тот факт, что информация на компьютерной системе жертвы - это не единственное место для получения сведений об атаке. В файлах журналов сетевого оборудования или сетевых систем мониторинга тоже содержатся данные об инциденте.

Примечание

Если информацию, полученную с помощью стандартных деловых процедур, можно использовать как доказательство в суде, то не упускайте такой возможности и соберите необходимые сведения. Однако если вы несерьезно относились к созданию резервных копий, то пользы от них будет немного.

Если у вас возникли сомнения относительно собранной информации, свяжитесь с судебным экспертом или правоохранительными органами - в любом случае это правильный шаг.

Взаимодействие с правоохранительными органами

Перед тем как обращаться в правоохранительные органы, свяжитесь с главным юрисконсультом своей организации. Он должен присутствовать во время переговоров с представителями этих служб.

Как только представители правоохранительных органов появятся в вашей организации для проведения расследования, правила изменятся. Они будут действовать как судебные приставы-исполнители в соответствии с правилами, установленными для сбора информации, используемой в качестве вещественных доказательств. После получения резервных копий или информации, хранящейся в системе, они будут контролировать доступ к этим вещественным доказательствам и защищать их в соответствии с законом.

Вопрос к эксперту

Вопрос. Если в организации осуществляется мониторинг ее сети, то является ли это нарушением закона об электронном прослушивании?

Ответ. Организация является владельцем и оператором компьютерной сети, поэтому ей разрешено собирать подобную информацию. Это не является нарушением законов 2511 и 2701 об электронном прослушивании.

Более того, если сбор последующей информация связан с получением ее из сети, правоохранительные органы имеют право предъявить повестку для вызова в суд или ордер на получение дополнительных сведений. Эти документы позволят им сделать запрос на журналы от поставщика услуг связи или установить аппаратуру для мониторинга. Без предъявления ордера это сделать невозможно. В данном случае представители правоохранительных органов действуют опять же в соответствии со своими собственными процедурами.

Совет

Правоохранительным органам не нужен ордер, если информация предоставляется по собственному желанию (например, самой организацией). Однако, если их представители захотят получить данные с вашего сайта, лучше потребовать предъявления соответствующего ордера, поскольку это защитит вас от некоторой ответственности. Такой подход следует использовать, если организация является поставщиком услуг связи, и правоохранительным органам нужны журналы, где регистрируется

деятельность, осуществляемая в сети. В любом случае запрос о выдаче магнитных лент или файлов журналов должен пройти через юридическое ведомство организации.

Гражданские вопросы

Любой гражданин имеет право обратиться с гражданским иском по какому-либо вопросу. Вероятность для гражданских исков существует и по отношению к компьютерам или сохраненной на них информации. В этом разделе мы рассмотрим некоторые примеры. Однако не надо расценивать их как юридические советы. Для получения квалифицированного ответа следует обратиться к адвокату или главному юрисконсульту.

Вопросы, касающиеся служащих

Компьютеры и компьютерные сети в организации предназначены для того, чтобы служащие использовали их в деловых целях. Эта простая концепция должна быть разъяснена всем сотрудникам. Она означает, что организация является владельцем систем и сетей, и вся информация в системах доступна для нее в любое время. Таким образом, служащие здесь не имеют никаких личных прав. Убедитесь, что ваша политика в этом вопросе соответствует действующему законодательству, привлеките главного юрисконсульта организации к разработке этой политики. Помните о том, что правовые нормы о неприкосновенности личной жизни в разных штатах отличаются друг от друга.

Внешний мониторинг

Если организация является поставщиком услуг связи и компьютерных служб, то ей разрешено контролировать информацию в сети и использование сети (как уже было сказано выше, это исключение из закона об электронном прослушивании). Служащих необходимо проинформировать о том, что подобная деятельность возможна. Это должно найти отражение в политике, а при входе в систему они должны видеть соответствующее сообщение. Сообщение может выглядеть так.

Эта система принадлежит "название организации" и предназначена для использования авторизованными пользователями. Все действия на этом компьютере или в сети могут быть проверены. Любой пользователь системы соглашается на этот контроль. Пользователь не имеет никаких личных прав в данной системе. Вся информация об этой или другой компьютерной системе является собственностью "название организации". Доказательство незаконных действий может быть передано представителям правоохранительных органов.

Вопросы политики

В политике организации определяются операции, выполняемые в системах, и поведение служащих. Если служащие нарушают политику организации, на них может быть наложено взыскание, вплоть до увольнения. Для уменьшения возможных проблем с законом служащих нужно обеспечить копиями политик организации (включая политику безопасности и информационную политику); они должны письменно подтвердить, что политики получены и осмыслены. Эта процедура должна периодически повторяться (например, каждый год), чтобы служащие не забывали о существовании этих политик. В политиках следует предусмотреть обновление сообщения, появляющегося при входе в систему (никаких личных прав, ведение мониторинга и т. д.).

Некоторые служащие могут отказаться подписывать такие документы. Эту ситуацию необходимо урегулировать при содействии отдела кадров и юрисконсульта организации.

Ответственность за прохождение данных

При оценке риска в организации необходимо принимать во внимание ответственность за прохождение данных. Суть этой проблемы такова. Если в организации А не реализованы надлежащие меры безопасности, и злоумышленникам удалось успешно взломать одну из систем, то эта система может быть использована для атаки на организацию Б. В этом случае организация А несет ответственность перед организацией Б (см. рис. 5.1). Вся проблема в том, что организация А не предприняла необходимые меры для предотвращения случившегося инцидента. Эти меры определены в действующих стандартах (например, в ISO 17799) и в существующей практике деловых отношений. При повторном возникновении инцидента сотрудники отдела безопасности должны обсудить этот вопрос с главным юрисконсультом организации.

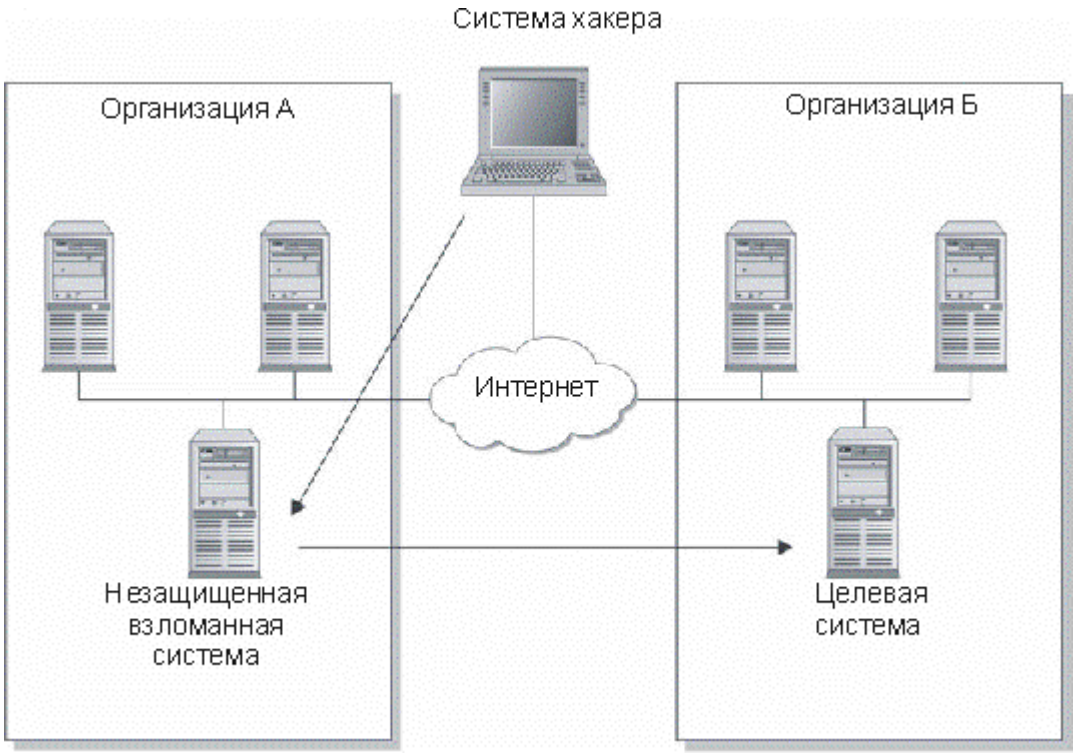

Рис. 5.1. Ответственность за прохождение данных

Вопросы конфиденциальности личной информации

Вопрос конфиденциальности личной информации в интернете на сегодняшний день превратился в центральную проблему. Мы уже сталкивались с подобной ситуацией при обсуждении личных прав служащих. Оказывается, это не единственная проблема, которая требует исследования и решения. В последние годы Федеральное правительство приняло соответствующие законы о конфиденциальности данных банковских и финансовых институтов.

Информация о клиенте

Информация о клиенте не является собственностью организации - она принадлежит клиенту. Таким образом, организация должна предпринимать надлежащие меры, чтобы защитить эту информацию от несанкционированного доступа. Это значит, что вы можете использовать эту информацию, но при этом должны соблюдать все меры предосторожности и употреблять ее только по назначению. Вот одна из причин, почему многие сайты в интернете помещают на своих страницах уведомление о том, что некоторые данные о клиенте могут использоваться в списках рассылки. В этой ситуации клиенты должны иметь возможность отказаться от использования их личной информации подобным образом.

Проблема, на которой я хочу заострить ваше внимание, - это доступ к личной информации клиента при взломе системы защиты. Какое решение примет организация, если она соблюдала все возможные меры предосторожности

для предотвращения этого взлома? В этой ситуации сотрудникам отдела информационной безопасности нужно работать вместе с генеральным юрисконсультом организации, чтобы рассмотреть все стороны этой проблемы и определить соответствующие меры.

Закон о переносимости и подотчетности документации о страховании здоровья

21 августа 1996 г. вышел в свет Закон о переносимости и подотчетности документации о страховании здоровья (Health Insurance Portability and Accountability Act, HIPAA). В этом законе сказано, что ответственность за создание и претворение в жизнь стандартов для защиты информации, касающейся здоровья, несет Министерство здравоохранения и социальных служб. Закон вводит стандартизацию информации о здоровье, уникальные идентификаторы пациентов и, что наиболее важно, стандарты безопасности для защиты конфиденциальности и целостности этой информации.

20 февраля 2003 г. Министерство здравоохранения и социальных служб США опубликовало правила техники безопасности HIPAA. Правила вступили в действие через 60 дней после опубликования (20 апреля 2003 г.). Установлены следующие даты ввода этих правил в различных организациях:

- организации планирования здравоохранения - 20 апреля 2005 г.;
- небольшие организации планирования здравоохранения (с годовым доходом в 5 млн. долларов и меньше) - 20 апреля 2006 г.;
- информационные центры - 20 апреля 2005 г.;
- службы здравоохранения - 20 апреля 2005 г.

Адресуемые и обязательные компоненты

В окончательно принятых правилах безопасности вводится понятие адресуемых компонентов. Многие положения правил являются обязательными для организации (они должны быть реализованы в обязательном порядке), а некоторые относятся к категории "применительно к организации"

Если в положение включен такой пункт, то организация должна оценить, является ли это положение для нее резонной и надлежащей мерой предосторожности. При положительной оценке необходимо обеспечить выполнение этого положения. В противном случае следует изложить в документальной форме, почему организация приняла такое решение, и разработать альтернативный механизм.

Требования правил безопасности

Правила безопасности включают общие положения и детальные требования в пяти специфических областях.

- Административные меры безопасности.
- Физические меры безопасности.
- Технические меры безопасности.
- Организационные требования.
- Политики, процедуры и требования к документации.

Основная цель этих положений состоит в том, чтобы гарантировать поддержку конфиденциальности, целостности и доступности защищенной информации о здоровье (Protected Health Information, PHI). Они позволяют использовать правильный подход к управлению риском при выполнении требований применительно к конкретной организации.

Любая организация, которая обрабатывает информацию о здоровье человека, должна изучить эти положения очень подробно и определить, что необходимо сделать. Организациям здравоохранения, конечно, потребуются существенные средства на обеспечение работы своих систем и выполнение процедур. Сотрудники отдела информационной безопасности в этом случае должны работать в тесном сотрудничестве с консультантом по вопросам соблюдения HIPAA и главным юрисконсультом организации.

Административные меры безопасности

HIPAA предписывает для каждой организации выполнение следующих требований.

- Управление безопасностью. Сюда входит регулярный анализ рисков; соответствующие меры безопасности для управления рисками; политика санкций, направленная на принудительное соблюдений требований; регулярный просмотр записей в журналах, содержащих информацию о выполняемых действиях.
- Назначение лиц, ответственных за безопасность. Должен быть назначен человек, отвечающий за вопросы безопасности.
- Меры безопасности, связанные с человеческим фактором. Следующие компоненты рассматриваются применительно к конкретной организации: процедуры авторизации, установление уровня допуска, процедуры увольнения.
- Управление доступом к информации. Обязательным компонентом является изоляция работы информационных центров здравоохранения. А эти компоненты рассматриваются применительно к конкретной организации: процедуры авторизации доступа, установления факта доступа и процедуры модификации.
- Понимание необходимости мер безопасности и обучение. Эти компоненты рассматриваются применительно к конкретной

организации: периодическое обновление положений безопасности; защита от вредоносного программного обеспечения; мониторинг входа в систему и управление паролями.

- Процедуры, связанные с возникновением инцидентов безопасности. Политики и процедуры, относящиеся к инцидентам безопасности, являются обязательными.
- План на случай возникновения непредвиденных обстоятельств. Эти компоненты являются обязательными: план создания резервных копий информации, план восстановления после стихийных бедствий и план действий в чрезвычайных обстоятельствах. Следующие компоненты рассматриваются применительно к конкретной организации: периодическая проверка и пересмотр планов, оценка относительной важности определенных приложений.
- Оценка. Необходимо проводить периодическую оценку защиты на местах в ответ на изменения в окружении.
- Контракты, связанные с ведением бизнеса, и другие мероприятия. Необходимо наличие контрактов, определяющих соответствующие меры безопасности, с любой организацией, совместно использующей PHI.

Физические меры безопасности

Правила безопасности HIPAA учитывают влияние общих физических мер безопасности, используемых в организации, на безопасность компьютеров и сетей. Поэтому сюда включены существенные требования для физической защиты.

- Управление доступом в помещение. Следующие компоненты рассматриваются применительно к конкретной организации: планы, разработанные на случай возникновения непредвиденных обстоятельств; план безопасности помещений; контроль доступа и подтверждения подлинности, процедуры для регистрации ремонтных работ и модификаций физических средств защиты.
- Используемые рабочие станции. Политика для определения физических параметров рабочих станций, с которых можно обращаться к PHI.
- Безопасность рабочих станций. Физические меры безопасности для всех рабочих станций, с которых можно обращаться к PHI.
- Контроль устройств и носителей информации. Эти компоненты являются обязательными: процедуры для размещения PHI и носителей, на которых она хранится, удаление PHI перед повторным использованием носителей. А эти компоненты рассматриваются применительно к конкретной организации: записи о перемещении аппаратных средств и носителей, создание резервных копий PHI перед этим перемещением.

Технические меры безопасности

Правила безопасности HIPAA содержат требования к техническим мерам безопасности. Определенные механизмы безопасности, которые организация выбирает для выполнения положений, могут отличаться в зависимости от оценки риска, произведенного организацией (и от прочих факторов). Ниже приведены эти требования.

- Управление доступом. Эти компоненты являются обязательными: назначение каждому пользователю уникального идентификатора, реализация процедур доступа в чрезвычайных обстоятельствах. Следующие компоненты рассматриваются применительно к конкретной организации: автоматический выход из системы и шифрование/дешифрование PHI.
- Управление аудитом. Включает реализацию механизмов для записи и исследования любой деятельности в системе, которая содержит PHI.
- Целостность. Разработка механизмов аутентификации электронной PHI.
- Аутентификация личности или объекта. Разработка механизмов подтверждения подлинности личности тех, кто пытается получить доступ к PHI.
- Безопасность при передаче данных. Следующие компоненты рассматриваются применительно к конкретной организации: механизмы обнаружения неправомочных модификаций PHI в процессе передачи и механизмы шифрования PHI.

Организационные меры безопасности

Правила безопасности HIPAA включают организационные требования, реализация которых ведет к модификации контрактов с партнерами и спонсорами. Любые контракты с организациями, которые будут обращаться к PHI, должны включать меры по обеспечению безопасности в качестве отдельных пунктов. Кроме того, документы, разрабатываемые органами планирования здравоохранения, должны предписывать спонсору выполнение соответствующих требований по защите PHI.

Политики, процедуры, и требования к документации

Каждой организации необходимо поддерживать надлежащие политики, процедуры и документацию. Вся документация должна храниться в течение шести лет с момента создания. Все политики и процедуры должны быть доступны тем, кто будет реализовывать механизмы безопасности. Политики и процедуры организации нуждаются в обновлении в ответ на изменения в окружении или эксплуатационных требованиях.

Закон о модернизации финансового обслуживания Грэма-Лича-Блайли

Закон о модернизации финансового обслуживания Грэма-Лича-Блайли (The Gram-Leach-Bliley Financial Services Modernization Act, GLBA) вышел в свет 12 ноября 1999 г. Важнейшие аспекты закона связаны с конфиденциальностью информации о клиентах. В связи с этой проблемой в подразделе A раздела 5 определено обязательство по защите частной информации клиентов. Раздел 502 запрещает финансовым организациям раскрывать частную информацию о клиенте, за исключением случая взлома систем организации, а также предписывает обеспечить для клиента возможность отказа от использования его личной информации.

В дополнение к вопросам конфиденциальности от финансовых институтов также требуется защита записей о клиенте от несанкционированного доступа. Данным вопросом занимались учреждения финансового надзора (Управление по контролю денежного обращения, Федеральная резервная система, Федеральная корпорация страхования депозитов и Управление по надзору за сберегательными учреждениями), которые издали совместное положение, содержащее конкретные требования. Этот документ называется "Межведомственные руководящие указания установленных стандартов по безопасности информации о клиентах" и доступен по адресу http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf.

Требования безопасности

Руководящие указания устанавливают требования к программе безопасности финансовых организаций в целом. Они включают следующее.

- Программа информационной безопасности. Каждая организация должна ввести в действие всестороннюю программу информационной безопасности, которая включает административные, технические и физические меры безопасности.
- Вовлечение руководства. Руководство организации должно одобрить программу и наблюдать за ее развитием, выполнением и непрерывным техническим обслуживанием.
- Оценка риска. Каждая организация должна проводить периодические оценки риска, выявляющие угрозы и уязвимые места.

Руководство и управление риском

Используя разработанную программу безопасности, организация руководит и управляет риском через развертывание следующих механизмов защиты.

- Управление доступом к информации.
- Физическое ограничение доступа к системам и записям.
- Шифрование секретной информации при ее передаче.

- Процедуры изменения и модификации системы не должны отрицательно влиять на безопасность.
- Процедуры двустороннего контроля, сегрегация режимов работы и фоновые проверки.
- Системы обнаружения вторжений для наблюдения за атаками.
- Процедуры ответных действий при возникновении инцидента.
- Защита окружающей среды для защиты записей от разрушения.

Руководящие указания требуют обучения сотрудников организации для осуществления программы, а также регулярных проверок на определение эффективности программы.

Примечание

Тестирование программы должно проводиться независимыми сторонами. Однако организация может проводить и свои собственные проверки.

Наблюдение за поставщиками услуг

Закон GLBA учитывает проблемы безопасности при вовлечении внешних сторонних организаций, предоставляющих финансовым институтам различные услуги. Эти организации могут получить доступ к секретной информации, поэтому их надо тщательно проверить. Руководящие указания определяют следующие требования.

- Должное усердие при отборе поставщиков услуг. Необходим серьезный подход к отбору сторонних организаций, предоставляющих свои услуги.
- Требования к поставщикам услуг о соблюдении безопасности. Организация должна требовать от своих поставщиков услуг соблюдения соответствующих мер безопасности - это оговаривается в контракте.
- Наблюдение за поставщиком услуг. Организация должна вести мониторинг сторонних организаций для наблюдения за выполнением обязательств по контракту.
- Корректировка программы. Организация должна вносить изменения в свою программу информационной безопасности, чтобы учитывать модификацию в технологиях и процедурах бизнеса, а также появление новых угроз.
- Отчет руководству. Организация должна периодические отчитываться перед руководством о выполнении статей своей программы безопасности.

Судебное преследование

Этот проект покажет вам, как можно применить к преступнику законы о компьютерных преступлениях. В качестве отправной точки используются результаты, полученные при выполнении проекта 2.

Шаг за шагом

1. Взгляните на стратегию атаки, разработанную в проекте 2.
2. Давайте предположим, что эта атака была успешной. Определите статьи Федерального закона о компьютерных преступлениях, которые были нарушены при выполнении этой атаки. Не забудьте оценить общий ущерб, нанесенный организации.
3. Теперь определите системы, которые можно использовать для сбора доказательств об атаке. Что это за доказательства?
4. Определите способы защиты этих доказательств.
5. Установите, если это возможно, источник атаки.

Выводы

Очевидно, что в этом случае нарушается закон 1030 Свода законов США. Однако, согласно закону 1030, величина общего ущерба должна составлять 5 000 долларов, поэтому нужно определить ущерб, причиненный в результате выполнения атаки. После определения взломанных систем не забудьте о проблемах, связанных с кредитными картами и авторскими правами. Утечка этой информации влечет за собой применение других статей закона.

Контрольные вопросы

1. Является ли сканирование порта системы, к которой у вас нет права доступа, федеральным преступлением?
2. Какова сумма минимального ущерба при нарушении Федерального закона о компьютерном мошенничестве и злоупотреблении?
3. Какие изменения внес Акт патриота для облегчения вынесения приговора преступникам?
4. По какой статье Федерального закона преследуется прослушивание (снифинг) информации?
5. Если обнаружен warez-сайт (сайт, содержащий коммерческое программное обеспечение, доступное для распространения), но владелец системы не может установить, что сумма ущерба составляет 5 000 долларов, попадает ли злоумышленник, организовавший такой сайт, под действие Федерального законодательства? Если да, то под действие какой статьи?
6. Какое главное отличие законов штатов США в области компьютерных преступлений от Федеральных законов?
7. Является ли кража конфиденциальной информации преступлением во всех штатах, где имеется соответствующее законодательство?

8. Как влияет законодательство других стран в области компьютерных преступлений на действия правоохранительных органов США?
9. Если в организации был произведен сбор доказательств с помощью стандартных процедур, но при этом не сделана криптографическая проверка контрольной суммы, считаются ли такие доказательства верными?
10. Что должны предъявить правоохранительные органы для сбора доказательств?
11. Если организация придерживается существующей практики деловых отношений, может ли она преследоваться за халатность?
12. Что является главной проблемой для выполнения обязательств?
13. Перечислите организации, которые уполномочены проводить аудит в соответствии с законом GLBA?
14. Какова главная цель положений закона GLBA?
15. К каким организациям применяются правила закона HIPAA?