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.

- **Примечание**
- Я не юрист, и эта лекция не содержит юридические советы. Ее целью является освещение некоторых юридических вопросов, связанных с безопасностью. Законодательство постоянно меняется, и поэтому по всем вопросам лучше обращаться к главному юрисконсульту 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 1039 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 "а" 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.
- **Примечание**
- В Закон 1030 США были внесены поправки после выхода Акта Патриота. Об этом будет рассказано дальше.
- **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 (см. раздел "Вопросы конфиденциальности личной информации" далее
- **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.