Содержание:

Введение

В мире информационных технологий все больший приоритет отдается защите данных. По мнению экспертов, наиболее важной проблемой, задерживающей информатизацию общества, является необходимость обеспечения надежного хранения личных данных, которая перетекает в условие поддержания национальной кибер-безопасности (социальной, экономической, политической и т.д.). В условиях применения технологий и электронно-вычислительной техники всеми странами сира производится большая работа по защите информации.

Развитие современных технологий порождается серьезной «ценой» информации. Процессы производства в организации имеют в своём составе материальный и нематериальный аспекты. Во-первых, это необходимые для производства материалы (оборудование, энергия, люди и т.п.). Вторая составляющая - технология производства, в своем роде «рецепт», уникальные шаги, позволяющие создать неповторимый продукт.

Информация играет важную роль не только в производственных процессах, но и является основой управления организацией, страховыми обществами, банками, организациями социальной сферы и т.д. Во многих из перечисленных случаев информация представляет большой интерес для криминальных элементов. Как и говорилось ранее, все преступления начинаются с утечки информации. Кроме того, с ростом применения компьютерных технологий в различных сферах становится возможным распространение разных злоупотреблений, связанных с использованием вычислительной техники (кибер-преступлений).

В данной работе будут рассмотрена история возникновения данной проблемы, а также какие решения для этого принимаются в двух сверхдержавах – США и России.

Проблема защиты информации.

Использование компьютерных систем обработки информации создало поле, которое обострило защиту информации, от несанкционированного доступа. Большинство проблем по защите информации в этих системах возникают из-за отсутствия четкой привязанности и отношения информации к носителю. Её копия и передача становится простым шагом в достижении цели. Нынешняя информационная система подвержена как внешним, так и внутренним угрозам.

Основная утечка информации связанна с нарушением информационной безопасности, источниками которых являются сами пользователи системы. По мнению экспертов, одной из наиболее опасных угроз является утечка информации, хранящейся и обрабатываемой внутри автоматизированной системы. Статистика показывает, что чаще всего угрозами являются бывшие сотрудники компаний, стремящиеся нанести организации как можно более сильный ущерб (финансовый, материальный). Всё это заставляет более пристально рассмотреть возможные каналы утечки информации и способы их предотвращения.

Перевод документооборота в электронную форму стал отправной точкой такого преступления, как использование чужих персональных данных в собственных целях. Поиск конфиденциальной информации, данных от банковских карт, паролей от соц. сетей т.д. - это только первые позиции в списке «Основные утечки в информационном поле».

В Соединенных Штатах Америки закон о правовой защите информации был принят с 1988 года. Россией так же принимаются подобные акты, начиная с 2006 года.

Защита информации в России

Главным документом, регулирующий информационное поле в сфере защиты, является Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.

Государство напрямую влияет и регулирует на защиту информации. Так в статье 12 (рис.1) этого закона перечислены виды отношений, которые попадают под данный закон.

Статья 12. Государственное регулирование в сфере применения информационных техно

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей;

4) обеспечение информационной безопасности детей.
(п. 4 введен Федеральным законом от 21.07.2011 N 252-ФЗ)

2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Рис.1. Выписка из ФЗ «Об информации» ст.12

Закон регламентирует обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации. Также этот закон регулирует деятельность обладателей какой-либо информации (рис.2)

Статья 16. Защита информации

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

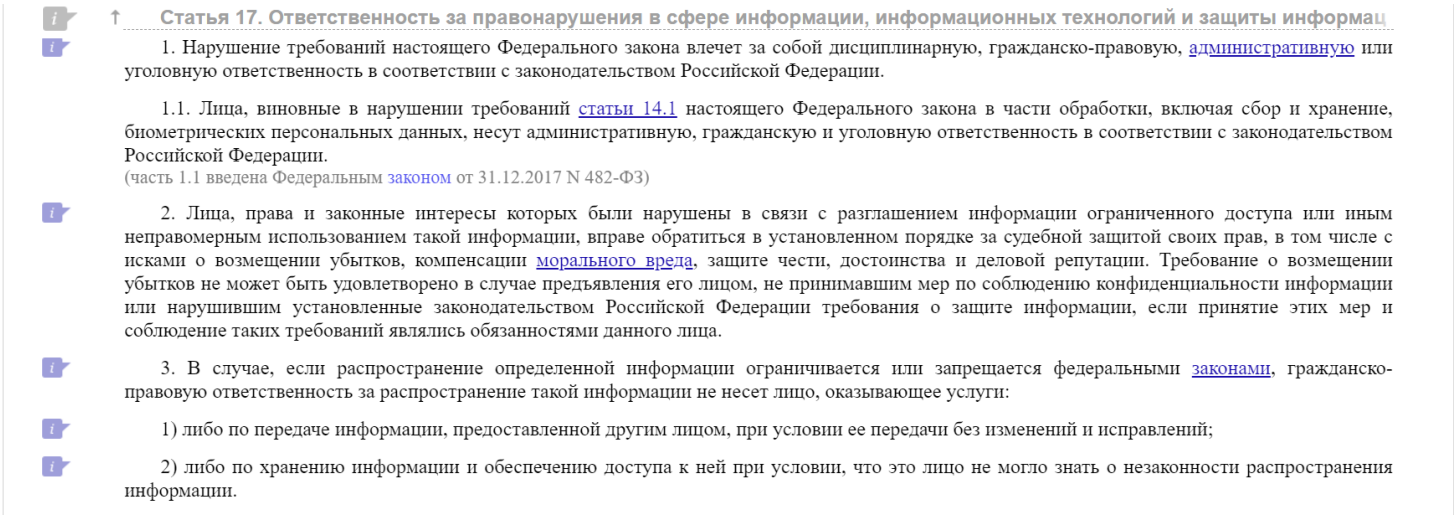
5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.
(п. 7 введен Федеральным законом от 21.07.2014 N 242-ФЗ)

Рис.2. Выписка из ФЗ «Об информации» ст.16 п. 4

В этом же законе предусмотрена ответственность (рис.3) за нарушение. Она затрагивает все 4 вида нарушений: дисциплинарную, гражданско-правовую, административную и уголовную, согласно законодательству Российской Федерации.



Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информац

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

1.1. Лица, виновные в нарушении требований статьи 14.1 настоящего Федерального закона в части обработки, включая сбор и хранение, биометрических персональных данных, несут административную, гражданскую и уголовную ответственность в соответствии с законодательством Российской Федерации.
(часть 1.1 введена Федеральным законом от 31.12.2017 N 482-ФЗ)

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3. В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

Рис.3. Выписка из ФЗ «Об информации» ст.17

Защита информации в США

Соединенные штаты Америки – страна с одной из наиболее развитой в мире информационной инфраструктурой. В этой стране существует наиболее жесткая система по защите информации, проникающая почти во все сферы государственной и общественной деятельности.

Ключевую роль в защите информации в США играет "Закон об информационной безопасности" (Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988). Его цель - реализация обеспечения безопасности информации без ограничений всего спектра возможных действий в федеральных компьютерных системах.

Характерно, что уже в начале Закона называется конкретный исполнитель - Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и правил, направленных на защиту от уничтожения и несанкционированного доступа к информации, выполняемых с помощью компьютеров. Таким образом, имеется в виду как регламентация действий специалистов, так и повышение информированности всего общества.

Согласно Закону, все операторы федеральных информационных систем (ИС), содержащих конфиденциальную информацию, должны сформировать базу и планы обеспечения информационной безопасности. Так же обязательным является и периодическое обучение всего персонала таких ИС. НИСТ, в свою очередь, обязан проводить исследования природы и масштаба уязвимых мест системы,

вырабатывать экономически оправданные меры защиты. Результаты исследований рассчитаны на применение не только в государственных системах, но и в частном секторе.

Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерство обороны, Министерство энергетики, Агентство национальной безопасности (АНБ) и т.д., чтобы избежать дублирования и несовместимости.

Существуют так же директивы, являющиеся основами для защиты информационного поля. Это директива PD/NSC – 24 «Политика в области защиты систем связи» и SDD – 145 «Национальная политика США в области безопасности систем связи автоматизированных информационных систем».

Еще одним толчком к принятию мер в защите информации стал террористический акт 11 сентября 2001 года. США предприняли ряд организационных и законодательных мер по повышению и усилению безопасности.

Совсем недавно, в 2015 году, в штате Калифорния был принят новый закон о конфиденциальности электронных коммуникаций
запрещает любому государственному правоохранительному органу или другому следственному органу принуждать бизнес передавать любые метаданные или цифровые сообщения — включая электронную почту, тексты, документы, хранящиеся в облаке — без соответствующего постановления. Он также требует постановление для отслеживания местоположения электронных устройств, таких как мобильные телефоны, или для их поиска.

Законопроект получил широкую поддержку среди сторонников гражданских свобод, таких как Американский союз гражданских свобод и Фонд электронных границ, а также передовых технологических компаний, таких как Apple, Google, Facebook, Dropbox, LinkedIn и Twitter.

Список литературы.

Интернет ресурсы:

1. Сайт «Консультант Онлайн». Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=182568188402075621770792013 3&

1. Сайт «Московского отделения Пензенского научно-исследовательского электротехнического института». Статья «Законодательство РФ в области защиты информации»

https://security.ru/legislation.php

1. Статья «Основные федеральные законы в сфере информационной безопасности»

https://www.securitylab.ru/blog/personal/shudrova/349419.php

1. Бормотов, В. Е. Проблемы защиты информации в компьютерной сети / В. Е. Бормотов. — Текст: непосредственный // Молодой ученый. — 2016. — № 11 (115). — С. 148-150
   https://moluch.ru/archive/115/31145
2. Сайт «Студопедия». Статья «Правовое регулирование информационной безопасности в США»
   https://studopedia.ru/6_14192_pravovoe-regulirovanie-informatsionnoy-bezopasnosti-v-ssha.html
3. Журнал «Wired». Закон «О цифровой конфиденциальности»
   https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law