УДК 004.056.5

МААЛЫМАТТЫК РЕСУРСТАРДЫ КОРГООНУН ЖОЛДОРУ ЖАНА ЫКМАЛАРЫ

Иванов Ю.В. – Б.Осмонов атындагы ЖАМУнун проф.Т.Бекболотов атындагы Аксы колледжи
edward_1988@bk.ru, тел: 0777 50-02-06

Анатация: *Адамдар өз сырларын коргоого умтулушат. Маалыматтык технологиялардын өнүгүшү, алардын адам ишинин бардык чөйрөлөрүнө кириши маалыматтык коопсуздук көйгөйлөрүнүн жыл сайын актуалдуу болуп, ошол эле учурда татаалдашып баратканына алып келет. Маалыматты иштетүү технологиялары тынымсыз өркүндөтүлүп, алар менен бирге маалыматтык коопсуздукту камсыз кылуунун практикалык ыкмалары да өзгөрүүдө.*

Ачкыч сөздөр: *Маалыматты коргоо, Маалымат технологиялар, Коркунучтардын булагы.*

СПОСОБЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Иванов Ю.В. ЖАГУ им Б.Осмонов Аксыйский колледж им. проф.Т.Бекболотова
edward_1988@bk.ru , тел: 0777 50-02-06

Анатация: *Людям свойственно защищать свои секреты. Развитие информационных технологий, их проникновение во все сферы человеческой деятельности приводит к тому, что проблемы информационной безопасности с каждым годом становятся всё более и более актуальными – и одновременно более сложными. Технологии обработки информации непрерывно совершенствуются, а вместе с ними меняются и практические методы обеспечения информационной безопасности.*

Ключевые слова: *Зашита информации, Информационные технологии, Источники угроз.*

WAYS AND METHODS OF PROTECTING INFORMATION RESOURCES

Ivanov Y.V. - JAGU named after B. Osmonov Aksy College named after Professor T. Bekbolotov
edward_1988@bk.ru, tel: 0777 50-02-06

Annotation: *People tend to protect their secrets. The development of information technologies, their penetration into all spheres of human activity leads to the fact that the problems of information security are becoming more and more relevant every year - and at the same time more complex. Information processing technologies are constantly improving, and with them the practical methods of ensuring information security are changing.*

Keywords: *Protected information, Information Technology, Sources of threats.*

Введение

Людям свойственно защищать свои секреты. Развитие информационных технологий, их проникновение во все сферы человеческой деятельности приводит к тому, что проблемы информационной безопасности с каждым годом становятся всё более и более актуальными – и одновременно более сложными. Технологии обработки информации непрерывно совершенствуются, а вместе с ними меняются и практические методы обеспечения информационной безопасности. Действительно, универсальных методов защиты не существует, во многом успех при построении механизмов безопасности для реальной системы будет зависеть от её индивидуальных особенностей, учёт которых плохо подаётся формализации. Поэтому часто информационную безопасность рассматривают как некую совокупность неформальных рекомендаций по построению систем защиты информации того или иного типа.1

Информационная сфера сегодня – не только одна из важнейших сфер международного сотрудничества, но и объект соперничества. Страны с более развитой информационной инфраструктурой, устанавливая технологические стандарты и предоставляя потребителям свои ресурсы, определяют условия формирования и осуществления деятельности информационных инфраструктур в других странах, оказывают воздействие на развитие их информационной сферы. Поэтому в промышленно развитых странах при формировании национальной политики приоритет получают развитие средств защиты и обеспечение безопасности информационной сферы. Концентрация информации в компьютерных системах вынуждает наращивать усилия по её защите. Национальная безопасность, государственная тайна, коммерческая тайна – все эти юридические аспекты требуют усиления контроля над информацией в коммерческих и государственных организациях. Работа, ведущаяся в этом направлении, привела к появлению новой дисциплины – «Информационная безопасность».

Специалист в области информационной безопасности отвечает за разработку, создание и эксплуатации системы, призванной обеспечить целостность, доступность и конфиденциальность циркулирующей в организации информации. В его функции входит обеспечение физической защиты (аппаратные средства, компьютерные сети), а также защиты данных и программного обеспечения.

Обеспечение информационной безопасности – дело не только очень дорогостоящее (затраты на покупку и установку технических и программных средств защиты могут составлять более половины стоимости компьютерной техники), но и очень сложное: при создании системы безопасности информации трудно определить возможные угрозы и уровень необходимой защиты, требуемый для поддержания информационной системы в рабочем состоянии. Современное информационное общество может формироваться и эффективно развиваться только в условиях правового государства, основанного на безусловном применении норм законодательства. Роль права в жизни информационного общества становится определяющей, все его члены должны исполнять нормы законов и разрешать возникающие споры цивилизованным способом на основе законодательства. 1

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных. Поэтому обеспечение информационной безопасности является одним из ведущих направлений развития информационных технологий. Рассмотрим основные понятия защиты информации и информационной безопасности:

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты – сама информация, носитель информации или информационный процесс, в отношении которых необходимо осуществлять защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации – желаемый результат защиты информации. Целью защиты информации может являться предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной потери (утечки) информации или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации – степень соответствия результатов защиты информации по отношению к поставленной цели.

Защита информации от утечки – деятельность по предотвращению распространения защищаемой информации (её разглашения), несанкционированного доступа к защищаемой информации и получения защищаемой информации злоумышленниками.

Защита информации от разглашения – предотвращение несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от несанкционированного доступа – предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами, собственником либо владельцем информации правил доступа к защищаемой информации. Заинтересованным субъектом может быть юридическое лицо, группа физических лиц, общественная организация, отдельное физическое лицо и даже государство.

Система защиты информации – совокупность органов и исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по установленным правилам, которые соответствуют правовым, организационно-распорядительным и нормативным документам по защите информации.

Под **информационной безопасностью** понимают защищённость информации от незаконного ознакомления, преобразования и уничтожения, а также защищённость информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной. (попытки проникновения злоумышленников, ошибки персонала, выход из строя аппаратных и программных средств, стихийные бедствия (ураган, землетрясение, пожар) и т. п.)1

Классификация и содержание возможных угроз информации Угрозы безопасности информации в современных системах её обработки определяются умышленными (преднамеренные угрозы) и естественными (непреднамеренные угрозы), разрушающими и искажающими воздействия внешней среды, надёжностью функционирования средств обработки информации, а также преднамеренных корыстным воздействием несанкционированных пользователей, целями которых являются хищение, уничтожение, разрушение, несанкционированная модификация и использование обрабатываемой информации. При этом под умышленными, или преднамеренными, понимаются такие угрозы, которые обусловливаются злоумышленными действиями людей. Случайными, или естественными, являются угрозы, не зависящие от воли людей. В настоящее время принята следующая классификация угроз сохранности (целостности) информации.

Источники угроз. Под источником угроз понимается непосредственный исполнитель угрозы с точки зрения её негативного воздействия на информацию. Источники можно разделить на следующие группы: — люди; — технические устройства; — модели, алгоритмы, программы; — технологические схемы обработки; — внешняя среда.

Предпосылки появления угроз. Существуют следующие предпосылки, или причины появления угроз:

— объективные (количественная или качественная недостаточность элементов системы) – не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы; — субъективные – непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.1

Угрозы информационным ресурсам проявляются в овладении конфиденциальной информацией, её модификации в интересах злоумышленника или её разрушении с целью нанесения материального ущерба.

Осуществление угроз информационной безопасности может быть произведено: через агентурные источники в органах коммерческих структур, государственного управления, имеющих возможность получения конфиденциальной информации;
Путём подкупа лиц, работающих на предприятии или в структурах, непосредственно связанных с его деятельностью;
Путём перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники, с помощью технических средств разведки и программно-математических воздействий на неё в процессе обработки и хранения;
Путём подслушивания переговоров, ведущихся в служебных помещениях, автотранспорте, в квартирах и на дачах;
Через переговорные процессы с зарубежными или отечественными фирмами, используя неосторожное обращение с информацией.
Через «инициативников» из числа сотрудников, которые хотят улучшить своё благосостояние с помощью «заработка» денег или проявляют инициативу по другим материальным или моральным причинам.1

Способы и методы защиты информационных ресурсов

Вместе с развитием способов и методов преобразования и передачи информации постоянно развиваются и методы обеспечения её безопасности. Современный этап развития этой проблемы характеризуется переходом от традиционного её представления как проблемы защиты информации к более широкому пониманию – проблеме информационной безопасности, заключающейся в комплексном её решении по двум основным направлениям.
К первому можно отнести защиту государственной тайны и конфиденциальных сведений, обеспечивающую главным образом невозможность несанкционированного доступа к ним. При этом под конфиденциальными сведениями понимаются сведения ограниченного доступа общественного характера (коммерческая тайна, партийная тайна и т. д.).
Ко второму направлению относится защита от информации, которая в последнее время приобретает международный масштаб и стратегический характер. При этом выделяют три основных направления защиты от так называемого информационного оружия (воздействия): – на технические системы и средства; – общество; – психику человека.
В соответствии с этим подходом уточнены и дополнены множества угроз информации, функции и классы задач по защите информации.1
Установление градаций важности защиты защищаемой информации (объекта защиты) называют категорированием защищаемой информации.2
Обеспечение безопасности информации требует сохранения следующих её свойств:
– целостности; – доступности; – конфиденциальности.

Целостность информации заключается в её существовании в неискажённом виде, т. е. неизменном по отношению к её исходному состоянию. Под целостностью информации понимается свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения.

Доступность – свойство, характеризующее способность информации обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.

Конфиденциальность – свойство, указывающее на необходимость введения ограничений на доступ к ней определённого круга пользователей, а также статус, предоставленный данным и определяющий требуемую степень их защиты.1
Деятельность, направленную на обеспечение информационной безопасности, принято называть **защитой информации.**
Методы обеспечения информационной безопасности весьма разнообразны.

Сервисы сетевой безопасности представляют собой механизмы защиты информации, обрабатываемой в распределённых вычислительных системах и

сетях. **Инженерно–технические методы** ставят своей целью обеспечение защиты информации от утечки по техническим каналам – например, за счёт перехвата электромагнитного излучения или речевой информации. **Правовые и организационные методы** защиты информации создают нормативную базу для организации различного рода деятельности, связанной с обеспечением информационной безопасности. **Теоретические методы** обеспечения информационной безопасности, в свою очередь, решают две основных задачи. Первая из них – это формализация разного рода процессов, связанных с обеспечением информационной безопасности. Так, например, формальные модели управления доступом позволяют строго описать все возможные информационные потоки в системе – а значит, гарантировать выполнение требуемых свойств безопасности. Отсюда непосредственно вытекает вторая задача – строгое обоснование корректности и адекватности функционирования систем обеспечения информационной безопасности при проведении анализа их защищённости. Такая задача возникает, например, при проведении сертификации автоматизированных систем по требованиям безопасности информации.1

Что касается подходов к реализации защитных мероприятий по обеспечению информационной безопасности, то сложилась трёхстадийная разработка таких мер.

I стадия – выработка требований – включает:

- определение состава средств информационной системы
- анализ уязвимых элементов информационной системы
- оценка угроз (выявление проблем, которые могут возникнуть из-за наличия уязвимых элементов)
- анализ риска (прогнозирование возможных последствий, которые могут вызвать эти проблемы)

II стадия – определение способов защиты – включает ответы на следующие вопросы:

какие угрозы должны быть устранены и в какой мере?

какие ресурсы системы должны быть защищаемы и в какой степени?

с помощью каких средств должна быть реализована защита?

какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учётом потенциальных угроз?

III стадия – определение функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты.2

Первоочередными мероприятиями по реализации политики обеспечения информационной безопасности государства являются: разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности; разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики; принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов, повышение правовой культуры и компьютерной грамотности общества, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения;

развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности.1

Реализация вышеперечисленных мер, обеспечивающих безопасность информационных ресурсов, существенно повышает эффективность всего процесса информатизации в организации, обеспечивая целостность, подлинность и конфиденциальность

дорогостоящей деловой информации, циркулирующей в локальных и глобальной информационных средах.2

Заключение

Процесс информатизации затронул практически все стороны жизни общества. Информатизация является характерной чертой жизни современного общества. Она пропитывает все направления человеческой деятельности. С появлением новых информационных технологий информация становится необходимым атрибутом обеспечения деятельности государств, юридических лиц, общественных объединений и граждан. От качества и достоверности информации, от её оперативности получения зависят многие решения, принимаемые на самых разных уровнях – от глав государств до рядового гражданина. Обеспечение информационной безопасности – комплексная задача, потому что сама информационная среда есть сложный и многоплановый механизм, где могут присутствовать такие компоненты, как персонал, электронное оборудование, программное обеспечение и т. д.

Для решения многих проблем обеспечения информационной безопасности необходимо применение следующих мер: законодательных, организационных и программно-технических. Игнорирование хотя бы одного из аспектов этой проблемы может привести к потере (утечке) информации, которая в жизни современного общества приобретает всё более важное значение и играет немаловажные роли.

Список литературы

1. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. краткий курс М.: Изд-во Феникс 2008.
2. Правовое обеспечение информационной безопасности: учеб. Пособие для студ. высш. учеб. заведений/(С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский и др.); под ред. С. Я. Казанцева. – 2-е изд., испр. и доп. – М.: Издательский центр «Академия», 2007. – 240 с.
3. Шаньгин В. Ф. информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «Форум»: Инфра-М, 2008 – 416 с.: ил. – (Профессиональное образование).
4. Сёмкин С.Н, Э. В. Беляков, С. В. Гребенев, В. И. Козачок. Основы организованного обеспечения информационной безопасности объектов информатизации. М.: Изд-во «Гелиос АРВ» 2005
5. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия – Телеком, 2006 -544 с.
6. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. краткий курс М.: Изд-во Феникс 2008
7. Правовое обеспечение информационной безопасности: учеб. Пособие для студ. высш. учеб. заведений/(С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский и др.); под ред. С. Я. Казанцева. – 2-е изд., испр. и доп. – М.: Издательский центр «Академия», 2007. – 240 с.