

УДК 004.77

ПРОБЛЕМЫ И ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ.

КОМПЬЮТЕРДИК СЕТТЕГИ МААЛЫМАТТЫ КОРГООНУН ПРОБЛЕМАЛАРЫ  
ЖАНА ОЗГОЧОЛУКТОРУ.

PROBLEMS AND PARTICULARITIES TO WIRED INFORMATION IN COMPUTER SET.

*Иванов Ю. – преподаватель,  
Аксы́йский колледж, ЖАГУ, [edward\\_1988@bk.ru](mailto:edward_1988@bk.ru)*

*Аннотация: Необходимо обеспечить секретность исследований в стратегически важных областях. Надо правильно распределять информацию и регулировать ее в современном обществе. Для этого возникает потребность в защите информации.*

*Стратегиялык жактан маанилүү жайларда изилдөөлөрдүн сырдуулугун камсыз кылуу. Азыркы коомдо маалыматты туура бөлүштүрүү жана башкаруу керек. Ошон үчүн маалыматты коргоо зарылдыгы келип чыкты.*

*It is necessary to provide secrecy of studies in strategic important areas. It needs correct distribution of information and adjust it in modern society. For that appears need for protection of information.*

К защищаемой относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации. Защитой информации называют деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.<sup>1</sup>

Наиболее остро необходимость в защите данных проявляется при использовании компьютеров для обработки, а также хранения информации секретного и частного характера. Проблема обеспечения необходимого уровня защиты информации оказалась весьма сложной, требующей для своего решения создания целостной системы организационных мероприятий и применения специфических средств и методов по защите информации. То есть становится актуальна проблема разработки эффективных систем защиты информации.<sup>2</sup>

Основные проблемы защиты информации при работе в компьютерных сетях, можно разделить на три группы:

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение работоспособности информационно-вычислительных систем.

Наиболее перспективными средствами защиты информации в компьютерных системах являются программные средства. Они позволяют создать модель защищенной системы с построением правил разграничения доступа, централизованно управлять процессами защит, интегрировать различные механизмы в единую систему, создавать удобный для пользователей интерфейс администратора безопасности. Не смотря на явные преимущества обработки информации в компьютерных сетях, возникает немало

<sup>1</sup> Хорев П. Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2006. – 430 с. - ISBN: 5-908916-87-8

<sup>2</sup> Материалы сайта «Защита информации и Информационная безопасность». [Электронный ресурс]. - Режим доступа: <http://www.zashita-informacii.ru>

сложностей при организации их защиты:

- расширенная зона контроля - следовательно, администратору отдельной подсети приходится контролировать деятельность пользователей, которые находятся вне пределов его досягаемости;

- неизвестный периметр - сети легко расширяются, и это ведет к тому, что определить четкие границы сети часто бывает сложно, один и тот же узел может быть доступен для пользователей различных сетей;

- использование разнообразных программно-аппаратных средств - соединение нескольких систем в сеть увеличивает уязвимость всей системы в целом, так как каждая система настроена на выполнение своих требований безопасности, которые могут оказаться несовместимы с требованиями на других системах;

- сложность в управлении и контроле доступа к системе - многие атаки на сеть могут осуществляться из удаленных точек без получения физического доступа к определенному узлу. В таких случаях идентификация нарушителя, как правило, бывает очень сложной;

- множество точек атаки - один и тот же набор данных в сетях может передаваться через несколько промежуточных узлов, причем, каждый из этих узлов является возможным источником угрозы. Кроме этого, к большинству сетей можно получить доступ с помощью коммутируемых линий связи и модема, что сильно увеличивает количество возможных точек атаки. Такой способ очень легко осуществить и столь же трудно проконтролировать, поэтому он считается одним из самых опасных. Уязвимыми местами сети также являются линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы, модемы и т. д.

Суть проблемы защиты сетей обусловлена их двойственным характером. С одной стороны, сеть - это единая система с едиными правилами обработки информации, а с другой, - совокупность отдельных систем, каждая из которых имеет свои собственные правила обработки информации. В связи с необходимостью обеспечить секретность исследований в стратегически важных областях, правильно распределять информацию и регулировать ее в современном обществе возникает потребность в защите информации.

К защищаемой относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации. Защитой информации называют деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.<sup>3</sup>

Наиболее остро необходимость в защите данных проявляется при использовании компьютеров для обработки, а также хранения информации секретного и частного характера. Проблема обеспечения необходимого уровня защиты информации оказалась весьма сложной, требующей для своего решения создания целостной системы организационных мероприятий и применения специфических средств и методов по защите информации. То есть становится актуальна проблема разработки эффективных систем защиты информации.<sup>4</sup>

Основные проблемы защиты информации при работе в компьютерных сетях, можно разделить на три группы:

- нарушение конфиденциальности информации;

---

<sup>3</sup> Хорев П. Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2006. – 430 с. - ISBN: 5-908916-87-8

<sup>4</sup> Материалы сайта «Защита информации и Информационная безопасность». [Электронный ресурс]. - Режим доступа: <http://www.zashita-informacii.ru>

- нарушение целостности информации;
- нарушение работоспособности информационно-вычислительных систем.

Наиболее перспективными средствами защиты информации в компьютерных системах являются программные средства. Они позволяют создать модель защищенной системы с построением правил разграничения доступа, централизованно управлять процессами защит, интегрировать различные механизмы в единую систему, создавать удобный для пользователей интерфейс администратора безопасности.

Не смотря на явные преимущества обработки информации в компьютерных сетях, возникает немало сложностей при организации их защиты:

- расширенная зона контроля - следовательно, администратору отдельной подсети приходится контролировать деятельность пользователей, которые находятся вне пределов его досягаемости;

- неизвестный периметр - сети легко расширяются, и это ведет к тому, что определить четкие границы сети часто бывает сложно, один и тот же узел может быть доступен для пользователей различных сетей;

- использование разнообразных программно-аппаратных средств - соединение нескольких систем в сеть увеличивает уязвимость всей системы в целом, так как каждая система настроена на выполнение своих требований безопасности, которые могут оказаться несовместимы с требованиями на других системах;

- сложность в управлении и контроле доступа к системе - многие атаки на сеть могут осуществляться из удаленных точек без получения физического доступа к определенному узлу. В таких случаях идентификация нарушителя, как правило, бывает очень сложной;

- множество точек атаки - один и тот же набор данных в сетях может передаваться через несколько промежуточных узлов, причем, каждый из этих узлов является возможным источником угрозы. Кроме этого, к большинству сетей можно получить доступ с помощью коммутируемых линий связи и модема, что сильно увеличивает количество возможных точек атаки. Такой способ очень легко осуществить и столь же трудно проконтролировать, поэтому он считается одним из самых опасных. Уязвимыми местами сети также являются линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы, модемы и т. д.

Суть проблемы защиты сетей обусловлена их двойственным характером. С одной стороны, сеть - это единая система с едиными правилами обработки информации, а с другой, - совокупность отдельных систем, каждая из которых имеет свои собственные правила обработки информации.

#### Литературы:

1. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2006. – 430 с. - ISBN: 5-908916-87-8
2. Материалы сайта «Защита информации и Информационная безопасность». [Электронный ресурс]. - Режим доступа: <http://www.zashita-informacii.ru>
3. Барсуков В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М., 2001 – 496 с.
4. Ярочкин В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. – М.: Академический проект: Трикта, 2005. – 544 с.
5. Барсуков В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. – 496 с., ил.
6. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия – Телеком, 2000. - 452 с., ил.

7. Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.]; под общ. Ред. А.П. Леонова. – Минск: АРИЛ, 2000. – 552 с.

Рецензент:

Раев З.Ж. – к.т.н., доцент