**Дата:16.12.2020**

**Группа: 19ИСиП 2**

**Наименование дисциплины: Компьютерные сети**

**Тема: Методы защиты информации в компьютерных сетях**

Рассмотрим основные понятия защиты информации и информационной безопасности компьютерных систем и сетей с учетом определений ГОСТ Р 50922—96.

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

**Объект защиты** — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

**Цель защиты информации** — это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

**Эффективность защиты информации** — степень соответствия результатов защиты информации поставленной цели.

**Защита информации от утечки** — деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

**Защита информации от разглашения** — деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

**Защита информации от НСД** — деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.

Заинтересованным субъектом, осуществляющим НСД к защищаемой информации, может выступать государство, юридическое лицо, группа физических лиц, в т. ч. общественная организация, отдельное физическое лицо.

**Система защиты информации** — совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Под **информационной безопасностью** понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной.

1. **Методы защиты информации**

Множество существующих методов обеспечения информационной безопасности можно классифицировать по разным признакам, но только уместные комбинации этих признаков позволяют сетевому администратору обеспечить надлежащий уровень информационной безопасности.
В целом все методы можно разделить на два класса:

1. организационно правовые методы, включающие воспитание у пользователей отношение недоступности и нетерпимости к нарушению информационной безопасности.
2. организационно технические методы. Правовые методы нашли отражение в серии документов международной и национальной организаций регламентирующие все аспекты обеспечения информационной безопасности. Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.

**Перечислим основные методы обеспечения информационной безопасности:**

**Авторизация**.
Этот метод позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.

**Идентификация** и аутентификация.
Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам.

**Аутентификация**- проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д. Последние годы активно внедряются следующие методы аутентификации:

- Биометрия. Используется аутентификация по геометрии руки, радужной оболочки сетчатки глаза, клавиатурный почерк, отпечатки глаза и т.п.

- SMART-карты (интеллектуальные карты). Их удобство заключается в портативном и широком спектре функций, которые могут быть легко модифицированы. Недостатком SMART-карты является их дороговизна, так как требуют определенных устройств для считывания информации.

- е-Token (электронный ключ) – аналог SMART-карты, выполненный в виде брелка, подключающегося через USB-порт. Достоинство e-Token заключается в том, что он не требует специальных, дорогостоящих карт -reader.

**Физическая защита**. Администратору сети необходимо знать все возможные точки физического проникновения в сеть или нанесения ущерба.

Физические устройства защиты:

* Физические устройства доступности к сетевым узлам и линиям связи.
* Противопожарные меры
* Защита поддержки инфраструктуры (электропитание, кондиционирование…)
* Защита мобильных и радио систем.
* Защита от перехвата данных.
* Поддержка текущей работоспособности.
* Резервное копирование.
* Управление носителями.
* Регламентированные работы.

Ещё 25—30 лет тому назад задача защиты информация могла быть эффективно решена с помощью организационных мер (выполнения режимных мероприятий и использования средств охраны и сигнализации) и отдельных программно-аппаратных средств разграничения доступа и шифрования. Этому способствовала концентрация информационных ресурсов и средств для их обработки на автономно функционирующих вычислительных центрах. Появление персональных ЭВМ, локальных и глобальных компьютерных сетей, спутниковых каналов связи, эффективных средств технической разведки и получения конфиденциальной информации существенно обострило проблему защиты информации.

Особенностями современных информационных технологий, прямо или косвенно влияющими на безопасность информации, являются:

1.  Увеличение числа автоматизированных процедур в системах обработки данных и усиление важности принимаемых на их основе решений;

2.  Территориальная распределенность компонентов компьютерных систем и передача информации между этими компонентами;

3.  Усложнение используемых программных и аппаратных средств компьютерных систем;

4.  Накопление и долговременное хранение больших массивов данных на электронных носителях, зачастую не имеющих твердых копий;

5.  Интеграция в единых базах данных информации различного назначения и различных режимов доступа;

6.  Непосредственный доступ к ресурсам компьютерных систем большого количества пользователей различных категорий и с различными полномочиями в системе;

7.  Рост стоимости ресурсов компьютерных систем.

Рост количества и качества угроз безопасности информации в компьютерных системах не всегда приводит к адекватному ответу в виде создания надежных систем защиты информации и информационных технологий.

**Меры по защите информации и сетей осуществляются в России нормами закона «Об информации, информационных технологиях и о защите информации»** [5].

В наиболее полной трактовке, под средствами сетевой безопасности имеются в виду меры предотвращения нарушений безопасности, которые возникают только при передаче информации по сетям, а также меры, позволяющие определять, что такие нарушения безопасности имели место.

**В современной практике выделяют следующие группы средств:**

·     организационные;

·     антивирусные;

·     защита с помощью паролей;

·     криптографические;

·     стенографические.

**Организационные методы защиты информации.**

Организационная защита информации — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией, включающая в себя организацию режима охраны, организацию работы с сотрудниками, с документами, а также организацию использования технических средств и работу по анализу угроз информационной безопасности.

Организационные методы создаются в каждой организации в соответствии с требованиями и условиями ее деятельности, в результате чего, в фирме имеются специфические способы и нормы защиты, однако, все они подчинены общим законам:

·     осуществление разработки политики безопасности бизнес-персоналом;

·     разграничение доступа к информации в соответствии с функционалом каждого специалиста;

·     отсутствие максимального доступа сотрудника к информации;

·     физическое разграничение административных и производственных процессов в сети;

·     организация сети на основе доменов.

Обеспечение защиты средств обработки информации и автоматизированных рабочих мест от несанкционированного доступа достигается системой разграничения доступа субъектов к объектам. Данная система реализуется в программно-технических комплексах в рамках операционной системы, систем управления базами данных или прикладных программ, в средствах реализации ЛВС, в использовании криптографических преобразований и методов контроля доступа.

Защита информации организационными средствами предполагает защиту без использования технических средств. Иногда задача решается простым удалением ОТСС (основных технических средств и систем) от границы контролируемой зоны на максимально возможное расстояние. Так же возможен вариант размещения, например, трансформаторной подстанции и контура заземления в пределах контролируемой зоны. К организационно-техническим можно отнести так же удаление ВТСС (вспомогательных технических средств и систем), линии которых выходят за пределы контролируемой зоны, запрещение использования ОТСС с паразитной генерацией для обработки информации, а также проведение специальных проверок технических средств на отсутствие закладочных устройств. Необходимо помнить, что организационно-технические меры требуют выполнение комплекса мер, предписанных нормативными документами.

При разработке СЗИ (средств защиты информации) так же следует принимать во внимание и то, что вся система состоит из более мелких систем. К ним относится: подсистема управления доступом, подсистема регистрации и учета, криптографическая защита информации и подсистема обеспечения целостности.

Общие принципы организации защиты конфиденциальной информации, применяемые при разработке СЗИ [2, c. 49]:

·     Непрерывность;

·     Достаточность;

·     Комплексность;

·     Согласованность;

·     Эффективность.

Для реализации мер защиты конфиденциальной информации должны применяться сертифицированные в установленном порядке технические средства защиты информации.

К мерам противодействия угрозам безопасности относят правовые, морально-этические, технологические, физические и технические меры. Морально-этические меры побуждают к созданию правовых мер (примером может быть неприязнь того, что кто-либо незнакомый Вам, может узнать Ваши фамилию имя и отчество, состояние здоровья или иную информацию личного характера). В свою очередь правовые меры побуждают к реализации организационных мер (разработка необходимых норм и правил при собирании, обработке, передаче и хранении информации), которые связаны с физическими и техническими мерами (технические средства защиты информации, физические барьеры на пути злоумышленника и т. д.).

Система безопасности — это организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия или государства от внутренних и внешних угроз, в задачи которой входит разработка и осуществление мер по защите информации, формирование, обеспечение и продвижение средств обеспечения безопасности, и восстановление объектов защиты, пострадавших в результате каких-либо противоправных действий.

Все эти задачи помогают в достижении целей своевременного выявления угроз, оперативного их предотвращения, нейтрализации, пресечения, локализации и уничтожения, а также отражения атак.

**Антивирусные методы защиты информации.**

Способы антивирусной защиты составляют технические и программные средства по защите информации от вирусов.

Вирус — это программа содержащая, вредоносный код, поэтому основным средством от их защиты является антивирусное ПО — приложение, обеспечивающее отслеживание и уничтожение вирусов.

Как и вирусы, антивирусы постоянно развиваются. Также постоянно расширяются общее определение и классификация антивирусного ПО.

**Антивирусная программа (антивирус)**— программа для обнаружения и лечения вредоносных объектов или инфицированных файлов, а также для профилактики и предотвращения заражения файла или операционной системы вредоносным кодом. Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить или предотвратить размножение, а также удалить компьютерные вирусы и другие вредоносные программы. Многие современные антивирусы позволяют обнаруживать и удалять также троянские программы и прочие вредоносные программы [4, c. 85].

Существует достаточно большое количество антивирусных программ. Наиболее эффективными, на мой взгляд, являются:

·     Антивирус Касперского (Россия);

·     NOD 32 (Словакия);

·     Symantec (США);

·     Dr. Web (Россия);

·     G DATA (Германия).

Как правило, все антивирусные программы платные. Существующие бесплатные программы, такие как Avast и Calm.AV, менее эффективны. Эффективность антивирусного ПО оценивается по проценту обнаруженных и обезвреженных вирусов и скорости реакции на вновь возникающие вирусные угрозы.

После успешного лечения компьютера от вирусов в системе все равно могут остаться неисправимые изменения, делающие систему неработоспособной. Поэтому лучшей защитой от вирусных атак является профилактика, заключающаяся в использовании проективной защиты, а также защиты компьютера от сетевых атак. Еще один действенный вариант — использование операционных систем семейства Linux, вирусы для которых на сегодня практически не получили распространения.

**Использование паролей для защиты информации.**

Использование надежного пароля является одним из наиболее важных факторов защиты компьютера от злоумышленников и других нежелательных пользователей.

Пароль — это условное слово или набор знаков, предназначенный для подтверждения личности или полномочий.

В 2003 году Infosecurity провели небольшое исследование, с целью выявления самых популярных паролей. Было опрошено 152 участника и в итоге были получены следующие результаты [3]:

·     16 % использовали собственное имя;

·     12 % использовали слово “password”;

·     11 % использовали название любимой спортивной команды;

·     8 % использовали дату рождения.

В начале 2013 года, в Лаборатории Касперского провели свое исследование с тем же вопросом, но уже в 25 странах. Картинка немного изменилась [3]:

·                        16 % использовали собственную дату рождения;

·                        15 % использовали сочетание цифр «123456»;

·                        6 % использовали слово “password” на местном языке;

·                        6 % использовали кличку домашнего животного.

Использование представленных паролей не может служить эффективной защитой информации. Пароль, несущий в себе высокую степень защиты, должен отвечать следующим требованиям:

·     длина не менее 6—8 символов;

·     использование цифр;

·     использование букв разных регистров;

·     использование букв разных алфавитов;

·     использование специальных символов;

·     отсутствие словарных выражений.

Использование паролей в организации также должно регламентироваться административными методами:

·     необходимо выделять программы и объекты информации, которые подлежать защите данным способом;

·     доступ к паролю к каждому ресурсу должен быть ограничен узким кругом ответственных лиц, как правило, исполнителем, пользующимся защищенным ресурсов, руководителем подразделения или системным администратором;

·     также должны быть разработаны правила хранения паролей, их смена в случаях взлома, утери и т. д.

**Криптографические методы защиты информации.**

Криптография — это комплексная наука о защите данных. Защита осуществляется на основе математических преобразований данных.

**Контрольные вопросы:**

1.Что включает в себя защита информации

2.Перечислите методы защиты информации

3. Что такое криптография

4. Антивирусные методы защиты информации

 Преподаватель\_\_\_\_\_\_\_\_\_А.К.Хунарикова