Современные подходы к защите информации, методы, средства и инструменты защиты

Домбровкая Л. А.[1], Яковлева Н. А.[2], Стахно Р. Е.[3]

[1]Домбровкая Лариса Александровна / Dombrovskaya Larisa Alexandrovna - кандидат педагогических наук, доцент;
[2]Яковлева Наталья Александровна / Yakovleva Natalia Alexandrovna - кандидат психологических наук;
[3]Стахно Роман Евгеньевич / Stahno Roman Evgenyevich - кандидат технических наук,
кафедра математики и информатики,
Санкт-Петербургский университет МВД России, г. Санкт-Петербург

Аннотация: *в статье рассмотрены современные подходы к построению систем защиты информации. Предлагаются оптимальные сочетания программных, организационных, физических и аппаратных свойств, применяемых на всех этапах обработки информации.*
Ключевые слова: *информационная безопасность, управление доступом, определение подлинности электронной подписи, обеспечение конфиденциальности информации.*

Необходимость защиты информации, содержащейся в информационных системах, в том числе государственных информационных системах (ГИС), устанавливает Федеральный Закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который обязывает владельца информации и оператора информационной системы обеспечить защиту информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий [2, с. 22] путем принятия правовых, организационных и технически мер, направленных на соблюдение конфиденциальности информации ограниченного доступа и реализацию права на доступ к общедоступной информации [2, с. 25].

Защита информации обеспечивается, в частности:

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

2) своевременным обнаружением фактов несанкционированного доступа к информации;

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

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

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

6) постоянным контролем за обеспечением уровня защищенности информации.

Реализация перечисленных и других мер создания эффективной системы информационной безопасности предполагает использование соответствующих подходов, методов и средств (инструментов) защиты информации.

Современные подходы к защите информации:

Системный подход к построению систем защиты, предполагающий оптимальное сочетание программных, организационных, физических и аппаратных свойств, применяемых на всех этапах обработки информации.

Принцип постоянного совершенствования системы. Современная защита информации предполагает постоянное совершенствование системы в соответствии с ростом рисков утечки информации. Данный процесс непрерывен и заключается в реализации современных методов и путей совершенствования систем информационной безопасности, постоянном контроле, выявлении её слабых мест и потенциальных каналов утечки информации. Непрерывное совершенствование систем обусловлено появлением новых способов доступа к информации извне.

Обеспечение надежности систем информационной защиты, т. е. контроль уровня надежности при отказе системы, возникновении сбоев, взломе и ошибках.

Контроль функционирования системы защиты. Непрерывное совершенствование средств и методов контроля над работоспособностью механизмов защиты.

Совершенствование методов борьбы с вредоносными программами и вирусами.

Оптимизация затрат на создание и эксплуатация систем контроля, выражающаяся в экономической целесообразности применения систем информационной безопасности.

К методам современной защиты информации можно отнести:

- криптографическую защиту различной степени конфиденциальности при передаче информации;
- управление информационными потоками как в локальной сети, так и при передаче каналами связи на различные расстояния;
- применение механизмов учета попыток доступа извне, событий в информационной системе и печатаемых документов;
- обеспечение целостности программного обеспечения и информации;
- внедрение средств восстановления современной защиты информации;

- осуществление физической охраны и учета техники и магнитных носителей;
- создание специальных служб информационной безопасности.

Современная защита информации предполагает внедрение в систему следующих основных **инструментов** защиты:

- управление доступом,
- механизмы шифрования (криптографические способы защиты информации),
- противодействие атакам вредоносных программ и вирусов,
- аппаратные средства защиты,
- физические средства защиты,
- программные средства защиты,
- организационные средства защиты,
- правовые и морально-этические средства защиты.

Рассмотрим кратко лишь некоторые средства (инструменты) защиты информации.

Управление доступом – средство защиты информации за счет регулирования использования всех информационных ресурсов, в т. ч. автоматизированной информационной системы организации. Управление доступом включает следующие функции защиты:

– идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);

– аутентификацию (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

– проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

– разрешение и создание условий работы в пределах установленного регламента;

– регистрацию (протоколирование) обращений к защищаемым ресурсам;

– реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основным и наиболее старым средством физического препятствия является установка прочных дверей, надежных замков, решеток на окна. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка противопожарной системы. Физические средства используются для охраны данных как на бумажных, так и на электронных носителях [1, с. 144].

Программные и аппаратные средства – незаменимый компонент для обеспечения безопасности современных информационных систем. Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации. Программные средства – программы, отражающие хакерские атаки. Кроме того, к программным средствам можно отнести программные комплексы, выполняющие восстановление утраченных сведений, а также реализующих парольную защиту в рамках управления доступом. При помощи комплекса аппаратуры и программ обеспечивается резервное копирование информации – для предотвращения потерь.

Организационные средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники организации хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных.

Правовые средства – комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации.

В сетях ЭВМ наиболее эффективными являются криптографические способы защиты информации. Если физические способы защиты могут быть преодолены путем, например, дистанционного наблюдения, подключения к сети или подкупа персонала, правовые не всегда сдерживают злоумышленника, а управление доступом не гарантирует от проникновения изощренных «хакеров», то криптографические методы, если они удовлетворяют соответствующим требованиям, характеризуются наибольшей надежностью.

Морально-этические средства – комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К данным средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе предприятия.

Следует отметить, что меры защиты информации, выбираемые для реализации в информационной системе, должны обеспечивать блокирование одной или нескольких угроз безопасности информации, включенных в модель угроз безопасности информации.

Систематическое применение всех перечисленных выше методов и средств современной защиты информации увеличивает надежность системы безопасности и предотвращает разглашение конфиденциальной информации.

Литература

1. *Кияев В., Граничин О*. Безопасность информационных систем. Открытый Университет «ИНТУИТ». 2016. 192 с.
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: [Электронный ресурс]. – Режим доступа: http://www.consultant.ru.