**Информационная безопасность: методы и средства защиты данных**

Бурнаева Е. М.

Бурнаева А. А.

*Тихоокеанский государственный университет*

На сегодняшний день развитие информационных технологий привело к тому, что информационная безопасность становится важной составляющей любой сферы. В данной статье рассматриваются основные методы и средства защиты информационных данных.

В настоящее время всеобщая компьютеризация ведет к тому, что значимость информационной безопасности, а именно защиты данных, становится обязательной. В современном обществе сформировался огромный класс систем обработки информации, разрабатывая которые, первостепенную роль и огромное значение отводится фактору безопасности (например: банковская система). Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования информационных систем, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в информационной системе.

Так, именно защита информационных данных помогает предотвратить несанкционированное использование, а также искажение или разрушение информационных ресурсов системы.

Для того, чтобы обеспечить защиту данных необходимо не только разработать частные механизмы защиты, а реализовать системный подход, который будет включать комплекс взаимосвязанных мер (к примеру, использование специальных технических и программных средств, нормативно-правовых актов, организационных мероприятий и т.д.) [2].

Защита информации – совокупность организационных, технических, а также правовых действий и мероприятий, которые помогают предотвратить угрозы информационной безопасности, а также способны устранить их последствия в процессе [1]. Что касается безопасности информационной системы, то в широком смысле понимается защищенность данных от намеренного или случайного вмешательства в процесс ее функционирования, а также хищения информации, модификации ее компонентов.

Угроза безопасности информации характеризуется действиями или событиями, способными привести к искажению, незаконному использованию, а также полностью уничтожить информационные ресурсы управляемой системы.

Создание систем информационной безопасности базируется на следующих ключевых принципах [4]:

-принцип непрерывного развития системы, который является одним из важнейших для компьютерных информационных систем, так как включает в себя непрерывный контроль, а также выявление слабых мест системы, потенциальных способов утечки данных;

-принцип разделения и минимизации полномочий по доступу к необходимой информации, для того, чтобы обрабатывать информацию было невозможно без предварительной регистрации;

-принцип надежности системы защиты, который поможет избежать утечки данных в случае сбоев в системе, взлома, а также случайных ошибок пользователей;

-принцип обеспечения контроля за функционированием системы защиты, необходимый для того, чтобы обеспечить контроль работоспособности механизмов защиты;

-принцип обеспечения различных средств по борьбе с вирусными программами;

-принцип обеспечения экономической целесообразности использования системы защиты, который заключается в расчете стоимости возможного ущерба и стоимости разработки средств защиты данных.

Система информационной безопасности должна иметь и собственное программное обеспечение, с помощью которого будет способна выполнять свою функцию. К видам программного обеспечения можно подразделить следующим образом:

-правовое обеспечение, характеризуется совокупностью нормативно-правовых документов, законодательных актов, положений, инструкций, требования которых являются обязательными в рамках сферы их деятельности в системе защиты информации;

-организационное обеспечение, характеризуется тем, что реализация информационной безопасности осуществляется определенными структурными единицами, такими, например, как служба безопасности фирмы и ее составные структуры: охрана, режим;

-информационное обеспечение, характеризуется тем, что включает в себя данные, сведения, показатели и параметры, которые лежат в основе решения задач, обеспечивающих функционирование систем информационной безопасности, к примеру: показатели учета, доступа, хранения, а также информационное обеспечение расчетных задач различного характера, связанных с деятельностью службы безопасности;

-техническое обеспечение, характеризуется использованием технических средств, которые необходимы как для обеспечения деятельности системы информационной безопасности, так и для защиты информации;

-программное обеспечение, характеризуется определенными статистическими, учетными, расчетными программами, которые обеспечивают оценку наличия и возможной опасности различных каналов утечки;

-математическое обеспечение, характеризуется методами, которые используются для различных расчетов, связанных с оценкой опасности технических средств, которыми располагают мошенники;

-лингвистическое обеспечение, характеризуется совокупностью определенных языковых средств общения специалистов и пользователей в сфере обеспечения информационной безопасности;

-нормативно-методическое обеспечение, характеризуется такими же критериями, как и правовое.

Необходимо отметить, что на сегодняшний день ведущая роль отводится организационным мероприятиям, следовательно, возникает вопрос об организации служб безопасности. Политика безопасности заключается в реализации контроля за функционированием информационной системы, настройками средств ее защиты.

Таким образом, соблюдение данных принципов позволит избежать значительного ущерба и возможных потерь, которые могут возникнуть в случае возникновения реальной угрозы.

К методам и средствам обеспечения защиты данных относят следующие:

-препятствие, т.е физическое преграждение пути к защищаемой информации;

-управление доступом, т.е. противостояние всевозможному несанкционированному доступу к информации. Сюда можно отнести следующие функции защиты: идентификация пользователей, опознание, проверка полномочий, регистрация, реагирование [5];

-механизм шифрования – криптографическое закрытие информации. Информационное сообщение, которое уже готово к отправке (первоначально открытое и незащищённое), шифруется и преобразуется в шифрограмму (закрытый текст, либо же вовсе графическое изображение документа). Далее передается по каналу связи (возможно и не защищенному), пользователь получает и дешифрует (раскрывает) его с помощью обратного преобразования криптограммы и получает исходный вид сообщения. Данному методу присуще использование специального алгоритма, действие которого запускается уникальным числом, который обычно и называют «шифрующим ключом» [3];

-использование антивирусных программ;

-регламентация, создание автоматизированной системы обработки, передачи и хранения данных;

-принуждение, соблюдение правил обработки, передачи и использования защищаемой информации под угрозой уголовной, материальной или административной ответственности [6].

Таким образом, противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера, применение которых позволит сохранить необходимые данные.

Обеспечение информационной безопасности является важным предметом, требующим пристального внимания, так как внедрение новых технологий, без должного обеспечения информационной защиты, становится источником новых серьезных проблем.

Список использованной литературы

1. Галатенко, В.А. Основы информационной безопасности. www.intuit.ru.
2. Титоренко Г.А. Информационные технологии управления. М., Юнити: 2014.
3. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика, Электронинформ, 2015.
4. Зегжда Д. П. Основы безопасности информационных систем. М.: Горячая линия-Телеком, 2020.
5. Крылов В. В. Информационные компьютерные преступления. М.: 2015.
6. Батурин Ю. М. Компьютерные преступления и компьютерная безопасность. М.: Юридическая литература, 2014.
7. Варлатая, С. К. Угрозы безопасности информации на игровых сервисах и методы защиты от них / С. К. Варлатая, Д. С. Колесникова // Молодой ученый. – 2016. – № 6 (110). – С. 41-44.