

УДК 004.056.53

ОСОБЕННОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПАНИЯХ

*Шустерова А. Н., студентка 3 курса экономического факультета
Научный руководитель - Голубев С. В., к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ*

Ключевые слова: защита информации, утечка информации, средства защиты информации, конфиденциальность данных, информационная безопасность, целостность, доступность.

Несмотря на развитие высоких технологий по защите данных, их уязвимость всё же подвергается вмешательствам со стороны хакеров. Поэтому актуальность проблем, связанных с защитой информации, все более усиливается.

Данная проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач, к которым можно отнести следующие:

- конфиденциальность данных;
- идентификация пользователя на основе анализа кодов [2].

Обеспечение информационной безопасности актуально для корпораций со сложной, многоуровневой структурой, таких как крупные банки, транснациональные и государственные компании (рисунок 1).

Защита информации – комплекс мероприятий, направленных на обеспечение целостности, доступности и конфиденциальности информации [3].

На сегодняшний момент сформулировано два базовых принципа по защите информации:

- защита от сбоев, ведущих к потере информации - ведется в направлении повышения надежности отдельных элементов и систем;
- защита от неавторизованного создания данных - обеспечивается физической защитой информации.

Следует подчеркнуть, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных от атак в компьютерных системах.

Атака - это совокупность действий злоумышленника, результатом которых может стать несанкционированный доступ нарушителя к информации.



Рисунок 1 - Направления обеспечения информационной безопасности



Рисунок 2 - Классификация сетевых атак

Существуют два основных типа атак: пассивные и активные. Пассивные - данные на компьютере отслеживаются и позже используются для вредоносных интересов, в то время как активные атаки включают изменения, при которых данные будут удалены (рисунок 2).

Таким образом, главными задачами любой системы информационной безопасности являются:

- обеспечение конфиденциальности сведений;
- обеспечение доступности данных для авторизированных пользователей;
- гарантия целостности информации, ее актуальности и защищенности от несанкционированного воздействия [1].

Библиографический список

1. Studopedia [Электронный ресурс] / Защита информации в корпоративных сетях экономических ИС. – Режим доступа: http://studopedia.ru/6_163840_zashchita-informatsii-v-korporativnih-setyah-ekonomicheskikh-is.html
2. Колешин, Г.М. Обязанности работника в отношении коммерческой тайны работодателя / Г.М. Колешин // Трудовое право.- 2014.- N 5.
3. Защита информации [Электронный ресурс]: реферат. – Режим доступа: <http://xreferat.com/33/6489-1-zashita-informacii.html>

PROTECTION OF INFORMATION IN COMPANIES

Shusterova A. N.

Key words: information security, information leakage, protection of information, data privacy, information security, integrity, availability.

Despite the development of advanced technologies for data protection, vulnerability still may be subject to interference from hackers. Therefore, the relevance of the problems related to the protection of information continues to escalate.