

Иремадзе Э.О.,

доцент, кандидат химических наук,

Стерлитамакский филиал Башкирского государственного университета г.

Стерлитамак, Россия

Имангулова Р.А.,

студент

2 курс, экономический факультет

Стерлитамакский филиал Башкирского государственного университета

г. Стерлитамак, Россия

Кибешева И.И.,

студент

2 курс, экономический факультет, Стерлитамакский филиал Башкирского

государственного университета

г. Стерлитамак, Россия

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

***Аннотация:** В данной статье рассматриваются вопросы, касающиеся безопасности информационных систем, приведены основные этапы построения системы безопасности ИС. Также, представлена классификация основных возможных угроз и меры их устранения.*

***Ключевые слова:** информационная система, безопасность информационных систем, угроза безопасности, вирусы.*

***Abstract:** This article discusses issues related to the security of information systems, describes the main stages of building an IP security system. Also, a classification of the main possible threats and measures to eliminate them are presented.*

***Keywords:** information system, security of information systems, security risk, viruses.*

Информационные технологии активно развиваются в самых разных сферах человеческой деятельности. Внедрение унифицированных технологий, таких как IP и Internet позволило промышленным системам управления перейти на новый, более высокий уровень. Интернет сегодня - это технология, которая полностью меняет весь уклад нашей жизни, меняет характер работы и даже способы общения людей друг с другом. Современное развитие мировой экономики с каждым разом становится все более зависимым от значительного объема информационных потоков. Эффективное применение информационных технологий является одним из важнейших факторов конкурентоспособности предприятия. Электронная коммерция, продажа информации в режиме on-line и прочие услуги становятся ведущими видами деятельности для определенных компаний. Однако, несмотря на все возрастающие усилия по созданию технологий защиты данных, их уязвимость не только не уменьшается, но и постоянно растет. Поэтому проблемы, связанные с защитой информационных данных различных предприятий являются весьма актуальными на сегодняшний день [1].

Информационная безопасность - это состояние информации, при котором исключается или существенно затрудняется нарушение ее секретности и целостности. При этом, информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании [2].

На сегодняшний день установлено три основных принципа, которые должна обеспечивать информационная безопасность:

1. Целостность данных. Подразумевает защиту от сбоев, которые ведут к потере информации, а также защита от неавторизованного создателя или уничтожения данных;
2. Конфиденциальность информации - обязательное требование не передавать информацию третьим лицам без согласия ее обладателя;
3. Доступность информации для всех авторизованных пользователей [3].

Современные ИТ обладают рядом признаков, которые включают в себя криптографическую защиту информации различной степени конфиденциальности при передаче данных; необходимость регистрации и учета попыток несанкционированного доступа; наличие средств восстановления системы защиты информации и многое другое. Однако, несмотря на новые усиливающиеся методы безопасности информационных систем, они по-прежнему содержат много уязвимостей. Источники угроз используют их для получения нелегальной выгоды путем нарушения безопасности информации [4].

Как известно, информационная система может подвергаться угрозам в любое время и для того, чтобы это предотвратить должен быть осуществлен постоянный контроль над безопасностью системы, ограничен доступ для незарегистрированных пользователей и многое другое [5].

Под угрозой безопасности информационных систем понимают возможность воздействия на информационную систему, которое прямо или косвенно может нанести вред ее безопасности. Существует множество классификаций угроз безопасности ИС. Мы рассмотрим основные из них [6].

Опасные угрозы безопасности информационных систем подразделяются на случайные и преднамеренные. Преднамеренные угрозы связаны непосредственно с целенаправленными действиями нарушителей. Их классифицируют в зависимости от того, кто выступает в качестве «агента угрозы» [7].

Первым и наиболее серьезным «агентом» угрозы являются террористы. Они заинтересованы в том, чтобы, нарушив процессы мониторинга и контроля управления, вывести систему безопасности из строя. Тем самым получить полный контроль над системой и использовать ее в своих интересах.

Вторым важным «агентом» угрозы для безопасности информационных систем являются инсайдеры. Инсайдер – внутренний пользователь, хорошо разбирающийся в системе и знающий ее изнутри. Он имеет доступ к конфиденциальной информации и может умышленно повредить оборудование или программное обеспечение. Администраторы и инженеры, у которых есть

доступ к системе, также могут неумышленно нанести вред ее функционированию, допустив ошибку в настройках системы [8].

Следующей угрозой выступают так называемые хакеры. Хакеры — это люди, хорошо разбирающиеся в программном обеспечении. Они заинтересованы в получении доступа к системе и контролю над ней любыми возможными путями взлома.

Случайные угрозы безопасности информационных систем могут быть вызваны рядом причин:

- аварийные ситуации из-за стихийных бедствий или отключения электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи из-за воздействий внешней среды.

Также выделяют классификацию угроз по разновидности нарушений:

- Угрозы нарушение конфиденциальности. Они направлены на разглашение секретной информации;
- Угрозы нарушения целостности информации. Нарушение приводит к искажению или полному уничтожению передаваемой информации;
- Угрозы нарушения работоспособности снижают работоспособность ИС и блокируют доступ к ее реестрам.

Абсолютно все информационные системы подвержены угрозам со стороны компьютерных вирусов, сетевых червей, троянских программ и программ «шпионов». Вирусы могут находиться не только в документах и вложениях, но и в аудио и видеофайлах. По статистике, компьютер каждого третьего пользователя Интернета в развитых странах хотя бы раз в течение года подвергается атакам компьютерных вирусов. Сейчас не осталось таких типов файлов, которые невозможно заразить вирусом. Также набирают обороты специальные вирусы, которые переносятся между мобильными телефонами и другими устройствами, в которых используется программное обеспечение.

Универсального способа для преодоления взломов пока не найдено. Сейчас, в современном обществе, человек задается вопросами: что необходимо сделать, чтобы сохранить личную информацию? И как сохранить безопасность информационных систем важных государственных объектов?

Для того чтобы хоть как то обеспечить безопасность информационной системы необходимо разработать комплексную систему защиты ИС которую можно разделить на несколько этапов:

1 этап: Необходимо оценить и обследовать безопасность ИС, проанализировать возможные угрозы и найти способы их предотвращения.

2 этап: Разработка системы информационной безопасности, проработка технической и организационной части функционирования системы;

3 этап: Внедрение информационной системы, защита данных и доступа к системе.

4 этап: Поддержка работоспособности информационной системы и постоянное ее улучшение.

Информационная безопасность относится к числу дисциплин, которые развиваются чрезвычайно быстро. Этому способствуют как общий прогресс информационных технологий, так и постоянное противостояние нападающих и защищающихся. Следовательно, важность защиты информационных систем - одна из актуальных проблем на сегодняшний день. Безопасность ИС – это необходимая составляющая любого технологического процесса. Информационные системы очень уязвимы и нуждаются в постоянном повышении защищенности данных и информационных продуктов.

Использованные источники:

1. Григорьева Т.В., Иремадзе Э.О., Белобородова Т.Г. Прогнозирование возможности банкротства предприятия на основе модели Альтмана // В сборнике: инновационные технологии в промышленности: Образование, Наука и Производство // Сборник материалов Всероссийской научно-практической конференции с международным участием. 2016. С. 322-323.

2. Иремадзе Э.О., Григорьева Т.В., Абуталипова Е.М., Белобородова Т.Г. Математическая модель планирования оптимальных финансовых результатов нефтехимического предприятия // Нефтегазовое дело. 2016. Т. 14. № 4. С. 215-220.
3. Иремадзе Э.О., Григорьева Т.В., Сакаева Э.З. Прогнозирование и анализ показателей финансовой устойчивости предприятия на основе математического моделирования // Вестник Московского государственного открытого университета. Москва. 2010. № 3. С. 78.
4. Бочкарева Е.А., Иремадзе Э.О. Оценка инвестиционной привлекательности и расчет риска банкротства страховой компании СПАО «Ингосстрах» // В сборнике: Математические методы и модели в исследовании актуальных проблем экономики России // Сборник материалов Международной научно-практической конференции. Ответственный редактор Р.Р. Ахунов. 2016. С. 188-193.
5. Захаров И.В., Иремадзе Э.О. Создание программного средства для расчетов показателей страхования жизни // В сборнике: Математические методы и модели в исследовании актуальных проблем экономики России // Сборник материалов Международной научно-практической конференции. Ответственный редактор Р.Р. Ахунов. 2016. С. 204-208.
6. Кутлыбаева Д.М., Иремадзе Э.О. Анализ вероятностных характеристик субпортфелей на страховом рынке // В сборнике: Математические методы и модели в исследовании актуальных проблем экономики России // Сборник материалов Международной научно-практической конференции. Ответственный редактор Р.Р. Ахунов. 2016. С. 214-217.
7. Iremadze E.O., Antonova N.A. Optimization model of consumer loans portfolio in commercial banks according to current problems on the example of JSC “Russian Standard” Bank // Международный научно-исследовательский журнал. 2016. № 7-1 (49). С. 30-31.
8. Кулинич О.В., Иремадзе Э.О. Моделирование современной экономической ситуации в России // В сборнике: Государство и бизнес.

Современные проблемы экономики Материалы VII Международной научно-практической конференции. Северо-Западный институт управления РАНХиГС при Президенте РФ, Факультет экономики и финансов. 2015. С. 16-20.