УДК 004.056.5

АКТУАЛЬНОСТЬ УЛУЧШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Абишова А.А., докторант
Казахстанский государственный гуманитарно-юридический
инновационный университет, Казахстан, г.Семей
Сагындыков К.М., к.т.н., доцент
Евразийский национальный университет
имени Л.Н.Гумилева, Казахстан, г.Нур-Султан
Дубинкин Д.М., к.т.н., доцент
Кузбасский государственный технический университет
им. Т. Ф. Горбачева, Россия, г. Кемерово

Развитие информационных технологий и широкое использование интернета в значительной степени способствовали разработке методов защиты информации [1, 2, 3, 4, 5].

Активное развитие интернета является одним из факторов, способствующих дальнейшему расширению сферы услуг. Таким образом, информационное общество, другими словами, потребность в информации, а также информационных услуг и растущий спрос, в соответствии с основным экономическим законом спроса и предложения, чтобы удовлетворить потребности, это привело к появлению (очень успешной) промышленности. Совокупность спроса и предложения создала новые формы общественных отношений, требующих надлежащего регулирования.

Развитие современных информационных технологий сопровождается ростом краж компьютерных преступлений и связанной с ними информации.

С развитием средств информационных коммуникаций, одновременно возникает и возможность нанесения ущерба информации, которая хранится и передается с их помощью, поэтому улучшение информационной безапасности является актуальным.

Сегодня обеспечение информационной безопасности требует изучение видов угроз, соблюдение требований и принципов, использование специальных методов и средств защиты информации.

Можно отметить следующие требования к информационной безопасности:

1. Информация должна быть защищена в контексте конкретной цели организации или владельца данных.

2. Все методы защиты должны соответствовать национальным стандартам, законам и правилам, регулирующим защиту конфиденциальной информации.

3. Мероприятия, связанные с совершенствованием системы поддержки и защиты труда, должны проводиться регулярно.

4. Защитное оборудование должно быть выбрано в соответствии с протечными каналами компании.

5. Методы защиты должны надежно блокировать любые попытки взлома охраняемой информации.

Цели информационной безопасности:

- препятствие при взломе конфиденциальной и секретной информации;
- единство информации и связанных с ней процессов (создания, ввода, обработки и вывода);
- открытость информации;
- учет информационных процессов.

Система информационной безопасности должна минимизировать ущерб вследствия нарушения требований целостности, конфиденциальности и доступности.

Достаточно нарушить одно из свойств защищенной информации, чтобы использование система стало бессмысленным.

Организация информационной безопасности предполагает разработку определённых принципов её обеспечения.

На практике используются следующие группы методов защиты:

- препятствие взлома информации путем применения физических и программных средств;
- координация элементов защищаемой системы;
- скрывание или модификация информации;
- создание нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;
- обязывание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;
- создание условий, которые мотивируют пользователей к должному поведению.

Методы защиты информации реализуется с помощью организационных и технических средств. В настоящее время выделяют следующие виды технических средств защиты информации:

- резервное копирование наиболее важных массивов данных в компьютерной системе;
- дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных;
- создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;
- обеспечение возможности использовать резервные системы электропитания;
- обеспечение безопасности от пожара или повреждения оборудования водой;
- установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.

Такие как устранение физических недостатков в компьютерных сетях, таких как помещения, с камерами и сигнализацией, являются техническими мерами. Для обеспечения информационной безопасности систем важно соблюдать требования к программно-аппаратному комплексу, организационным мероприятиям и применимым средствам защиты.

Таким образом, сегодня проблема информационной безопасности стала вопросом национальной безопасности для любой страны. В концепции информационной безопасности Республики Казахстан [1] говориться, что «Информационная безопасность рассматривается в Казахстане как неотъемлемая часть национальной безопасности и трактуется как состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны».

Список литературы:

1. Концепция информационной безопасности Республики Казахстан от 10 октября 2006 года №199

2. Гладких А.А. Базовые принципы информационной безопасности вычислительных сетей: учебное пособие для студентов, обучающихся по специальностям. 2010, – 598с.

3. Иванов К. К., Юрченко Р. Н., Ярмонов А. С. Защита информации в автоматизированных системах // Молодой ученый. – 2016. - №29. – С. 22-24.

4. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. – М., 2006 г.

5. Информационная безопасность – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii – Загл. с экрана.