СОВРЕМЕННЫЕ УГРОЗЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ИНТЕРНЕТ- ПРОСТРАНСТВЕ

Комилова Гавхар Махтумжановна
магистр кафедры информационных технологий Ферганского филиала Ташкентского университета информационных технологий имени Мухаммада ал-Хорезми

Аннотация: *В статье рассматриваются современные угрозы защите конфиденциальной информации в сети Интернет и их классификация.*

Ключевые слова: *фактор, тенденция, информационная безопасность, цифровизация, защита, система, база данных, обеспечение безопасности, программный комплекс, политика безопасности.*

Annotation: *The article discusses about modern threats to the protection of confidential information on the Internet and their classification.*

Key words: *factor, tendency, information security, digitalization, protection, system, database, security, software package, security policy.*

Современные информационно-телекоммуникационные сети представляют собой сложную распределенную систему, характеризующуюся наличием множества взаимодействующих ресурсов и одновременно протекающих системных и прикладных информационных и телекоммуникационных процессов.

Применение новых информационных и телекоммуникационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности (ИБ). Учитывая тенденцию к созданию единого информационного пространства и, как следствие, подключения защита конфиденциальной информации в интернет пространстве к глобальной сети Интернет, следует ожидать атак на такие системы с целью их разрушения или получения коммерческой выгоды По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается ее уязвимость Основными факторами, способствующими повышению этой уязвимости, являются:

- резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой в защита конфиденциальной информации в интернет пространстве.

- сосредоточение в единой информации различного назначения и различных принадлежностей.

- расширение круга пользователей, имеющих непосредственный доступ к ресурсам защита конфиденциальной информации в интернет пространстве и

находящимся в ней данных широкомасштабная стандартизация и унификация средств вычислительной техники, программного обеспечения, протоколов информационного взаимодействия в значительной степени расширяют возможности несанкционированного воздействия на информацию в современных защита конфиденциальной информации в интернет пространстве. Подобное положение дел резко обостряет проблему ЗИ в современных корпоративных сетях.

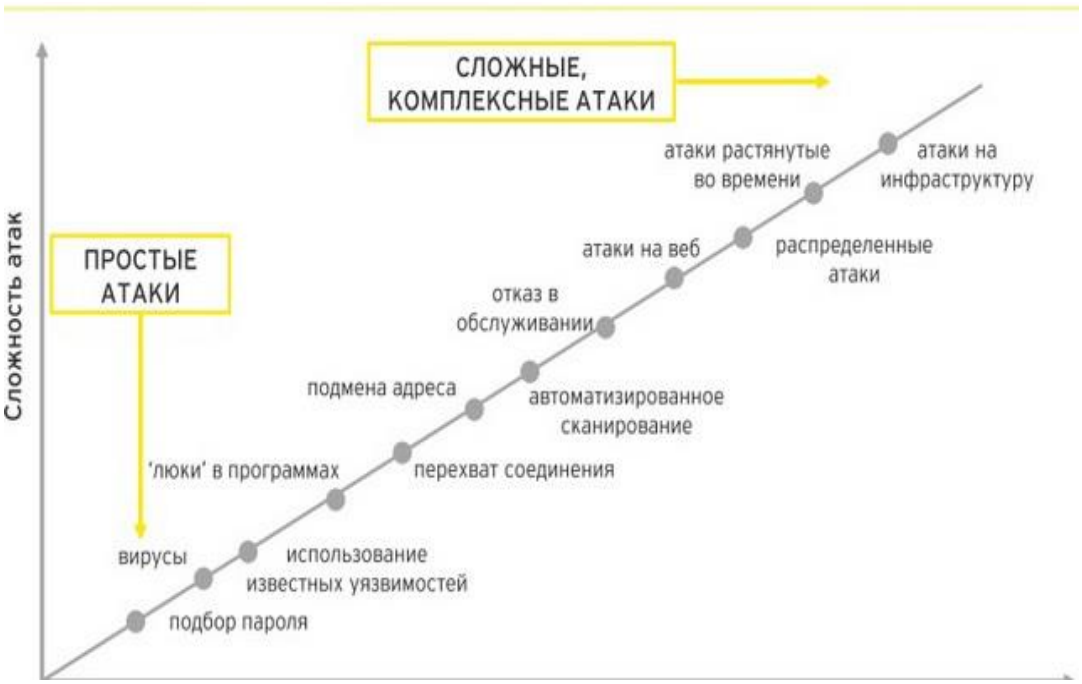
Существующие в настоящее время работы обладают рядом недостатков, к которым относятся следующие не разработана единая методология обеспечения защищенности информации в современных защита конфиденциальной информации в интернет пространстве на этапах проектирования, эксплуатации и реконструкции, недостаточно полно формализованы модели и методы построения системы ЗИ в защита конфиденциальной информации в интернет пространстве.

Таким образом, становится актуальной задача опережающего создания методов, алгоритмов и средств защиты корпоративной сети от атак злоумышленников, при этом в условиях рыночной экономики необходимо одновременно решать задачу оптимизации систем защиты *с* целью минимизации расходов на их приобретение, внедрение и сопровождение

Проявление угроз в интернете характеризуется рядом закономерностей. Во-первых, незаконным овладением конфиденциальной информацией, ее копированием, модификацией, уничтожением в интересах злоумышленников, с целью нанесения ущерба. Кроме этого, непреднамеренные действия обслуживающего персонала и пользователей также приводят к нанесению определенного ущерба.

Во-вторых, основными факторами воздействия угроз, обусловливающими информационные потери и приводящими к различным видам ущерба, возрастание убытков от неправомерных действий, являются:

- несчастные случаи, вызывающие выход из строя оборудования и информационных ресурсов (пожары, взрывы, аварии, удары, столкновения, падения, воздействия химических или физических сред);
- поломки элементов средств обработки информации;
- последствия природных явлений (наводнения, бури, молнии, землетрясения и др.);
- кражи, преднамеренная порча материальных средств;
- аварии и выход из строя аппаратуры, программного обеспечения, баз данных;
- ошибки накопления, хранения, передачи, использования информации;
- ошибки восприятия, чтения, интерпретации содержания информации, соблюдения правил, ошибки как результат неумения, оплошности, наличие помех, сбоев и искажений отдельных элементов и знаков или сообщения;
- ошибки эксплуатации: нарушение защиты, переполнение файлов, ошибки языка управления данными, ошибки при подготовке и вводе информации, ошибки операционной системы, программирования, аппаратные ошибки, ошибки толкования инструкций, пропуск операций и др.;
- концептуальные ошибки внедрения;
- злонамеренные действия в материальной сфере;
- болтливость, разглашение;
- убытки социального характера (уход, увольнение, забастовка и др.).



Оценивать угрозы информационной безопасности необходимо комплексно, при этом методы оценки будут различаться в каждом конкретном случае. Так, чтобы исключить потерю данных из-за неисправности оборудования, нужно использовать качественные комплектующие, проводить регулярное техническое обслуживание, устанавливать стабилизаторы напряжения. Далее следует устанавливать и регулярно обновлять программное обеспечение (ПО). Отдельное внимание нужно уделить защитному ПО, базы которого должны обновляться ежедневно.

ЛИТЕРАТУРА:

1. Anne Marie Willhite ~ Systems Engineering at MITRE Risk Management -Rl, MP96B0000120, September 2015. -p.212
2. Code of practice for Information security management. ~ British Standard, BS7799, 2015. -p.315
3. Code of Professional Ethics for Information Systems Control Professionals. ~ IS ACA Guidelines, 2018. -p.159
4. Kathleen M. Moriarty. Transforming information security. - Wagon lane: Emerald publishing limited, UK. –P.69
5. Death, Darren Information Security Handbook.- P.88
6. John Vacca. Managing Information Security. – New York: Waltham, MA Syngress, 2014. –P.347.