ISSN 3060-4567

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учитель специального предмета, Янгикорджанский районный политехнический техникум №2, Наманганская область

Тулабоева Назокат Дадамирзаевна

Аннотация: *В статье рассматриваются концепции информационной безопасности. В статье также рассматриваются причины защиты информации, политика информационной безопасности в Узбекистане, виды угроз и их причины. Основной акцент сделан на классификации видов методов защиты информации. В статье также анализируются и изучаются теоретические основы современных методов защиты, таких как парольная и биометрическая аутентификация.*

Ключевые слова: *информация, информационная безопасность, общедоступная информация, секретная информация, документированная информация, конфиденциальная информация, угроза, искусственная угроза.*

ВВЕДЕНИЕ

Информационная безопасность означает защиту информации от случайных и преднамеренных атак. Информационная безопасность — многогранная сфера деятельности, требующая для успеха как системного, так и комплексного подхода. Закон Республики Узбекистан от 12 декабря 2002 года № 439-II «О принципах и гарантиях свободы информации» дает следующие определения информации и ее видов: информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от источников и формы их представления; защита информации - меры по предупреждению угроз безопасности информации и ликвидации их последствий; Средства массовой информации — документированная информация, печатные, аудио-, аудиовизуальные и иные сообщения и материалы, предназначенные для неограниченного круга лиц; Документированная информация — информация,

ISSN 3060-4567

зафиксированная на материальном объекте с идентификационными данными; Конфиденциальная информация – документированная информация, использование которой ограничено в соответствии с законодательством. Данное определение выражено в Постановлении Кабинета Министров Республики Узбекистан от 7 ноября 2011 года № 296 «О мерах по реализации Постановления Президента Республики Узбекистан «О дополнительных мерах по защите национальных информационных ресурсов» от 8 июля 2011 года № ПП-1572» следующим образом: конфиденциальная информация — документированная информация, использование которой ограничено в соответствии с законодательством Республики Узбекистан, и информация, не составляющая государственную тайну. Конфиденциальная информация — документированная информация, использование которой ограничено в соответствии с законом. Под информацией в широком смысле можно понимать сведения об окружающем нас мире, являющиеся объектом хранения, преобразования, передачи и использования в определенных целях. Согласно этой концепции, человек находится под воздействием постоянно меняющегося информационного поля, которое влияет на его образ жизни и действия. Информация в зависимости от ее характера может быть политической, военной, экономической, научно-технической, промышленной или коммерческой, а также может быть секретной, конфиденциальной или несекретной.

ГЛАВНАЯ ЧАСТЬ

Защита информации — комплекс мер, направленных на обеспечение важнейших аспектов информационной безопасности (целостности информации, доступности и, при необходимости, конфиденциальности информации и ее ресурсов, используемых при вводе, хранении, обработке и передаче информации). В защищенной системе доступ к информации контролируется лицами или процессами, действующими от их имени, которые используют соответствующие аппаратные и программные средства для чтения, записи, создания и удаления информации. Известно, что абсолютно безопасных систем не существует, но используются надежные системы в смысле «системы,

ISSN 3060-4567

которой можно доверять». Надежной считается система, которая при использовании достаточных аппаратных и программных средств позволяет одновременно обрабатывать данные разной степени конфиденциальности группой пользователей, не нарушая их прав доступа. Основными критериями оценки надежности являются политика и гарантии безопасности.

Процессы глобальной информационной глобализации требуют не только внедрения информационно-коммуникационных технологий в экономику и другие сферы деятельности стран, но и обеспечения безопасности информационных систем. Одним из первых в Центральной Азии он присоединился к международной системе безопасности в сфере информационно-коммуникационных технологий. Государственный комитет связи, информатизации и телекоммуникационных технологий осуществляет следующие мероприятия по обеспечению информационной безопасности: проводит государственную политику по совершенствованию и развитию информационной безопасности в системах передачи данных, телекоммуникационных сетях, телерадиовещании и информационных системах; Организация и участие в разработке законодательных и нормативных правовых актов в области обеспечения информационной безопасности; Обеспечение информационной безопасности комплексов информационных систем, ресурсов и баз данных; Оказывать содействие в разработке и внедрении политик обеспечения информационной безопасности информационных систем и ресурсов органов государственного управления; представлять в установленном порядке в Государственный комитет по информатизации и телекоммуникациям статистические данные о результатах мониторинга информационной безопасности государственных информационных систем и ресурсов; Взаимодействие с операторами и провайдерами сетей телекоммуникаций, организация совместной работы государственных органов по вопросам профилактики правонарушений в сфере использования вычислительной техники и информационных технологий, а также координация их деятельности; Своевременное информирование пользователей

ISSN 3060-4567

национальной сети Интернет о возникающих угрозах информационной безопасности в национальном сегменте сети Интернет, а также оказание консультационных услуг по вопросам защиты информации; сотрудничать с правоохранительными органами в вопросах анализа и выявления правонарушителей, анализа методов и средств, используемых для совершения несанкционированных и деструктивных действий в информационном пространстве; Развивать международное сотрудничество в области обеспечения информационной безопасности в целях организации совместной практической работы по предупреждению инцидентов информационной безопасности в национальном сегменте сети Интернет. Предотвращение несанкционированного доступа к информации из сети со стороны неавторизованных лиц или процессов; Под этим понимается доверие, что информация и ресурсы, предоставленные (проданные) собственником, будут использоваться только на основе соглашений, согласованных сторонами.

Несомненно, что многие киберпреступники используют Интернет в коммерческих целях, осуществляя следующие 13 коммерческих атак:

1. Фишинг.

2. Киберпреступники любят выбирать легкие пути, когда им предоставляется возможность заразить компьютеры ничего не подозревающих жертв. В подобных схемах электронная почта является излюбленным инструментом злоумышленников. Суть метода заключается в том, чтобы заставить получателя отправить письмо от имени законной организации (банка, налоговой службы, популярного интернет-магазина и т. д.). В таких случаях целью обычно является получение банковской информации.

3. Кибербуллинг.

4. Еще одним популярным методом борьбы с финансово мотивированной киберпреступностью является насилие. Обычно после того, как пользователь или компания загружает вредоносный код, файлы шифруются, а затем предлагается обменять их на денежное вознаграждение (обычно в виде биткоинов или другой зашифрованной валюты).

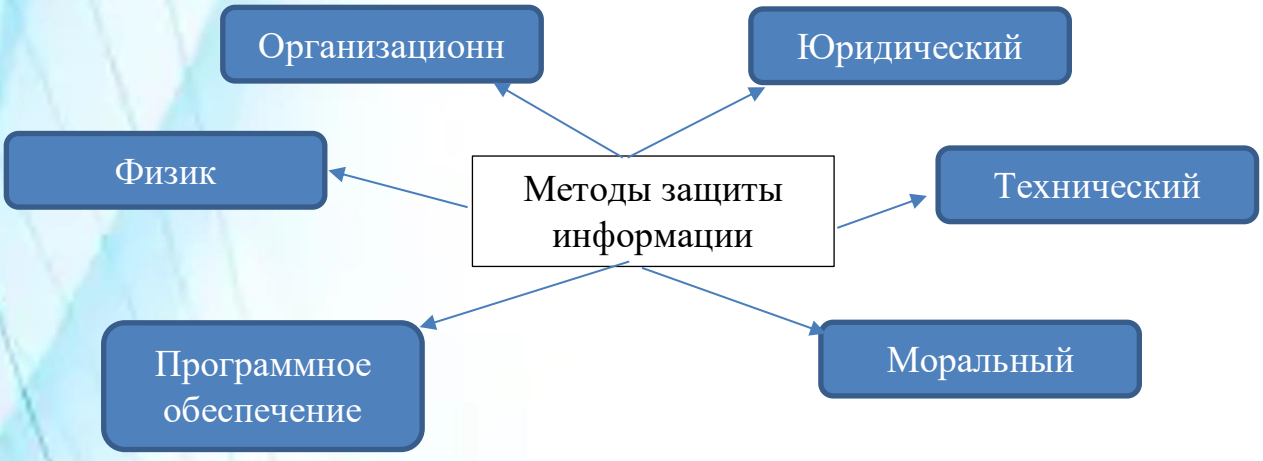
ISSN 3060-4567

Государственные деньги отслеживаются, а потому сложно отследить криптовалюту (что такое криптовалюта, мы говорили ранее).

5. Финансовое мошенничество.

6. Наиболее сложные финансовые мошенничества связаны со взломом компьютерных систем розничных операторов с целью получения банковской информации клиентов (целевые атаки) или последующей манипуляцией полученными данными. Некоторые виды финансового мошенничества очень трудно обнаружить.

Методы защиты информации можно описать следующим образом:



Методы физической защиты: системы противопожарной защиты Системы противопожарной защиты являются важным фактором обеспечения физической безопасности. Определить возникновение пожара можно в автоматизированной или неавтоматизированной формах.

ЗАКЛЮЧЕНИЕ

Потребность в защите информации в Узбекистане отражается в создании государственной системы защиты информации и развитии правовой основы информационной безопасности. Приняты и реализованы законы «Об информации», «О сохранении государственной тайны», «О правовой охране программ для ЭВМ и баз данных» и другие законы, а также ряд постановлений правительства. Защита информации должна обеспечивать предотвращение ущерба, причиненного добровольной утратой информации (хищение, подделка,

ISSN 3060-4567

подделка). Необходимо организовать меры защиты информации на основе действующего законодательства и нормативных документов по информационной безопасности и в соответствии с интересами пользователей информации. Чтобы гарантировать высокий уровень защиты информации, необходимо регулярно решать сложные научно-технические задачи и совершенствовать средства защиты.

СПИСОК ЛИТЕРАТУРЫ:

1. Мирзиёев Ш.М. Вместе мы построим свободный, процветающий и демократический Узбекистан. Выступление на совместном заседании палат Олий Мажлиса, посвященном церемонии вступления в должность Президента Республики Узбекистан, Ташкент, 2016 г.566.

2. Мирзиёев Ш.М. Критический анализ, строгая дисциплина и личная ответственность должны стать ежедневным правилом деятельности каждого лидера. Доклад на расширенном заседании Кабинета Министров об основных итогах социально-экономического развития нашей страны в 2016 году и важнейших приоритетных направлениях экономической программы на 2017 год, 14 января 2017 г. Ташкент, Узбекистан, 2017. 104-6.

3. Сеймур Босворт, Мишель Йе. Кабай, Эрик Уайн. Справочник по компьютерной безопасности. Уайли.2014.

4. Шон Харрис. ВСЕ В ОДНОМ CISSP. Макгроу-Хилл 2013.

5. Ганиев С.К., Каримов М.М., Ташев К.А. «Информационная безопасность». Коммуникатор. 2008.

6. Макаренко С.И. Информационная безопасность. Учебник. Ставрополь, 2009.

7. Майкл Йе. Уитмен. Герберт Дж. Мэттord. Принципы информационной безопасности, четвертое издание. Технология курса, Cengage Learning. 2012.

8. www.intuit.ru

9. www.sec.ru

10. http7/opensecuritvtraining.info/