https://gospodarkainnowacje.pl

GOSPODARKA I INNOWACJE

LABORATORIUM WIEDZY Artur Borcuch

Volume: 35 | 2023

Economy and Innovation
ISSN: 2545-0573

For more information contact: editor@gospodarkainnowacje.pl

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В БОРЬБЕ С КОРРУПЦИЕЙ

Турдиев Валижон Алиханович

Андижанский машиностроительный институт Борьба с коррупцией управление системой "комплаенс-контроль" начальник отдела

Сирожиддинова Ирода Махаммадовна

Андижанский машиностроительный институт к.п.н., доцент

Солиев Бобуржон Абдираим оглы

Андижанский машиностроительный институт Борьба с коррупцией управление системой "комплаенс-контроль" ведущий специалист отдела информационной безопасности

ARTICLEINFO.

Ключевые слова: техническая защита информации, зона контроля, технические средства защиты, демаскирующие признаки объекта, маскирующие.

Аннотация

В данной статье рассматривается вопрос технической защиты информации в информационных системах, использование комплексных и усовершенствованных методов защиты информации и объектов, хранящихся, обрабатываемых и передаваемых в современных информационных системах, комплексный подход к проблеме защиты информации с учетом широты спектра угроз, приобретение системами защиты информации достаточно широкого спектра технических средств защиты и его существенное значение.

Техническая защита информации-это защита информации, предусматривающая обеспечение информационной безопасности некриптографическими методами с использованием технических, программных и программно-технических средств в соответствии с действующим законодательством.

К объектам технической защиты информации можно отнести:

- объект информатизации
- информационная система;
- информационная система ресурсы;
- информационные технологии;
- программные инструменты;
- Сети связи.

Территория контроля-охраняемая (территория, здание, офис и др.).), внутри которого располагаются все точки, соединяющие устройства связи, а также локальные структурные устройства информационной сети [1-3].

К объектам, которые могут быть затронуты в информационных системах, можно отнести:

- аппаратное обеспечение;
- программное обеспечение;
- коммуникации (передача и обработка информации по каналам связи или коммуникационным устройствам);
- Обслуживающий персонал.

В целях нарушения конфиденциальности, целостности и допустимости информации к объектам воздействия относятся не только элементы информационной системы, но и поддерживающая ее инфраструктура (системы электро - теплоснабжения, охлаждения). Кроме того, необходимо обращать внимание на район расположения технических средств, то есть размещать их на охраняемой территории. При установке средств беспроводной связи рекомендуется, чтобы расстояние их действия (Зона действия) не выходило за пределы контролируемой зоны [4-6].

Технические средства защиты-это средства защиты объекта с помощью технических устройств, комплексов или систем. Преимущество технических средств проявляется в решении широкого спектра задач, высокой надежности, возможности создания комплексной развитой системы защиты, адекватной реакции на попытки несанкционированного использования, традиционности использования методов выполнения защитных действий.

Под маскирующими (маскирующими) признаками (демаскирующими признаками) понимается свойство объекта отличаться от других объектов каким-либо описанием. Отличительные характеристики могут оцениваться по количеству или качеству.

Демаскирующие признаки объекта-это свойство объекта защиты, которое техническая разведка может использовать для обнаружения или идентификации объекта, а также для получения необходимой информации об объекте. Владение информацией осуществляется путем анализа демаскирующих признаков. Следовательно, эти символы являются своего рода каналом вывода информации. Демаскирующие распределители символов являются физическими полями, непосредственно связанными с этими символами.

Мероприятия технического характера в информационной системе-инженерно-технический элемент системы информационной безопасности предназначен для активного и пассивного противодействия средствам технической разведки и формирования сферы контроля на основе их комплекса. [7-9].

В защите информации важен этот элемент, в состав которого входят:

- организация физической защиты от проникновения посторонних лиц на территорию зданий, сооружений, линий связи;
- технические средства противодействия каналам утечки информации, возникающим в процессе работы с компьютерными устройствами, средствами связи, модемами, факсами и другими устройствами, участвующими в передаче информации по каналу связи;
- средства защиты здания от технической разведки визуальными методами;
- идентификация средств наблюдения, оповещения, сигнализации, передачи информации, технических средств при нарушении их работоспособности или изменении величин сетевой связи;
- приборы и устройства технической разведки (слух, наблюдение, передача и др.) средства идентификации;
- технические средства контроля, препятствующие выносу с рабочего места обслуживающим

персоналом специально замаскированных (замаскированных) предметов, носителей информации, внешних воспоминаний и т.п.;

- Создание резерва технических средств, формирование копий носителей информации.

Развитие применения компьютерной техники и информационных систем в экономике, управлении, коммуникациях, научных исследованиях, образовании, сфере услуг, торговле, финансах и других сферах человеческой деятельности является определяющим направлением развития информатизации и общества в целом. Вопросами защиты информации занимается наука криптология (Cryptos-тайна, logos-наука). Цели криптологии делятся на области криптографии и криптоанализа, которые имеют два противоположных направления.

О взаимодействии криптографии с математическими методами шифрования открытых данных было сказано выше.

Криптоанализ, с другой стороны, занимается решением проблем поиска исходного состояния (соответствующей открытой информации) зашифрованной информации без знания метода (ключа или алгоритма) шифрования.

Современная криптография включает следующие разделы:

- Симметричные криптосистемы.
- Криптосистемы, основанные на открытом стиле или, другими словами, алгоритме открытых ключей.
- Криптографические системы электронной цифровой подписи.
- Управление разработкой и использованием ключей криптостойкости для криптосистем. Материалы и методика исследования.

Обеспечение информационной безопасности в противодействии коррупции предполагает осуществление разносторонней деятельности систематического и комплексного характера. При его реализации необходимо уделять особое внимание задачам, которые ставятся перед заинтересованными сторонами в информационной безопасности. Эти различные районные задачи можно разделить на несколько основных групп:

1. Обеспечение доступа к информации, т. е. получение информационной услуги в оптимальные сроки и снятие несанкционированного запрета на получение информации;
2. Обеспечение информационной целостности, т. е. устранение несанкционированных модификаций или искажений информации;
3. Обеспечение конфиденциальности информации, т. е. исключение несанкционированного доступа к информации. Информационная безопасность – состояние надежной защиты культурного имущества страны, интеллектуальной собственности хозяйствующих субъектов и граждан, специальной информации, относящейся к государственной и профессиональной тайне. Обычно выделяют следующие четыре категории субъектов информационной безопасности, отличающихся друг от друга правовым, техническим, финансовым, организационным и иным ресурсным обеспечением информационной безопасности: - целое государство; - государственные организации; - коммерческие структуры; - отдельные граждане. [10-12].

В основе информационной безопасности лежит деятельность по защите информации— обеспечение ее конфиденциальности, доступности и целостности, а также недопущение каких-либо компромиссов в критической ситуации. К таким случаям относятся природные, техногенные и социальные катастрофы, компьютерные сбои, физические кражи и другие. Хотя рабочие процессы большинства организаций в мире по-прежнему основаны на бумажных

документах и требуют соответствующих мер информационной безопасности, количество инициатив по внедрению цифровых технологий на предприятиях неуклонно растет. Это требует привлечения специалистов по информационной безопасности (ИТ) для защиты информации. Эти специалисты обеспечивают технологию информационной безопасности (во многих случаях своего рода компьютерные системы). В этом контексте компьютер относится не только к бытовому персональному компьютеру, но и к цифровым устройствам любой сложности и назначения, от примитивных и изолированных, таких как электронные калькуляторы и бытовая техника, до суперкомпьютеров, подключенных через промышленные системы управления и компьютерные сети. Крупные предприятия и организации в силу жизненной значимости и ценности информации для своего бизнеса, как правило, нанимают в свой штат специалистов по информационной безопасности. Их миссия-защитить все технологии от злонамеренных кибератак, направленных на кражу конфиденциальной информации или контроль над внутренними системами организации.

Сегодня информированное общество интенсивно формируется, и в информационном мире исчезает понятие государственных границ. Глобальная компьютерная сеть приобретает особое значение в социально-экономической, политической, духовной и культурной жизни государств мира. Поэтому защита информации считается важной государственной задачей в любой стране. Необходимость защиты информации в Узбекистане нашла свое выражение в создании государственной системы защиты информации и развитии правовой базы информационной безопасности. В связи с этим приняты и действуют законы Республики Узбекистан "О защите государственной тайны", "об информатизации" и другие.

Государственная политика в области информатизации в нашей стране направлена на создание национальной информационной системы с учетом современных мировых принципов развития и совершенствования информационных ресурсов, информационных технологий и информационных систем.

Использованная литература.

1. S. K. Ganiyev, M. M. Karimov, K.A. Tashev. Axborot xavfsizligi. T. , 2017 yil.
2. Mahammadovna S. I. Features of Cluster Design in Modern Paradigms of Education //Telematique. – 2023. – Т. 22. – №. 01. – С. 348-355.
3. Сирожиддинова И. Методика смешанной отборки при комплексном проектировании профессиональной подготовки будущих инженеров //Общество и инновации. – 2022. – Т. 3. – №. 7/S. – С. 87-92.
4. MAXAMMADOVNA S. I. Таълим жараёнини мониторинг тадқиқ қилиш учун ташхис материалларини ишлаб чиқиш //Results of National Scientific Research. – 2022.
5. Iroda M. et al. Rational Methods Awakening and Stimulating University Students Professional and Creative Abilities //Eastern European Scientific Journal. – 2019. – №. 1.
6. S. S. Qosimov. Axborot xavfsizligini ta`minlashning kriptografik usullari va ularning qo`llanilishi.
7. Zakirovich N. I., Mahammadovna S. I. LEVELS OF DEVELOPMENT OF HUMAN ABILITIES //Новости образования: исследование в XXI веке. – 2023. – Т. 1. – №. 7. – С. 341-344.
8. MAXAMMADOVNA S. I. PEDAGOGICAL OPPORTUNITIES FOR THE DEVELOPMENT OF PROFESSIONAL AND CREATIVE ABILITIES IN STUDENTS //International Journal for Innovative Enginering and Management Research…. – 2021.
9. Mahammadovna S. I. DEVELOPMENT OF A METHODOLOGICAL SYSTEM OF TRAINING BASED ON THE CLUSTER APPROACH //Archive of Conferences. – 2022. – С. 30-33.

10. Sirojiddinova I. TECHNOLOGICAL CHARACTER OF THE EDUCATIONAL PROCESS WHEN DESIGNING PEDAGOGICAL OBJECTS //Solution of social problems in management and economy. – 2023. – Т. 2. – №. 2. – С. 130-132.
11. Sirojiddinova I. THE IMPORTANCE OF THE CLUSTER APPROACH TO THE CREATION OF A MOTIVATIONAL AND METHODOLOGICAL TEACHING SYSTEM //Вестник Ошского государственного педагогического университета имени А. Мырсабекова. – 2022. – Т. 2. – №. 2. – С. 146-150.
12. Sirojiddinova I. M. ENGINEERING STUDENTS HAVE SUCCEEDED IN CREATING A TECHNOLOGY CLUSTER // Pedagogy & Psychology Theory and practice International scientific journal № 5 (43), 2022 ISSN 2412-8201. Volgograd, 2022/ 22-25