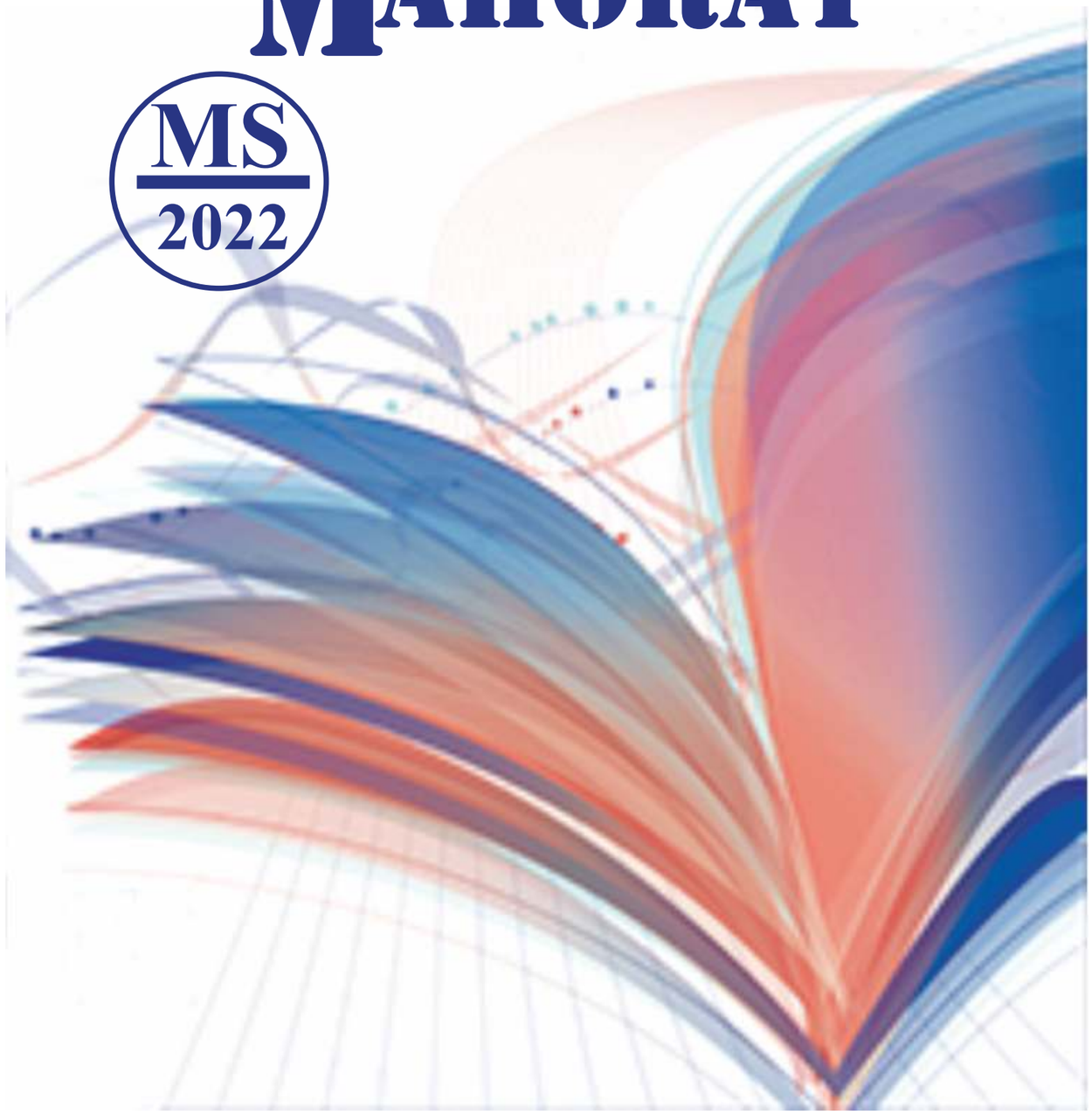
ISSN 2181-6833

PEDAGOGIK MAHORAT

MS
2022



ISSN 2181-6833

MUNDARIJA

ТАХИРОВ Бехзод Насриддинович

Преподаватель Бухарского государственного университета

КАИМОВА Мунисахон Бахтиёр кизи

Студент Бухарского государственного университета

ЖУРАКУЛОВ Нажмиддин Жахон угли

Студент Бухарского государственного университета

ЗАЩИТА ИНФОРМАЦИИ – ВАЖНЕЙШАЯ СОСТАВЛЯЮЩАЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В данной статье рассматривается понятие защиты информации. Базовые принципы информационной безопасности, система мер защиты информации, которая используется при создании программных средств защиты информации. Приватность информации в Интернете. Правовые основы защиты информации.

Ключевые слова: *информация, защита информации, информационная безопасность, целостность данных, конфиденциальность, доступность, предупреждение угроз, выявление угроз, локализация угрозы, пароль, государственная политика.*

AXBOROTNI HIMOYA QILISH ZAMONAVIY AXBOROT TEXNOLOGIYALARINING ENG MUHIM TARKIBIY QISMIDIR

Ushbu maqolada axborotni himoya qilish tushunchasi muhokama qilinadi. Axborot xavfsizligining asosiy prinsiplari, axborotni himoya qilish uchun dasturiy vositalarni yaratishda foydalaniladigan axborotni himoya qilish choralari tizimi, internetdagi ma'lumotlarning maxfiyligi, axborotni himoya qilishning huquqiy asoslari to‘g‘risida so‘z boradi.

Kalit so'zlar*: axborot, axborotni himoya qilish, axborot xavfsizligi, ma'lumotlarning yaxlitligi, maxfiylik, mavjudlik, tahdidlarning oldini olish, tahdidlarni aniqlash, tahdidlarni lokalizatsiya qilish, parol, davlat siyosati.*

INFORMATION PROTECTION IS THE MOST IMPORTANT COMPONENT OF MODERN INFORMATION TECHNOLOGIES

This article discusses the concept of information protection. Basic principles of information security, a system of information security measures that is used in the creation of information security software. Privacy of information on the Internet. Legal basis of information protection.

Keywords: *Information, information protection, information security, data integrity, confidentiality, accessibility, threat prevention, threat detection, threat localization, password, government policy.*

Введение. Важнейшей составляющей жизни является информация, а вместе с этим и информационные технологии, которые стали неотъемлемой частью жизни современного человечества. Поскольку информация обрела значительную важность, ей необходима защита.

Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем. На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:

- целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

Защита информации — система мер, направленных на достижение безопасного защищенного документооборота с целью сохранения государственных и коммерческих секретов. Для достижения результата реализуются режимные требования, применяются сложные, как правило, электронные устройства. Для защиты информации в компьютерах и сетях применяются программно-технические решения, в том числе с применением криптографии.[1]

Основная часть. В современном мире большая часть информации поступает к нам с помощью ИКТ и обеспечение мер информационной безопасности включает в себя соответствующие технологии, обеспечивающие защиту информации. Это и технические приспособления, а также и

программные средства. Программные средства, обеспечивающие, электронную защиту информационных ресурсов используют следующую систему мер, которые направлены:

- на предупреждение угроз. Предупреждение угроз — это меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
- на выявление угроз. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;
- на обнаружение угроз. Обнаружение имеет целью определение реальных угроз;
- на локализацию разрушительных действий и принятие мер по ликвидации угрозы;
- на ликвидацию последствий угроз и разрушительных действий и восстановление статус-кво.

В наше время большую роль играет умение пользоваться сетью Интернет и при этом, сохранять свою приватность в сети. Так как в сети циркулирует масса личной информации о каждом из нас. Однако спецслужбы — не единственная угроза нашей анонимности. Многие интернет-компании зарабатывают на продаже сетевой рекламы. Для того, чтобы этот инструмент работал эффективно, рекламодателям необходимо получить максимум информации о своей аудитории. Когда мы пользуемся любым бесплатным веб-сервисом, мы, по сути, расплачиваемся информацией о себе — контактными данными, списками знакомых, даже информацией о перемещениях. Нет ничего криминального в самой рекламе и в желании сделать ее максимально эффективной. Но вся собранная о нас информация хранится по всему интернету, и эти данные легко могут «уйти» в публичный доступ: из-за хакерской атаки, человеческой ошибки или чьего-то намерения.

Для сохранения приватности в сети нужно соблюдать некоторые несложные правила.

1. *Выбирайте правильные пароли*

Необходимо отделаться от привычки указывать везде один и тот же пароль. Не важно, насколько сложную комбинацию букв и цифр вы выбрали, ее можно подобрать, а затем последовательно вскрыть все ваши аккаунты. Если вы вдруг где-то прочитаете, что веб-сервис, которым вы пользуетесь, был атакован хакерами и потерял базу логинов и паролей (среди которых и ваш) — знайте, что злоумышленники уже наверняка пытаются использовать полученные комбинации для входа на другие сайты.

Самый простой способ защиты — менеджер паролей. Это специальная программа, которая поможет вам сгенерировать для каждого сайта уникальный ключ и сохранит эти данные в зашифрованном месте. Большинство менеджеров паролей полностью автоматизируют вход в учетные записи на сайтах. Потребуется привыкнуть к новому инструменту (обычно это занимает меньше недели), но вскоре вы поймете, что это очень удобно.

Есть платные и бесплатные менеджеры паролей, к последним относится, например, LastPass. Он доступен для разных браузеров и умеет синхронизироваться на различных устройствах пользователя. Кроме того, LastPass сам сообщит пользователю, если посещаемый им ресурс был взломан, и посоветует план дальнейших действий.

2. *Сообщайте сайтам, что плохо относитесь к слежке*

Сбор информации о посещаемых пользователем страницах в рекламе иногда называют поведенческим анализом. Некоторые интернет-компании готовы отказаться от сбора информации о пользователе, если он им об этом скажет.

При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на обеспечение компьютерной безопасности, основными среди них являются технические, организационные и правовые.

В Узбекистане, как и в любом правовом государстве, имеется конституционный закон о защите информации. «Государственная политика в области обеспечения информационной безопасности направлена на регулирование общественных отношений в информационной сфере и определяет основные задачи и направления деятельности органов государственной власти и управления, а также место и роль органов самоуправления граждан, общественных объединений и других негосударственных некоммерческих организаций, граждан в области обеспечения информационной безопасности личности, общества и государства.» [2]

Таким образом, защита информации — есть комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию на правовой основе условий, ограничивающих её распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и её носителям.

Чтобы акцентировать внимание на защите информации в высших учебных заведениях ведутся занятия по дисциплине «Защита информации». Одной из тем предмета является «Виды информационных угроз».

Виды угроз информации делятся на:

1. Виды природных угроз.
2. Виды искусственных угроз.

Виды природных угроз:

1-рисунок. Виды природных угроз

Природные явления:

- Огонь.
- Наводнение.
- Землетрясение.
- Магнитная буря.
- Радиоактивные излучения.

Технические инциденты:

- Сила информационных систем.
- Системы снабжения.

Типы искусственных угроз:

2-рисунок. Типы искусственных угроз

Случайные угрозы:

- Ошибки пользователя.
- Необразованные и безответственные пользователи.
- Ошибки в информационных системах.

Преднамеренные угрозы:

- Физическое воздействие на информационные системы.
- Кража информации.
- Хакерские атаки.

Комплексная мера защиты информации:

1. Законодательство. Использование правовых актов, строго определяющих права и обязанности юридических и физических лиц, а также государства в сфере защиты информации.

2. Духовно-этический. Создавать и поддерживать обстановку, в которой нарушения установленных правил поведения на объекте крайне негативно воспринимаются большинством работников.

3. Физика. Создание физических барьеров, препятствующих несанкционированному доступу к защищенной информации.

4. Административный. Установите соответствующие режимы конфиденциальности, доступа и внутренние режимы.

5. Технические. Использование электронных и других средств защиты информации.

6. Криптографический. Внедрение шифрования и кодирования, предотвращающего несанкционированный доступ к обрабатываемой и передаваемой информации.

7. Программное обеспечение. Используйте программные средства, чтобы ограничить удобство использования.

Все носители информации, включая физические, аппаратные, программные и документальные средства, рассматриваются как объект комплексной защиты. Обычно в последнее время использование, хранение, передача и обработка информации осуществляется в различных формах информационных систем.

Информационная система – это прикладной программный, а иногда и программно-аппаратный комплекс, который обычно предназначен для сбора, хранения, поиска и обработки текстовой или графической информации. Материальной основой существования информации в информационной системе являются электронные и электромеханические устройства, а также носители информации.

В качестве носителей информации могут использоваться бумажные, магнитные и оптические носители, электронные схемы. Поэтому необходимо защищать устройства и системы, а также носители информации.

В различных информационных системах пользователи могут быть обслуживающим персоналом, источниками и носителями информации.

Процесс управления угрозами можно разделить на следующие этапы:

1. Уровень детализации при выборе анализируемых объектов и их просмотре.
2. Выбор методологии оценки угроз.
3. Идентификация активов.
4. Анализ угрозы и ее последствий, выявление слабых мест защиты.
5. Оценка угрозы.
6. Выбор защитных мероприятий.
7. Применение и проверка выбранных мер.
8. Оценка остаточной угрозы.

Правовое регулирование этих отношений может и должно осуществляться прежде всего путем страхования от информационных угроз.

Заключение. Таким образом после рассмотрения темы, можно определить, что защита информации включает в себя комплекс мероприятий с различными подходами к защите информации. Физическая, правовая, духовно-этническая, административная, техническая, криптографическая и программная защита информации обеспечит полный защитный комплекс при разработке мер информационной защиты. Преподавание данной дисциплины в ВУЗах полностью себя оправдывает и позволяет обучить студентов основам разработки программного обеспечения, позволяющее защитить информацию.

Литература:

1. Словарь «Борисов А.Б. Большой экономический словарь. — М.: Книжный мир, 2003. — 895 с.»
2. Закон Республики Узбекистан «О принципах и гарантиях свободы информации». Статья 12. Государственная политика в области обеспечения информационной безопасности. 12.12.2002 г. N 439-II.
3. http://sec4all.net
4. http://www.itsec.ru/articles2/Inf_security