Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Кафедра информационных систем и технологий**

**Лабораторная работа № 1**

Разработка и внедрение политики безопасности

организации или учреждения

Вариант № 2

Студент: Войцехович Е.А.

ФИТ 3 курс 10 группа

Преподаватель: Ржеутская Н.В.

Минск 2023

**Цель:** приобретение практических навыков разработки и внедрения эффективной политики информационной безопасности Event-компании.

**1. Обоснование актуальности, цели и задачи разработки ПИБ Event-компании.**

Развитие и рост предприятий очень тесно связаны с ростом ИТ-инфраструктуры и информационных систем, сложность и масштабы которых постоянно растут, порождая при этом новые виды угроз, уязвимостей и рисков, которые прямым образом влияют на деятельность организации. Актуальность темы данной работы определяется возросшим уровнем проблем информационной безопасности даже в условиях стремительного роста технологий и инструментальной базы для защиты данных. Возникновение проблем в информационной безопасности организации приводит как к финансовым, так и к репутационным потерям. Важная задача руководства – предотвратить эти угрозы, минимизировать риски и обеспечить должный уровень безопасности ИТ-инфраструктуры предприятия.

Разработка политики информационной безопасности является основополагающим и одним из главных этапов при создании каждой коммерческой компании. Политика информационной безопасности Event-компании неразрывно связана с её развитием, стратегическим планированием, она определяет общие принципы и порядок обеспечения информационной безопасности на предприятии. Политика информационной безопасности тесно интегрируется в работу предприятия на всем этапе его существования. Все решения, предпринимаемые на предприятии, должны учитывать её требования.

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков ИБ.

Адекватный уровень информационной безопасности в современной организации может быть обеспечен только на основе комплексного подхода, реализация которого начинается с разработки и внедрения эффективных политик безопасности. Такие политики определяют необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски информационной безопасности до приемлемой величины. Для того чтобы политика безопасности оставалась эффективной, необходимо осуществлять непрерывный контроль ее исполнения, повышать осведомленность сотрудников организации в вопросах безопасности и обучать их выполнению правил, предписываемых ею.

**2. Объекты защиты. Описание структуры организации (учреждения), периметра и внутренней структуры ИВС. Полный обзор всех возможных объектов, а также субъектов информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности.**

По варианту необходимо разработать политику безопасности для Event-компании. Рассмотрим, что является субъектом и объектом ИБ и какая между ними взаимосвязь.

**Объект** — пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

Для Event-компании **объектами** информационной системы выступают: документы об оказании услуг клиентам; носители, хранящие информацию о клиентах; различные базы данных, архивы, директории; папки, хранящиеся на электронных устройствах; ПО, которое предназначено для нормального функционирования отдела по работе с клиентами; файлы, содержащие данные отчетов бухгалтерии; персональная информация о сотрудниках компании. Договор заключается путем подписания клиентом соответствующего документа или иными способами, предусмотренными Порядками оказания услуг. Предлагая подписать договор, компания обязуется предоставлять качественные услуги и соответственно не разглашать личную информацию клиента. Компания обрабатывает персональные данные Пользователей с их согласия.

**Персональные данные клиента могут включать в себя:**

* ФИО;
* Контактный телефон;
* Адрес электронной почты;
* Персональные данные, которые необходимы для разработки веб-сайта или оказания услуг копирайтинга;
* Иная информация, необходимая для качественного оказания услуг, а также необходимая при заключении договора на оказание услуг.

Компания обрабатывает персональные данные Пользователей автоматизированным способом, с использованием средств вычислительной техники, а также неавтоматизированным способом.

Действия по обработке персональных данных включают сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение.

В отношении персональных данных Пользователей сохраняется их конфиденциальность, кроме случаев добровольного предоставления Пользователями информации о себе для общего доступа неограниченному кругу лиц.

Под **субъектами** информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры. **Субъект** — активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

**Субъектами** информационной системы являются Event-компания, которая может инициировать поток информации, в частности личные данные клиента, а также персональные данные сотрудников агентства.

Организационная структура Event-компании представлена на рисунке 1.1.

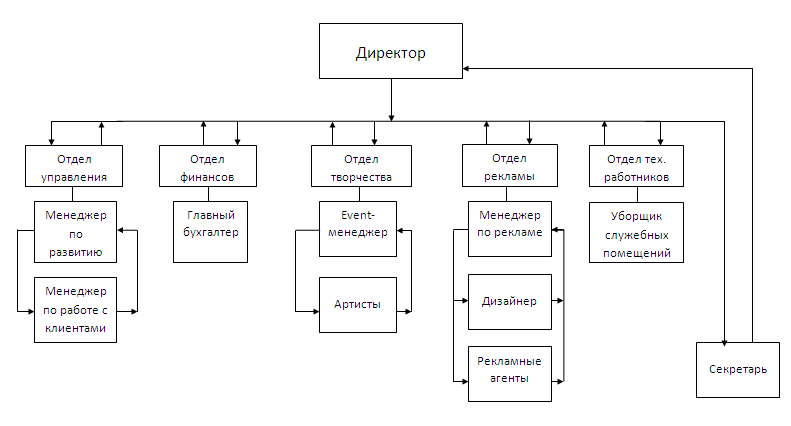


Рисунок 1.1­ Структура Event-компании

В ходе существования Event-компании могут возникать различные проблемы с утечкой информации, несанкционированный доступ к данным, которые должны быть остаться конфиденциальными, а также доступ к денежным средствам компании. Для этого необходимо грамотно подойти к политике безопасности, чтобы избегать проблем в будущем.

**3. Основные угрозы и их источники. Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних.**

Угроза информационной безопасности объекта — возможные воздействия на него, приводящие к ущербу.

Природа воздействий на информационный объект бывают непреднамеренными и преднамеренными, однако все воздействия могут привести к последствиям 3-х видов:

– нарушение конфиденциальности;

– нарушение доступности;

– нарушение целостности.

Под **угрозами** информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

* + несанкционированное распространение (передача) персональных данных;
  + утрата сведений, составляющих конфиденциальную информацию, персональные данные Учреждения и иную защищаемую информацию, а также искажение такой информации;
  + утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д);
  + недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;
  + отсутствие планирования и контроля;
  + низкая степень надежности программного обеспечения;
  + недостаточная осведомленность персонала, низкая квалификация персонала и пользователей в области информационных технологий.

Источники угроз по отношению к Event-компании могут быть как внешними, так и внутренними.

Источниками **внутренних угроз** могут являться:

* сотрудники организации;
* программное обеспечение;
* аппаратные средства.

**Внутренние угрозы** могут проявляться в следующих формах:

* ошибки системных администраторов;
* нарушения сотрудниками установленных регламентов сбора, обработки, передачи и уничтожения информации;
* ошибки в работе программного обеспечения;
* отказы и сбои в работе компьютерного оборудования.

К **внешним источникам** угроз относятся:

* компьютерные вирусы и вредоносные программы;
* организации и отдельные лица;
* стихийные бедствия.

**Внешние угрозы** могут проявляться в следующих формах:

* несанкционированный доступ к персональным данным клиентов агентства и сотрудников компании;
* неработоспособность компьютерного оборудования вследствие стихийных бедствий;
* кража денежных ресурсов компании;
* ущерб, связанный с разглашением персональных данных отдельных лиц.

По происхождению угрозы можно подразделить на преднамеренные и непреднамеренные.

**Непреднамеренные угрозы** — это действия, которые совершают люди по неосторожности, незнанию, невнимательности или из любопытства. К такому типу угроз относят установку программных продуктов, которые не входят в список необходимых для работы, и в последствии могут стать причиной нестабильной работы системы и потеря информации.

**Преднамеренные угрозы** — угрозы, связанные со злым умыслом преднамеренного физического разрушения, впоследствии выхода из строя системы. К преднамеренным угрозам относятся внутренние и внешние атаки.

В свою очередь, информационные угрозы могут быть обусловлены:

* Естественными факторами
* Человеческими факторами.

Человеческие факторы в свою очередь подразделяются на угрозы, несущие случайный неумышленный характер и угрозы умышленного характера, которые делятся на активные/неактивные и внутренние/внешние.

**Пассивные угрозы** направлены на несанкционированное использование информационных ресурсов (прослушивание).

**Активные угрозы** имеют цель: нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на информационные ресурсы.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:

* информационные;
* программные;
* физические.

К **информационным угрозам** относятся:

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* хищение информации из архива, отделов и баз данных;
* нарушение технологии обработки информации;
* противозаконный сбор и использование информации;

К **программным угрозам** относятся:

* использование ошибок в ПО;
* компьютерные вирусы и вредоносные программы.

К **физическим угрозам** относятся:

* уничтожение или разрушение средств обработки информации и связи;
* хищение носителей информации;
* хищение программных или аппаратных ключей и средств криптографической защиты данных;
* воздействие на персонал (шантаж, нападение).

**Специфические угрозы** безопасности:

* возможность отключения электричества, что приведет к сбою незавершенных операций и потерям в базах данных;
* угроза возникновения ошибок при передаче информации от клиентов;
* угроза передачи сотрудниками информации о счетах организации, прибыли и выручке третьим лицам;
* угроза разглашения личной информации, контактных данных, идентификационных сведений клиентов, сведений о регистрации движимого и недвижимого имущества;
* угроза проникновения на рабочие места сотрудников людей, не являющихся работниками отделов, которые имеют туда доступ и т. д.

**4. Оценка угроз, рисков и уязвимостей. Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты.**

В таблице 1.1. приведена условная численная шкала для оценки ущерба Event-компании от несанкционированного доступа.

**Условная численная шкала для оценки ущерба от НСД**

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб Event-компании |
| 1 | Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение Event-компании на рынке не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время банк терпит убытки, но его положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные потери на рынке и в прибыли. От Event-компании уходит ощутимая часть клиентов |
| 4 | Потери очень значительны, Event-компания на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы |
| 5 | Event-компания прекращает существование |

В таблице 1.2. приведена вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам.

**Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам**

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

В таблице 1.3. приведены возможные угрозы и оценка рисков.

**Оценка рисков**

|  |  |  |  |
| --- | --- | --- | --- |
| Потенциальная угроза | Ущерб | Вероятность | Риск |
| Несанкционированный доступ к техническим средствам и информационным ресурсам | 3 | 0,1 | 0,3 |
| Использование вредоносных программ | 1 | 0,1 | 0,1 |
| Хищение информационных ресурсов (персоналом) | 3 | 0,1 | 0,3 |
| Форс-мажорные ситуации | 1 | 0,1 | 0,1 |
| Спам | 1 | 0,4 | 0,4 |

Интегральный риск не превышает допустимый уровень, однако следует произвести работу по снижению влияния указанных проблем или полному устранению.

**5. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Описание разработанной политики ИБ и программы обеспечения безопасности на всех уровнях работы организации (учреждения). Выводы и предложения.**

Задача управления рисками включает выбор и обоснование выбора контрмер, позволяющих снизить величины рисков до приемлемых. При выборе варианта средств обеспечения безопасности активов, в зависимости от разработанной стратегии управления рисками, определяются подходы к снижению риска, такие как уменьшение риска, уклонение от риска, изменение характера риска, принятие риска. Управление рисками включает в себя также оценку стоимости реализации контрмер, которая должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть тем больше, чем меньше возможность (достоверность) причинения ущерба.

Снижение рисков за счет использования контрмер может осуществляться различными **способами**:

* уменьшением вероятностей осуществления угроз безопасности;
* ликвидацией уязвимостей или уменьшением их величин;
* уменьшением величины возможного ущерба;
* восстановлением ресурсов, которым был нанесен ущерб;
* выявлением атак и других нарушений безопасности.

Выбор варианта защиты активов осуществляется на основании результатов оценки рисков с учетом требований безопасности и существующих стоимостных и других ограничений.

**Система мер**, рекомендуемая для большинства компаний, перед которыми стоит вопрос защиты информации, призвана обеспечить соблюдение основных признаков ее безопасности:

− Доступность сведений. Под этим определением понимается возможность и для авторизованного субъекта в любое время получить требуемые данные, и для клиентов в регулярном режиме получать информационные услуги;

− Целостность информации. Это означает ее неизменность, отсутствие любых посторонних, неавторизованных вмешательств, направленных на изменение или уничтожение данных, нарушение системы их расположения;

− Конфиденциальность или абсолютная недоступность данных для неавторизованных субъектов;

− Отсутствие отказа или невозможность отрицать принадлежность действий или данных;

− Аутентичность или возможность достоверного подтверждения авторства информационных сообщений или действий в системе.

**Требования** об обеспечении информационной безопасности Учреждения и **обработке персональных данных** обязательны к соблюдению всеми работниками Учреждения и пользователями информационных систем. Руководство Учреждения приветствует и поощряет в установленном порядке деятельность работников Учреждения и пользователей информационных систем по обеспечению информационной безопасности. Неисполнение или некачественное исполнение сотрудниками Учреждения и пользователей информационных систем обязанностей по обеспечению информационной безопасности и обработке персональных данных может повлечь применение к виновным **административных мер воздействия**, степень которых определяется установленным в Учреждении порядком либо требованиями действующего законодательства. Система обеспечения безопасности информационных ресурсов должна соответствовать экономической целесообразности. Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс **организационных, технических, криптографических, программных средств и мер** по защите информации в процессе документооборота, при работе работников с персональными данными, конфиденциальными документами и сведениями, при обработке информации в информационных системах различного уровня и назначения, при передаче по каналам связи, при ведении деловых переговоров.

**Технические меры** обеспечения информационной безопасности включают в себя:

* обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам информационных систем Учреждения и информации, обрабатываемой в них;
* применение программных, программно-аппаратных средств криптографической защиты информации;
* обеспечение бесперебойной работы информационной системы обработки персональных данных и сети связи;
* обеспечение возобновления работы информационных ресурсов и сети связи после прерываний и нештатных ситуаций;
* применение средств защиты от вредоносных программ;
* применение средств обнаружения вторжений;
* обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
* предотвращения несанкционированного изменений программ и оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.;
* проверку машинных и ручных протоколов выполнения работ со стороны пользователей;
* применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме (пассивная защита).

**Организационные** меры обеспечения информационной безопасности включают в себя:

* организацию контроля доступа в здания и помещения Учреждения, предназначенные для обработки сведений конфиденциального и персонального характера;
* разработку и осуществление разрешительной системы допуска работников к работам с документами и персональными данными;
* заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности, обработки персональных данных и сохранность конфиденциальной информации (персональных данных);
* установление единого порядка хранения и обращения персональных данных, конфиденциальной информации (носителей информации);
* координацию работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи;
* проведение периодического обучения и повышения квалификации работников Учреждения в области информационной безопасности;
* минимизацию данных конфиденциального (персонального) характера, доступных работникам;
* обеспечение физической сохранности автоматизированной системы и дополнительного оборудования;
* практическую проверку функционирования мер защиты обработки персональных данных и конфиденциальной информации.

**Управление инцидентами** информационной безопасности в Учреждении включает в себя:

* сбор информации о событиях информационной безопасности;
* выявление и анализ инцидентов информационной безопасности;
* расследование инцидентов информационной безопасности;
* оперативное реагирование на инцидент информационной безопасности;
* минимизация негативных последствий инцидентов информационной безопасности;
* оперативное доведение до руководства Учреждения информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
* выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
* пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности.

**Вывод:** приобрели практические навыки разработки и внедрения эффективной политики информационной безопасности Event-компании.

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Кафедра информационных систем и технологий**

**Лабораторная работа № 2**

Элементы теории информации. Параметры и характеристики

дискретных информационных систем

Вариант № 2

Студент: Войцехович Е.А.

ФИТ 3 курс 10 группа

Преподаватель: Ржеутская Н.В.

Минск 2023

**Цель**: приобретение практических навыков расчета и анализа параметров и информативных характеристик дискретных ИС.

**Практическая часть**

а) рассчитать энтропию на кириллице.

Рисунок 1 — Гистограмма частоты появления символов

|  |
| --- |
| function lab2\_task1() {  let A = [0.042331714, 0.009100501, 0.024268003, 0.007781588, 0.014903719, 0.053020311, 0.003561066,  0.011210762, 0.056449486, 0.007781588, 0.01398048, 0.01595885, 0.021102611, 0.057372725, 0.062120812,  0.016486415, 0.0349512, 0.035083092, 0.036797679, 0.016354524, 0.005539436, 0.007517805, 0.007649697,  0.004616196, 0.003429174, 0.00395674, 0.001318913, 0.017145872, 0.008045371, 0.000395674, 0.004879979, 0.010683197];  /\* оруглённое до тысячных  let p = [0.042, 0.009, 0.024, 0.008, 0.015, 0.053, 0.004, 0.011, 0.056, 0.008, 0.014, 0.016, 0.021, 0.057, 0.062, 0.017, 0.035, 0.035, 0.037, 0.016, 0.006, 0.008, 0.008,0.005, 0.003, 0.004, 0.001, 0.017, 0.008, 0.0004, 0.005, 0.011];\*/    let H = entropy\_alph(A);  console.log( "Энтропия алфавита = " + H)  return H;  }  function entropy\_alph(a) {  let H = 0;    for(let i = 0; i < a.length; i++) {  H += -(a[i] \* Math.log2(a[i]));  }    return H;  } |

Листинг 1 – Поиск энтропии алфавита

б) для входных документов, представленных в бинарных кодах, определить энтропию бинарного алфавита

|  |
| --- |
| function lab2\_task2() {  //Зорко одно лишь сердце. Самого главного глазами не увидишь.  let str = "11010000 10010111 11010000 10111110 11010001 10000000 11010000 10111010 11010000 10111110 00100000 11010000 10111110 11010000 10110100 11010000 10111101 11010000 10111110 00100000 11010000 10111011 11010000 10111000 11010001 10001000 11010001 10001100 00100000 11010001 10000001 11010000 10110101 11010001 10000000 11010000 10110100 11010001 10000110 11010000 10110101 00101110 00100000 11010000 10100001 11010000 10110000 11010000 10111100 11010000 10111110 11010000 10110011 11010000 10111110 00100000 11010000 10110011 11010000 10111011 11010000 10110000 11010000 10110010 11010000 10111101 11010000 10111110 11010000 10110011 11010000 10111110 00100000 11010000 10110011 11010000 10111011 11010000 10110000 11010000 10110111 11010000 10110000 11010000 10111100 11010000 10111000 00100000 11010000 10111101 11010000 10110101 00100000 11010001 10000011 11010000 10110010 11010000 10111000 11010000 10110100 11010000 10111000 11010001 10001000 11010001 10001100 00101110";  let zero = (str.match(/0/g) || []).length;  let one = (str.match(/1/g) || []).length;  let p = [];  p.push(zero / str.length);  p.push(one / str.length);    let h = entropy\_bin(p);  console.log("Энтропия бинарной строки = "+ h) ;  return h;  }  function entropy\_bin(p) {  let H = 0;  H = -p[0] \* Math.log2(p[0]) - p[1] \* Math.log2(p[1]); //2.4  return H;  } |

Листинг 2 – Поиск энтропии бинарной строки

в) используя значения энтропии алфавитов, полученных в пунктах (а) и (б), подсчитать количество информации в сообщении, состоящем из собственных фамилии, имени и отчества (на основе исходного алфавита – (а) и в кодах ASCII – (б));

|  |
| --- |
| function lab2\_task3() {  let str = "Войцехович Екатерина Алексеевна";  let bin\_str = "";  for(let i = 0; i < str.length; i++) {  bin = str.charCodeAt(i); //числовое значение Юникода для символа по индексу  bin\_str += decToBin(parseInt(bin));  }  let info\_from\_a = lab2\_task1() \* str.length;  let inf\_from\_b = lab2\_task2() \* bin\_str.length;  console.log("Количество информации в сообщении");  console.log("на основе исходного алфавита: " + info\_from\_a );  console.log("в кодах ASCII: " + inf\_from\_b );  }  function decToBin(dec) {  let binary= parseInt(dec.toString(), 2);  return binary;  } |

Листинг 3 – Реализация задания в)

г) выполнить задание пункта (в) при условии, что вероятность ошибочной передачи единичного бита сообщения составляет: 0,1; 0,5; 1,0.

|  |
| --- |
| function lab2\_task4() {  let str = "Войцехович Екатерина Алексеевна";  let bin\_str = "";  for(let i = 0; i < str.length; i++) {  bin = str.charCodeAt(i);  bin\_str += dec2bin(parseInt(bin));  }  console.log("Для q=0.1");  let inf = mistaken\_entropy(0.1) \* str.length;  let inf\_bin = mistaken\_entropy(0.1) \* bin\_str.length;  console.log("a) " + inf);  console.log("б) " + inf\_bin );  console.log("Для q=0.5 ");  inf = mistaken\_entropy(0.5) \* str.length;  inf\_bin = mistaken\_entropy(0.5) \* bin\_str.length;  console.log("a) " + inf );  console.log("б) " + inf\_bin );  console.log("Для q=1 ");  inf = mistaken\_entropy(1) \* str.length;  inf\_bin = mistaken\_entropy(1) \* bin\_str.length;  console.log("a) " + inf);  console.log("б) " + inf\_bin );  }  function mistaken\_entropy(q) {  let p = 1 - q;  if(p != 0 && p != 0.5) {  h\_u = -p \* Math.log2(p) - q \* Math.log2(q);  h = 1 - h\_u;  } else  if(p == 0) {  h = 0;  } else {  h = -Math.log2(p);  }  return h;  } |

Листинг 4 – Реализация задания г)

**Вывод:** в ходе лабораторной работы были приобретены практические навыки расчета и анализа параметров и информативных характеристик дискретных ИС, а также разработано приложение для расчёта энтропии для кириллического и бинарного алфавита.

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Кафедра информационных систем и технологий**

**Лабораторная работа № 3**

Элементы теории информации. Параметры и характеристики

дискретных информационных систем

Вариант № 2

Студент: Войцехович Е.А.

ФИТ 3 курс 10 группа

Преподаватель: Ржеутская Н.В.

Минск 2023

**Цель**: приобретение практических навыков выполнения операций с числами для решения задач в области криптографии и разработка приложений для автоматизации этих операций.

**Практическая часть**

1. Найти все простые числа в интервале [2, n] (n= 553). Подсчитать количество простых чисел в указанном интервале. Сравнить это число с n/ln(n).

|  |
| --- |
| function lab3\_task1() {  let countNumbers = 0;  let strOfNumbers="";  console.log("Простые числа в интервале [2, n]: ");  nextPrime:  for (let i = 2; i <= n; i++) { // Для всех i...  for (let j = 2; j < i; j++) { // проверить, делится ли число..  if (i % j == 0) continue nextPrime; // не подходит, берём следующее  }  countNumbers++  strOfNumbers+=i+" ";  }  console.log(strOfNumbers);  console.log("Количество простых чисел интервале = " + countNumbers);  if(countNumbers > n / Math.log(n)) {  console.log("Больше n/ln(n)");  } else if(countNumbers < n / Math.log(n)) {  console.log("Меньше n/ln(n)");  } else {  console.log("Равно n/ln(n)");  }  } |

Листинг 1 – Реализация задания 1

2. Повторить п. 1 для интервала [m, n].

|  |
| --- |
| function lab3\_task2() {  let countNumbers = 0;  let strOfNumbers="";  console.log("Простые числа в интервале [m, n]: ");  nextPrime:  for (let i = m; i <= n; i++) {  for (let j = 2; j < i; j++) {  if (i % j == 0) continue nextPrime;  }  countNumbers++  strOfNumbers+=i+" ";  }  console.log(strOfNumbers);  console.log("Количество простых чисел интервале = " + countNumbers);  if(countNumbers > n / Math.log(n)) {  console.log("Больше n/ln(n)");  } else if(countNumbers < n / Math.log(n)) {  console.log("Меньше n/ln(n)");  } else {  console.log("Равно n/ln(n)");  }  } |

Листинг 2 – Реализация задания 2

3. Записать числа m и n в виде произведения простых множителей (форма записи – каноническая).

|  |
| --- |
| //проверка на простое число  function isPrime(n) {  if (n===1) {  return false;  }  else if(n === 2) {  return true;  } else {  for(var x = 2; x < n; x++) {  if(n % x === 0) {  return false;  }  }  return true;  }  }  function isInt(value) {  return !isNaN(value) && (function(x) {  return(x | 0) === x;  })(parseFloat(value))  }  function lab3\_task3(n) {  let mass = [];  for(i = 1; i < (n ^ 0.5) + 0.1; i++) {  if(isPrime(i) == 1) {  let x = n / i;  if(isInt(x)) {  n = x;  mass.push(i);  i = 1;  }  }  }  for(i=0;i<mass.length;i++){  console.log(mass[i])  }  return mass;  } |

Листинг 3 – Реализация задания 3

4. Проверить, является ли число, состоящее из конкатенации цифр m ǀǀ n (табл. 1.2), простым.

|  |
| --- |
| function lab3\_task4() {  let concatNumbersStr = m.toString() + n.toString();  concatNumbers = Number(concatNumbersStr);  if(isPrime(concatNumbers)) {  console.log("число, состоящее из конкатенации цифр m и n простое");  } else {  console.log("число, состоящее из конкатенации цифр m и n не является простым");  }  } |

Листинг 4 – Реализация задания 4

5. Найти НОД (m, n).

|  |
| --- |
| function lab3\_task5() {  console.log("НОД чисел = "+nod(n,m));  }  function nod(n, m) {  if(m > 0) {  var k = n%m;  return nod(m, k);  }  else {  return n;  }  } |

Листинг 5 – Реализация задания 5

6. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• вычислять НОД двух либо трех чисел;

• выполнять поиск простых чисел.

|  |
| --- |
| function findNod() {    let first\_num=prompt("Введите первое число");  let second\_num=prompt("Введите второе число");  let mass = [first\_num, second\_num];  while(mass.length <= 1) {  mass.push(1);  }  let nod;  let first = lab3\_task3(parseInt(mass[0]));  for(let i = 1; i < mass.length; i++) {  let second = lab3\_task3(parseInt(mass[i]));  let same = getCommonElements(first, second);  nod = 1;  for(let j = 0; j < same.length; j++) {  nod = nod \* same[j];  }  first = lab3\_task3(nod);  }  console.log("НОД(" + mass + ")=" + nod);  return first;  }  function getCommonElements(a, b) {  b = new Set(b)  return [...new Set(a.filter(x => b.has(x)))]  }  function findPrimeNum() {  let PrimeNumbers = [];  let first\_num=prompt("Введите первое число границы");  let second\_num=prompt("Введите второе число границы");  let mass = [first\_num, second\_num];  for(i = parseInt(mass[0]); i < parseInt(mass[1]); i++) {  let flag = 0;  for(j = 1; j < i + 0.1; j++) {  if(i % j == 0) {  flag += 1;  }  }  if(flag == 2 || flag == 1) {  PrimeNumbers.push(i);  }  }  console.log("В диапазоне [" + mass + "] простые числа: " + PrimeNumbers);  } |

Листинг 6 – Реализация задания 6

**Вывод:** приобрела практические навыки выполнения операций с числами для решения задач в области криптографии и разработла приложение для автоматизации этих операций.