Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Вятский государственный университет»

Колледж ВятГУ

**ОТЧЕТ**

**ПО ПРАКТИЧЕСКОЙ РАБОТЕ №1**

**«Политика информационной безопасности»**

**«МДК 07.02 Сертификация информационных систем»**

Выполнил: студент учебной группы

ИСПк-302-52-00

Холин П.Э.

Преподаватель:

Самоделкин П.А.

Киров

2024

**Цель работы –** приобретение необходимого объёма знаний и практических навыков в области политики безопасности.

**Задание:**

1. Изучить теоретический материал.
2. Ознакомиться с примерами Политики информационной безопасности (см. папку “Доп. материалы”). В отчете дать ответы на контрольные вопросы по Политике ИБ.
3. Для любого сайта сформировать Политику обработки персональных данных при помощи любого из конструкторов:
4. <https://tilda.cc/ru/privacy-generator>
5. <https://artbashlykov.ru/generator-politiki-konfidencialnosti>
6. <https://els24.com/docs/policy-generator>
7. Полученный документ в виде приложения вложить в отчет. Ответить на контрольные вопросы по Политике обработки персональных данных.
8. Отчет сдать преподавателю.

**Контрольные вопросы по Политике ИБ:**

1. Какие события безопасности должны фиксироваться в документе?
2. Какие параметры определяют политику безопасности?
3. Целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?
4. Целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?
5. Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?
6. Нужно ли ограничивать права пользователей по запуску прикладных программ и почему?
7. Какое из дополнительных правил ограниченного использования программ кажется Вам наиболее эффективным и почему?
8. Из каких этапов состоит построение политики безопасности для компьютерной системы?
9. К чему может привести ошибочное определение политики безопасности (приведите примеры)?
10. Почему, на Ваш взгляд, системные администраторы могут пренебрегают использованием большинства из рассмотренных в данной лабораторной работе параметров политики безопасности?

**Результаты выполнения задания**

**1.** **Политика в отношении обработки персональных данных**

##### 1. Общие положения

Настоящая политика обработки персональных данных составлена в соответствии с требованиями Федерального закона от 27.07.2006. №152-ФЗ «О персональных данных» и определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных

VK

 (далее – Оператор).

1. Оператор ставит своей важнейшей целью и условием осуществления своей деятельности соблюдение прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
2. Настоящая политика Оператора в отношении обработки персональных данных (далее – Политика) применяется ко всей информации, которую Оператор может получить о посетителях веб-сайта vk.com.

##### 2. Основные понятия, используемые в Политике

1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;
2. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
3. Веб-сайт – совокупность графических и информационных материалов, а также программ для ЭВМ и баз данных, обеспечивающих их доступность в сети интернет по сетевому адресу;
4. Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий, и технических средств;
5. Обезличивание персональных данных — действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному Пользователю или иному субъекту персональных данных;
6. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
7. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
8. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому Пользователю веб-сайта;
9. Пользователь – любой посетитель веб-сайта;
10. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
11. Распространение персональных данных – любые действия, направленные на раскрытие персональных данных неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
12. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу;
13. Уничтожение персональных данных – любые действия, в результате которых персональные данные уничтожаются безвозвратно с невозможностью дальнейшего восстановления содержания персональных данных в информационной системе персональных данных и (или) результате которых уничтожаются материальные носители персональных данных.

##### 3. Оператор может обрабатывать следующие персональные данные Пользователя

1. Фамилия, имя, отчество;
2. Электронный адрес;
3. Номера телефонов;
4. Год, месяц, дата и место рождения;
5. Фотографии;
6. Также на сайте происходит сбор и обработка обезличенных данных о посетителях (в т.ч. файлов «cookie») с помощью сервисов интернет-статистики (Яндекс Метрика и Гугл Аналитика и других).
7. Вышеперечисленные данные далее по тексту Политики объединены общим понятием Персональные данные.

##### 4. Цели обработки персональных данных

1. Цель обработки персональных данных Пользователя — информирование Пользователя посредством отправки электронных писем; заключение, исполнение и прекращение гражданско-правовых договоров; предоставление доступа Пользователю к сервисам, информации и/или материалам, содержащимся на веб-сайте.
2. Также Оператор имеет право направлять Пользователю уведомления о новых продуктах и услугах, специальных предложениях и различных событиях. Пользователь всегда может отказаться от получения информационных сообщений, направив Оператору письмо на адрес электронной почты

 с пометкой «Отказ от уведомлениях о новых продуктах и услугах и специальных предложениях».

1. Обезличенные данные Пользователей, собираемые с помощью сервисов интернет-статистики, служат для сбора информации о действиях Пользователей на сайте, улучшения качества сайта и его содержания.

##### 5. Правовые основания обработки персональных данных

1. Оператор обрабатывает персональные данные Пользователя только в случае их заполнения и/или отправки Пользователем самостоятельно через специальные формы, расположенные на сайте

. Заполняя соответствующие формы и/или отправляя свои персональные данные Оператору, Пользователь выражает свое согласие с данной Политикой.

1. Оператор обрабатывает обезличенные данные о Пользователе в случае, если это разрешено в настройках браузера Пользователя (включено сохранение файлов «cookie» и использование технологии JavaScript).

##### 6. Порядок сбора, хранения, передачи и других видов обработки персональных данных

Безопасность персональных данных, которые обрабатываются Оператором, обеспечивается путем реализации правовых, организационных и технических мер, необходимых для выполнения в полном объеме требований действующего законодательства в области защиты персональных данных.

1. Оператор обеспечивает сохранность персональных данных и принимает все возможные меры, исключающие доступ к персональным данным неуполномоченных лиц.
2. Персональные данные Пользователя никогда, ни при каких условиях не будут переданы третьим лицам, за исключением случаев, связанных с исполнением действующего законодательства.
3. В случае выявления неточностей в персональных данных, Пользователь может актуализировать их самостоятельно, путем направления Оператору уведомление на адрес электронной почты Оператора

 с пометкой «Актуализация персональных данных».

1. Срок обработки персональных данных является неограниченным. Пользователь может в любой момент отозвать свое согласие на обработку персональных данных, направив Оператору уведомление посредством электронной почты на электронный адрес Оператора

 с пометкой «Отзыв согласия на обработку персональных данных».

##### 7. Трансграничная передача персональных данных

1. Оператор до начала осуществления трансграничной передачи персональных данных обязан убедиться в том, что иностранным государством, на территорию которого предполагается осуществлять передачу персональных данных, обеспечивается надежная защита прав субъектов персональных данных.
2. Трансграничная передача персональных данных на территории иностранных государств, не отвечающих вышеуказанным требованиям, может осуществляться только в случае наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных и/или исполнения договора, стороной которого является субъект персональных данных.

##### 8. Заключительные положения

1. Пользователь может получить любые разъяснения по интересующим вопросам, касающимся обработки его персональных данных, обратившись к Оператору с помощью электронной почты.
2. В данном документе будут отражены любые изменения политики обработки персональных данных Оператором. Политика действует бессрочно до замены ее новой версией.
3. Актуальная версия Политики в свободном доступе расположена в сети Интернет по адресу https://vk.com/privacy.

**Контрольные вопросы**

1. Документ должен фиксировать события безопасности, связанные с управлением доступом и регистрацией, защитой от вредоносного ПО, использованием ресурсов сети Интернет и СКЗИ.
2. Параметры, определяющие политику безопасности, включают в себя общие требования по обеспечению ИБ, требования при назначении и распределении ролей, требования на стадиях жизненного цикла ИС, требования к управлению доступом, защите от вредоносного ПО и использованию ресурсов сети Интернет.
3. Нецелесообразно, так как функции администратора связаны с управлением системой, а функции аудитора - с оценкой безопасности системы. Объединение этих функций может привести к конфликту интересов и снижению уровня безопасности.
4. Нет, так как анонимный доступ не позволяет контролировать и отслеживать действия пользователей, что увеличивает риск несанкционированного доступа и атаки.
5. Передача пароля по сети должна осуществляться с использованием шифрования, чтобы защитить данные от перехвата и подслушивания.
6. Да, нужно ограничивать права пользователей, чтобы предотвратить запуск вредоносных программ, которые могут повредить систему или украсть данные.
7. Наиболее эффективным является правило, которое требует предварительного разрешения на запуск программ от администратора. Это помогает контролировать использование программ и предотвращает запуск нежелательных приложений.
8. Построение политики безопасности включает в себя анализ рисков, определение целей и задач безопасности, выбор мер защиты, внедрение и управление политикой, а также мониторинг и оценку эффективности политики.
9. Ошибочное определение политики безопасности может привести к недостаточной защите системы, что может привести к атакам, кражам данных, нарушению доступности системы и другим негативным последствиям.
10. Системные администраторы могут пренебрегать использованием большинства параметров политики безопасности из-за недостатка времени, ресурсов или опыта, а также из-за отсутствия понимания важности этих параметров для обеспечения безопасности системы.
11. Из документов видно, что обе политики включают принципы и меры по защите информации, в том числе и персональных данных. В Политике информационной безопасности говорится о защите информации от различных угроз, таких как несанкционированный доступ, изменение или потеря данных. Она также предусматривает меры по управлению доступом к информации, классификации информации и оценке рисков.

Политика обработки персональных данных, в свою очередь, регулирует порядок обработки персональных данных и включает меры по их защите. Она предусматривает выполнение требований законодательства, обработку данных в соответствии с целями их сбора, меры по обеспечению конфиденциальности и безопасности данных, а также защиту от неправомерного использования.

**Выводы по работе**

В ходе работы были приобретены навыки и знания в области политики безопасности.