МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФГБОУ ВО «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

ИНСТИТУТ ЦИФРОВЫХ ТЕХНОЛОГИЙ, ЭЛЕКТРОНИКИ И ФИЗИКИ (ИЦТЭФ)

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

И ЭЛЕКТРОНИКИ (ВТиЭ)

**Отчет по лабораторной работе № 8**

по курсу “Защита информация”

**“Построение системы информационной безопасности.**

**Политика информационной безопасности.”**

Выполнил студент 506 гр.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.В. Осипенко

Проверил: ст. преп. кафедры ИБ.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ П.С. Ладыгин.

Лабораторная работа защищена

“\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г.

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Политика информационной безопасности

**1. Сведения о документе**

1.1. Политика информационной безопасности ИС “UnknPC” (далее – Политика) является основополагающим документом, отражающим видение администратора ИС касательно обеспечения информационной безопасности (далее – ИБ). Политика разработана для установления целей, принципов и подходов к обеспечению информационной безопасности в ИС.

1.2. Политика распространяет свое действие на всех пользователей ИС и является документом, обязательным к ознакомлению и исполнению каждым пользователем ИС.

1.3. Внутренние документы, детализирующие Политику, не должны вступать в противоречие с ней. В случае противоречия они приводятся в соответствие с Политикой в ходе очередной актуализации.

1.4. Документ разработан Администратором ИС.

1.5. Срок действия: до замены (отмены).

1.6. Политика направлена на определение адекватных мер и технологии защиты информационных ресурсов ИС от возможного нанесения им ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи.

1.7. Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам. Доступ к ссылочным документам Политики может быть ограничен.

**2. Нормативные ссылки**

При разработке Политики были использованы следующие документы:

- законодательство и нормативно-правовые акты Российской Федерации в сфере информационной безопасности;

- руководящие и методические документы ФСТЭК России и ФСБ России;

- модель угроз ИС “UnknPC”.

**3. Обозначения и сокращения**

| ИС | Информационная система |
| --- | --- |
| ИБ | Информационная безопасность |
| НСД | Несанкционированный доступ |
| ПО | Программное обеспечение |

**4. Термины и определения**

В Политике используются следующие термины и определения:

**Аутентификация** – проверка принадлежности субъекта доступа предъявленного им идентификатора; подтверждение подлинности.

**Документ** – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

**Доступность информации** – состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

**Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и нарушение ее доступности.

**Информационная безопасность (ИБ)** – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

**Информация** – сведения (сообщения, данные) независимо от формы их предназначения.

**Информационная система (ИС)** – совокупность содержащейся на информационных носителях информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Идентификация** – присвоение субхектам доступа, оьхектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Конфиденциальная информация** – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, или по решению ее владельца.

**Несанкционированный доступ** – доступ к информации или действия с информацией, нарущающие правила разграничения доступа с использованиям штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

**Целостность информации** – устойчивость информации к преднамеренному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

**5. Основные цели и задачи**

5.1. К основным целям обеспечения информационной безопасности в ИС относятся:

1) достижение следующих стратегических целей ИС:

- соответствие требованиям законодательства;

- поддержания работоспособности ИС;

- обеспечение конфиденциальности, целостности и доступности информации в ИС;

- достижение адекватности мер по защите от угроз ИБ.

2) предотвращение всевозможных негативных последствий и рисков, которые могут возникнуть при реализации внешних и внутренних угроз ИБ.

5.2. Основными задачами ИБ в ИС является:

1) создание комплексной, эффективной и управляемой системы ИБ, соответствующей требованиям использования ИС, Российского законодательства, стандартам, лучшим мировым практика;

2) прогнозирование, выявление и противодействие угрозам и инцидентам ИБ;

3) эффективное управление рисками информационной безопасности;

4) постоянное повышение осведомленности пользователей ИС в вопросах ИБ.

**6. Основные принципы**

6.1 Обеспечение информационной безопасности в ИС осуществляется в соответствии со следующими принципами:

1) Доступность. ИБ рассматривается как инструмент предоставление беспрепятственного доступа пользователям ИС;

2) Целостность. ИБ рассматривается как инструмент сохранения целостности информации и всей ИС вцелом;

3) Конфиденциальность. ИБ рассматривается как инструмент ограничения несанкционированного доступа к определенным данным и (или) частям ИС.

4) Актуальность. Мероприятия в отношении ПО и информационных ресурсов для поддержания актуальных версий и технологий по обеспечению безопасности ИС.

5) Законность. Мероприятия по ИБ в отношении информации и информационных ресурсов, необходимость обеспечения безопасности которых обусловлена требованиями законодательства, должны быть реализованы в строгом соответствии указанным требованиям;

**7. Система ИБ**

7.1. Для достижения целей ИС и реализации принципов обеспечения информационной безопасности в ИС создается Система информационной безопасности (далее Система).

7.2. Система состоит из:

1) Системы управления информационной безопасности;

2) Комплекса технических средств защиты информации.

7.3. Внутренние и распорядительные документы ИС, регламентирующие процессы ИБ на каждом из уровней Системы, составляют единую систему документов ИС в области ИБ.

7.4. Состав и структура системы управления информационной безопасности (в том числе состав объектов защиты, система распределения ролей и ответственности, система документации, процессы и меры в области обеспечения информационной безопасности), а также состав подсистем информационной безопасности, определяются и регламентируются другими внутренними документами ИС (стандарты, положения, методики, модели, инструкции и др.), детализирующими и расрывающими положения настоящей Политики.

**8. Ответственность**

8.1. Администратор ИС принимает на себя ответственность за реализацию настоящей Политики.

8.2. Пользователи ИС несут ответственность за выполнение своих обязанностей по поддержанию деятельности по обеспечению и выполнению требований ИБ в соответствии с документами системы управления ИБ, а представители третьих сторон, имеющие доступ к информационным мресуксам ИС - в соответсвии с договорными обязательствами.

# 

# Инструкция пользователя по обеспечению безопасности персональных данных

**1. Общие сведения**

1.1. К защищаемой информации, обрабатываемой и хранимой в информационной системе (далее – ИС), относится информация ограниченного доступа: персональные данные пользователей ИС, технологическая информация информационных систем, парольная и финансовая информация.

1.2. Допуск пользователей к работе в ИС осуществляется в соответствии с надлежащими правами пользования.

1.3. Настоящая Инструкция устанавливает единый порядок обеспечения безопасности информации пользователями при ее обработке с использованием ИС и определяет:

- общие меры обеспечения безопасности информации и правила работы с информацией ограниченного доступа;

- правила по организации парольной защиты;

- правила по организации антивирусной защиты;

- правила по использованию съемных носителей;

- правила при работе с ресурсами сети Интернет и электронной почтой.

1.4. Данная Инструкция обязательна для исполнения всеми пользователями ИС.

1.5. Пользователь несет персональную ответственность за свои действия.

**2. Обязанности пользователя**

2.1. Знать и выполнять требования действующих нормативных методических документов, а также внутренних организационно- распорядительных документов, регламентирующих порядок обработки и защиты ПДн при их обработке.

2.2. Выполнять указания Администратора безопасности ИС персональных данных.

2.3. Соблюдать режим допуска в помещения, где проводится обработка ПДн.

2.4. Выполнять на автоматизированном рабочем месте только те процедуры, которые определены для него должностными обязанностями и на основании Разрешительной системы доступа к ресурсам, программным, и техническим средствам соответствующей ИС персональных данных.

2.5. Знать и строго выполнять правила работы со средствами защиты информации, установленными на элементах ИС персональных данных.

2.6. Хранить в тайне от других свой пароль.

2.7. Использовать при работе только учтенные машинные носители информации.

2.8. Перед началом работы с машинными носителями информации осуществить проверку носителя на предмет отсутствия компьютерных вирусов.

2.9. Передавать для хранения установленным порядком свое устройство личной идентификации и другие реквизиты разграничения доступа только Администратору.

2.10. Обо всех выявленных нарушениях, связанных с ИБ, а также для получения консультации необходимо обратится к Администратору.

2.11. Пользователю запрещается:

- разглашать сведения, содержащие ПДн, третьим лицам;

- обрабатывать с помощью средств ИС информацию и выполнять другие работы, не предусмотренные для данной ИС.

- фиксировать на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

- записывать и хранить информацию на незарегистрированных машинных носителях информацией.

- подключать к ИС незарегистрированные машинные носители информации.

- самостоятельно устанавливать, тиражировать или модифицировать ПО и аппаратное обеспечение, изменять установленные алгоритм функционирования технических и программных средств, вскрывать и ремонтировать технические средства;

- открывать общий доступ к папкам в ИС;

- отключать средства защиты информации;

- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИС;

- привлекать посторонних лиц для производства ремонта или настройки ИС без согласования с Администратором;

- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

- передавать ПДн по открытым каналам связи.

2.13. Принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций с целью уменьшения либо ликвидации их последствий.

2.14. Обеспечивать раздельное хранение ПДн, обработка которых осуществляется в различных целях.

2.15. При отсутствии визуального контроля за ИС доступ к ПК должен быть немедленно заблокирован.

**3. Организация парольной защиты**

3.1. Личные пароли доступа к элементам ИС Пользователи получают у Администратора.

3.2. Полная плановая смена паролей в ИС проводится не реже 1 раза в год.

3.3. Правила хранения пароля:

- запрещается записывать пароли в файле, электронной записной книжке и других носителях информации;

- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.4. Лица, использующие пароли, обязаны:

- четко знать и строго выполнять требования настоящей Инструкции;

- своевременно сообщать Администратору об утечке, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

3.5. Удаление (в т.ч. внеплановая смена) личного пароля любого Пользователя должна проводится в следующих случаях:

- в случае подозрения дискредитации пароля;

- по указанию Администратора ИС.

**4. Организация антивирусной защиты**

4.1. Установка и настройка средств антивирусного контроля осуществляется Администратором ИС.

4.2. Обязательному антивирусному контролю подлежат все файлы, получаемые для обработки в элементах ИС.

4.3. Вновь полученные файлы должны пройти антивирусный контроль до начала их обработки в элементах ИС.

4.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и.т.п.) Пользователь обязан немедленно сообщить о своих подозрениях Администратору ИС и затем выполнить внеочередной антивирусный контроль.

4.5. Передаваемые в сторонние организации файлы должны проходить антивирусный контроль непосредственно перед отправлением или перед записью на носитель.

4.6. Если при проведении антивирусной проверки информационных ресурсов ИС были обнаружены вирусы или их воздействие на носители информации, пользователь обязан:

- сообщить Администратору ИС;

- провести «лечение» файла;

- в случае обнаружения нового вируса, не поддающегося «лечению» применяемыми антивирусными средствами, исключить из обработки зараженный вирусом файл;

- выполнить проверку всех носителей информации в ИС, которые могли стать носителями вируса;

- попытаться найти источник заражения и по возможности вылечить его от вирусов, в противном случае исключить возможность взаимодействия источника заражения с элементами ИС.

**5. Порядок реагирования на аварийную ситуацию**

5.1. В настоящем документе под аварийной ситуацией понимается

некоторое происшествие, связанное со сбоем в функционировании элементов ИС. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных ниже.

- отключение электроэнергии;

- сбой в работе вычислительной сети (коммутационного оборудования);

- нарушение конфиденциальности, целостности и доступности персональных данных;

- физический разрыв внешних каналов связи.

5.2. В случае реализации любой из угроз (выявлении предпосылок к ее реализации) Пользователь обязан:

- предпринять попытку сохранения обрабатываемой информации, содержащей ПДн;

- прекратить работу на автоматизированном рабочем месте;

- немедленно оповестить Администратора ИС, о возникновении аварийной ситуации.

# 

# Вывод

В ходе данной работы были разработаны “Политика информационной безопасности” и “Инструкция пользователя по обеспечению безопасности персональных данных”.

# Контрольные вопросы

1) Какие рекомендации вы можете дать пользователю вашей ИС? Составьте перечень из не менее чем 10 пунктов.

– Рекомендации пользователю моей ИС:

- работает, не трогай;

- без спроса – не лезь;

- не знаешь - не трогай;

- что-то сломал, обязательно сообщи;

- не используй простые и предсказуемые пароли;

- не вставляй невнятные внешние устройства хранения информации;

- делай сохранения файлов и работы;

- делай бекапы системы;

- не стоит обновлять система сразу после выхода свежих обновлений;

- следить за чистотой системы.