МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ХЕРСОНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ХТУ»)

П Р И К А З

31.07. 2025 Геническ № 1216

Об утверждении политики информационной безопасности и положения о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных, в ФГБОУ ВО «Херсонский технический университет»

В соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», в соответствии с требованиями пунктов п.4.14, п.п.11 п.4.20, п.4.23 Устава ФГБОУ ВО «ХТУ»,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Политику информационной безопасности ФГБОУ ВО «Херсонский технический университет», приложение №1.
2. Утвердить и ввести в действие Положение о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных ФГБОУ ВО «Херсонский технический университет», приложение №2.
3. Утвердить и ввести в действие Перечень мероприятий по защите персональных данных ФГБОУ ВО «Херсонский технический университет», приложение №3.

4. Возложить на начальника отдела информационной безопасности Управления комплексной безопасности университета следующие обязанности:

- создание условий для осуществления своевременного обнаружения и оперативного реагирования на инциденты информационной безопасности, в том числе их закрытия;

- предотвращение и (или) снижение негативного влияния инцидентов информационной безопасности на осуществление технологических процессов ФГБОУ ВО «Херсонский технический университет»;

- оперативное совершенствование системы обеспечения информационной безопасности ФГБОУ ВО «Херсонский технический университет».

5. Начальнику Управления информационной политики опубликовать настоящий приказ и приложение к нему на официальном сайте ФГБОУ ВО «Херсонский технический университет».

6. Контроль за исполнением данного приказа возложить на проректора по комплексной безопасности университета.

7. Приказ вступает в силу с момента его подписания.

Ректор Г.А. Райко

Приложение № 2
к приказу ФГБОУ ВО «ХТУ"
«31» 07 2025г.№ 216
(п.2)

ПОЛОЖЕНИЕ
О ПОРЯДКЕ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ «ХЕРСОНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

1. Общие положения

1.1 Настоящее Положение о порядке реагирования на инциденты информационной безопасности (далее - Положение) устанавливает порядок действий лиц, ответственных за обеспечение информационной безопасности при выявлении инцидента информационной безопасности в целях снижения его негативных последствий, а также порядок проведения расследования инцидента информационной безопасности (далее - инцидент).

1.2 Настоящее положение разработано с учетом ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

1.3 Настоящее положение обязательно к исполнению сотрудниками ФГБОУ ВО «ХТУ», участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

1.4 В ФГБОУ ВО «ХТУ» приказом ректора назначается лицо, ответственное за информационную безопасность – начальник отдела информационной безопасности управления комплексной безопасности университета.

1.5 Разбирательство по всем инцидентам информационной безопасности, проводится начальником отдела информационной безопасности с привлечением в необходимых случаях руководителей и работников структурных подразделений.

2. Основные понятия

1.1. В Положении используются следующие понятия и определения:

- Информационная безопасность - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

- Событие информационной безопасности - идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности;

- Инцидент информационной безопасности - появление одного или нескольких нежелательных, или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности;

- Обработка инцидентов информационной безопасности - деятельность по своевременному обнаружению инцидентов информационной безопасности, адекватному и оперативному реагированию на них, направленная на минимизацию и (или) ликвидацию негативных последствий;

- Закрытие инцидента информационной безопасности - действия сотрудников ФГБОУ ВО «ХТУ» в рамках реагирования на инцидент информационной безопасности, результатом которых являются:

- устранение нарушений, реализованных в результате Инцидента информационной безопасности;
- устранение причин выявленного Инцидента информационной безопасности;
- выяснение причин нетипичного поведения сотрудников ФГБОУ ВО «ХТУ» и (или) иных лиц, нештатного функционирования информационных систем и иных объектов среды информационных активов ФГБОУ ВО «ХТУ», а также нетипичных событий в осуществлении технологических процессов.

- Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

- 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;

- Информационная система персональных данных - совокупность содержащихся

в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Сокращения

3.1 В Положении используются следующие сокращения:

- **ИБ** - информационная безопасность;
- **ИСПДн** - информационная система персональных данных;
- **ОС** - операционная система;
- **ПДн** - персональные данные;
- **СЗИ** - средство защиты информации;
- **СЗПДн** - система защиты персональных данных.

Основными целями обработки Инцидентов информационной безопасности являются:

- создание условий для осуществления своевременного обнаружения и оперативного реагирования на Инциденты ИБ в том числе их закрытия;
- предотвращение и (или) снижение негативного влияния Инцидентов информационной безопасности на осуществление технологических процессов ФГБОУ ВО «ХТУ»;
- оперативное совершенствование системы обеспечения информационной безопасности ФГБОУ ВО «ХТУ».

3.2 Основными задачами обработки Инцидентов информационной безопасности являются:

- своевременное обнаружение инцидентов информационной безопасности;
- оперативное реагирование на инциденты информационной безопасности;
- координация деятельности работников структурных подразделений ФГБОУ ВО «ХТУ» в рамках процессов реагирования на инциденты информационной безопасности, в том числе их закрытия;
- ведение базы данных зарегистрированных инцидентов информационной безопасности;
- накопление и повторное использование знаний по обнаружению инцидентов информационной безопасности и реагированию на них;
- анализ инцидентов информационной безопасности;
- оценка эффективности и совершенствование процессов обработки инцидентов информационной безопасности;
- предоставление руководству информации и отчётов по результатам обработки инцидентов ИБ, в том числе информации о фактах обнаружения инцидентов информационной безопасности и результатах реагирования на них.

4. Обнаружение инцидентов информационной безопасности

4.1 Обнаружение инцидентов ИБ выполняется сотрудниками ФГБОУ ВО «ХТУ», в том числе с использованием соответствующих технических средств.

4.2 Регистрация информации об инцидентах ИБ, включая сбор информации, выполняется в соответствии с внутренними локальными нормативными документами.

4.3 Основными источниками информации об инцидентах ИБ, связанных с нарушениями требований к обеспечению защиты информации в информационных системах персональных данных, могут быть:

- сообщения сотрудников ФГБОУ ВО «ХТУ»;
- сведения, отражённые в журналах регистрации событий информационных систем;
- результаты работы средств защиты информации;
- результаты внутренних проверок;
- другие источники информации об Инцидентах ИБ.

5. Порядок анализа и реагирования на инциденты ИБ

5.1 Начальник отдела ИБ УКБ при выявлении инцидентов ИБ реализует комплекс мер, направленных на устранение последствий, причин, вызвавших инцидент, и на недопущение его повторного возникновения.

5.2 Анализ инцидентов ИБ выполняется на основе:

- результатов проведения контроля выполнения процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ;
- анализа отчетности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ;
- анализа записей об инцидентах ИБ, содержащих информацию о событиях ИБ, затронутых инцидентом ИБ информационных активах, автоматизированных системах, степени тяжести последствий от обнаруженных инцидентов ИБ.

5.3 В процессе анализа устанавливаются причины возникновения выявленных инцидентов ИБ.

5.4 В процессе анализа определяются наиболее проблемные с точки зрения подверженности инцидентам ИБ сегменты и компоненты информационной инфраструктуры, наиболее существенные уязвимости и недостатки в обеспечении ИБ.

5.5 В процессе анализа инцидентов ИБ оценивается достаточность принятых мер и выделенных ресурсов для реагирования на инциденты ИБ, проводится оценка результатов реагирования на выявленные инциденты ИБ.

5.6 В процессе анализа проверяются действия работников, осуществляемые при реагировании на инциденты ИБ. Целью проведения данной проверки является формирование (инициирование) совершенствований в части:

- корректировки внутренних документов, определяющих порядок обнаружения и реагирования на инциденты ИБ;
- изменения состава лиц, привлекаемых к реагированию на инциденты ИБ;
- корректировки порядка эксплуатации технических средств защиты информации.

5.7 По результатам анализа инцидентов ИБ начальник отдела ИБ УКБ формирует акты по результатам обработки инцидентов ИБ (форма акта - приложение 1/1, форма журнала регистрации - приложение 1/2).

6. Ответственность

6.1 Все работники, осуществляющие защиту ПДн, обрабатываемых в ИСПДн, обязаны ознакомиться с данным Положением под подпись.

6.2 Сотрудники несут персональную ответственность за выполнение требований настоящего Положения.

7. Срок действия и порядок внесения изменений

7.1 Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно до замены его новым Положением.

7.2 Настоящее Положение подлежит пересмотру не реже одного раза в три года.

Проректор по комплексной безопасности
ФГБОУ ВО «ХТУ» С.С. Азаркин

Приложение к Положению о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных

АКТ (номер вносится в журнал)
об инциденте информационной безопасности

г. Геническ

№_____ / ____ «____»_____ 202__г.

Инцидент зафиксирован: _____
(дата, фамилия и инициалы работника (-ов))

В инциденте задействованы следующие работники: _____
(дата, фамилия и инициалы работника (-ов))

Описание инцидента: _____

Причины инцидента: _____

Меры, принятые для устранения причин, последствий инцидента:

«___» _____ 20___г. _____ / _____ /
(подпись) (Фамилия И.О.)

Приложение к Положению о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных

ФОРМА ЖУРНАЛА
учета инцидентов информационной безопасности

на	листах	
Начат		20
Окончен		20

Ответственный за ведение журнала: _____
(ФИО, подпись)

№. п/п	**Краткое описание инцидента**	**Фамилия, имя, отчество, должность сотрудника, обнаружившего инцидент, дата и время обнаружения**	**Дата и время пресечения несанкционированного воздействия**	**Дата, время доведения информации об инциденте в департамент; фамилия, имя, отчество, должность сотрудника, принявшего информацию**	**Подпись системного администратора / администратора безопасности**
1	2	3	4	5	6

Приложение № 3
к приказу ФГБОУ ВО «ХТУ"
«31» 07 2025г.№ 12.16
(п.3)

ПЛАН
МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

План мероприятий по обеспечению защиты персональных данных (далее - План мероприятий) содержит необходимый перечень мероприятий для обеспечения защиты персональных данных в ФГБОУ ВО «Херсонский технический университет» (далее по тексту Университет, ФГБОУ ВО «ХТУ».

План мероприятий составлен на основании списка мер, методов и средств защиты, определенных в Политике в отношении обработки персональных данных.

Выбор конкретных мероприятий осуществляется на основании анализа отчета о результатах обследования ИСПДн и Модели угроз безопасности.

В План мероприятий включены следующие категории мероприятий:

- организационные (административные);
- физические;
- технические (аппаратные и программные);
- контролирующие.

В План мероприятий включена следующая информация:

- название мероприятия;
- исполнитель мероприятия/ответственный за исполнение;
- итог выполнения мероприятия.

Меры (мероприятия) по защите персональных данных

Любое юридическое лицо в силу требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» обязано принимать меры по защите персональных данных, при этом перечень таких мер оно вправе определять самостоятельно.

Мероприятия по защите персональных данных можно разделить на две большие подгруппы: по внутренней и внешней защите персональных данных.

К мерам по внутренней защите персональных данных относятся следующие действия:

- ограничение числа работников (с регламентацией их должностей), которым открыт доступ к персональным данным. Кого может включать этот перечень? Абсолютно всех, кто имеет доступ к личным делам, т.е. сотрудников отделов кадров или ответственных за кадровое делопроизводство, работников бухгалтерии, секретарей-делопроизводителей, специалистов, которые заключают договоры с физическими лицами, а также инженеров, программистов, юристов;

- назначение ответственного лица, обеспечивающего исполнение организацией законодательства в рассматриваемой сфере;

- утверждение перечня документов, содержащих персональные данные;

- издание внутренних документов по защите персональных данных, осуществление контроля за их соблюдением;

- ознакомление работников действующими нормативами в области защиты персональных данных и локальными актами;

- проведение систематических проверок соответствующих знаний работников, обрабатывающих персональные данные, и соблюдения ими требований нормативных документов по защите конфиденциальных сведений. Следует иметь в виду, что все сотрудники, которые имеют доступ к персональным данным других людей, должны быть ознакомлены с особенностями законодательства в области защиты персональных данных;

- рациональное размещение рабочих мест для исключения несанкционированного использования защищаемой информации;

- утверждение списка лиц, имеющих право доступа в помещения, в которых хранятся персональные данные;

- утверждение порядка уничтожения информации;

- выявление и устранение нарушений требований по защите персональных данных;

- проведение профилактической работы с сотрудниками по предупреждению разглашения ими персональных данных.

Меры (мероприятия) по внешней защите персональных данных:

- введение пропускного режима, порядка приема и учета посетителей;

- внедрение технических средств охраны, программных средств защиты информации на электронных носителях и др.

Несмотря на то, что законом не установлены конкретные требования к количеству и содержанию локальных актов, принимаемых в организации по вопросам обработки и защиты персональных данных, практика реализации данного нормативного акта сформировала необходимый минимум документов, которые должны быть разработаны в учреждении:

- общий документ, определяющий политику организации в отношении обработки персональных данных, например Политика обработки в отношении персональных данных;

- список лиц, обрабатывающих персональные данные;

- приказ о назначении сотрудника, ответственного за организацию обработки персональных данных. Указанное лицо должно осуществлять внутренний контроль за соблюдением организацией и ее работниками законодательства о персональных данных, в том числе требований к их защите, доводить до сведения персонала положения законодательства о персональных данных, локальных актов по вопросам их обработки, а также требования к защите таких данных, организовывать прием и обработку обращений и запросов субъектов персональных данных и (или) контролировать прием и обработку таких обращений и запросов;

- положение о правовых, организационных и технических мерах защиты персональных данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных. В данном положении прописаны конкретные меры по защите персональных данных (введение пропускного режима, применение программных средств защиты информации - паролей, антивирусных программ, хранение персональных данных обособленно от других сведений, на отдельных материальных носителях и в специально оборудованных помещениях с ограниченным доступом и т. д.);

- локальный акт, устанавливающий процедуры, направленные на предотвращение и выявление нарушений законодательства в сфере защиты персональных данных, устранение последствий таких нарушений. Так, в компании могут быть разработаны план мероприятий по внутреннему контролю безопасности персональных данных, инструкция о порядке проведения служебного расследования по фактам нарушений законодательства в сфере защиты персональных данных, вестись журнал антивирусных проверок и контроля работы с персональными данными, журнал обучения, инструктажа и аттестации по вопросам защиты персональных данных.

2. План мероприятий по обеспечению безопасности персональных данных (организационные меры)

№ п/п	Мероприятие	Исполнитель	Итог выполнения мероприятий
1.	Утвердить и ознакомить под роспись работников с Разработанными организационно-распорядительными документами.	Ответственный за организацию обработки персональных данных	Выполнение требований ФЗ-152, ПП РФ от 15.09.2008 г. №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", требований ПП РФ № 1119
2.	Добавить пункт о соблюдении конфиденциальности в трудовые договора. Заключить дополнительные соглашения с физическими лицами, в части соблюдения конфиденциальности и обеспечения безопасности персональных данных по приведенному в документах примеру.	Ответственный за организацию обработки персональных данных. Начальник отдела кадров.	Приведение договоров с третьими лицами в соответствие с требованиями ФЗ
3.	При необходимости, заключить дополнительные соглашения с организациями, имеющие доступ к БД ИСПДн - в части соблюдения конфиденциальности и обеспечения безопасности персональных данных по приведенному в документах примеру.	Ответственный за организацию обработки персональных данных.	Приведение договоров С третьими лицами в соответствие с требованиями ФЗ-152
4.	Получить согласия на, обработку персональных данных сотрудников. Добавить пункт о согласии на обработку ПДн для сбора данных через сайт. (Отдельные документы)	Ответственный за организацию обработки персональных данных. Начальник отдела кадров.	Выполнение требований ФЗ-152
5.	Оформить с работниками, осуществляющими обработку персональных данных по форме Приложения Приказа «Об организации мероприятий по защите персональных данных» обязательствам неразглашении персональных данных.	Ответственный за организацию обработки персональных данных. Начальник отдела кадров.	Выполнение требований ФЗ-152
6.	Копию «Политики в отношении обработки персональных» разместить на официальном сайте, в приемной в общедоступном месте.	Ответственный за организацию обработки персональных данных.	Выполнение требований ФЗ-152

7.	Организоватьрассмотрение запросов субъектов ПДн и их законных представителей в соответствие с Приложением Приказа «Об организации мероприятий по защите персональных данных»	Ответственный за организацию обработки персональных данных.	Выполнение требований ФЗ-152
8.	ПО номенклатуре дел определить документы, у которых истек срок хранения, уничтожить их составив Акт об уничтожении - Приложение Типовая форма акта об уничтожении ПДн Приказа «Об организации мероприятий по защите персональных данных»	Ответственный за организацию обработки персональных данных.	Приведение в соответствие требования ФЗ-152. «Акты уничтожение носителей ПДн». Выполнение требований ПП РФ № 687
9.	Создать комиссию и утвердить «Акт определения уровня защищенности персональных данных при их обработке в информационной системе»	Ответственный за обработку персональных данных	Выполнение требований ПП РФ № 1119; Акт определения уровня защищенности персональных данных при их обработке в информационной системе
10.	Подписать и направить нарочно или почтовым отправлением Уведомление (изменение в уведомление) об обработке персональных данных в территориальный орган Роскомнадзора.	Ответственный за организацию обработки персональных данных	Выполнение требований ФЗ-152
11.	При заключении договоров с третьими лицами, оказание услуг которыми подразумевает передачу персональных данных работников, необходимо перед заключением договора получить согласие на передачу персональных данных от сотрудников.	Ответственный за организацию обработки персональных данных	Выполнение требований ФЗ-152
12.	При заключении договоров с третьими лицами, оказание услуг которыми подразумевает передачу персональных данных работников или доступ третьих лиц к информационной системе персональных данных необходимо в договор включить соответствующий пункт.	Ответственный за организацию обработки персональных данных	Выполнение требований ФЗ-152

13.	Приобретение средств защиты информации (СЗИ) в соответствии с разработанной документацией, технических средств обеспечения ограничения доступа к ИСПДн и местам хранения ПДн.	Ответственный за организацию обработки персональных данных	Выполнение требований ПП РФ № 1119, Приказов ФСТЭК России № 1721, Отметки в журнале учета СЗИ, СКЗИ
14.	Внедрение СЗИ в соответствии с требованиями нормативных актов	Лицензиат ФСТЭК и ФСБ	Выполнение требований ПП РФ № 1119, Приказа ФСТЭК России № 1721, Акт установки и ввода в эксплуатацию СЗИ; Эксплуатационная документация на применяемые средства защиты информации

Проректор по комплексной безопасности

ФГБОУ ВО «ХТУ» С.С. Азаркин

Приложение № 3
к приказу ФГБОУ ВО «ХТУ"
«31» 07 2025г.№ 12-16
(п.3)

Памятка
для обучающихся в ФГБОУ ВО «ХТУ» об информационной безопасности

С каждым годом молодежи в интернете становиться больше, а студенты одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС.
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "Wireless Fidelity", который переводится как "беспроводная точность".

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность".

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;

2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;
4. Не используй публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://";
6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, StROng!;;
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети.

Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь, и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "тема13";
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
2. Управляй своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
5. Соблюдай свою виртуальную честь смолоду;
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.
9.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

- Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
- Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
- Необходимо обновлять операционную систему твоего смартфона;
- Используй антивирусные программы для мобильных телефонов;
- Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
- После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
- Периодически проверяй, какие платные услуги активированы на твоем номере;
- Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
- Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
3. Не указывай личную информацию в профайле игры;
4. Уважай других участников по игре;
5. Не устанавливай неофициальные патчи и моды;
6. Используй сложные и разные пароли;
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей";
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные студенты - активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

Проректор по комплексной безопасности
ФГБОУ ВО «ХТУ» С.С. Азаркин

Приложение № 3
к приказу ФГБОУ ВО «ХТУ"
«31» 07 2025г.№ 1216
(п.3)

ПАМЯТКА
педагогическим работникам
ФГБОУ ВО «Херсонский технический университет»

Необходимо объяснить обучающимся:

- Что нельзя сообщать незнакомым людям, свой адрес, сведения о школе, номер телефона, и другие персональные данные, которые должны знать только родные, друзья и классный руководитель.
- Что необходимо уважать права других людей в Интернете, быть вежливыми и доброжелательными, не допускать оскорблений и агрессии в адрес других пользователей.
- Объясните им смысл понятия «авторское право», расскажите об ответственности за его нарушение, о том, что в случаях использования авторских материалов (фотографий, статей, видео, и т.д.) необходимо размещать ссылки на источник.
- В случае получения информации о проблемах в «виртуальной» жизни обучающихся необходимо сообщить об этом родителям (законным представителям), привлекайте к решению проблем педагога-психолога, педагога социального.
- Необходимо научить обучающихся внимательно относиться к информации, получаемой из сети Интернет, сформировать представление о достоверности и недостоверности публикуемой информации. Рекомендовать к посещению только проверенные сайты.

Проректор по комплексной безопасности
ФГБОУ ВО «ХТУ» С.С. Азаркин

Приложение № 3
к приказу ФГБОУ ВО «ХТУ"
«31» 07 2025г.№12-16
(п.3)

СОГЛАСИЕ
на обработку персональных данных абитуриента ФГБОУ ВО «ХТУ»

№ _____ / ____ «____»_____ 202__г.

Я, абитуриент _____,
(Фамилия, Имя, Отчество)

в дальнейшем – Субъект, разрешаю федеральному государственному бюджетному образовательному учреждению высшего образования «Херсонский технический университет», юридический адрес: 273003, Херсонская область, г.о. город Херсон, г. Херсон, ш. Бериславское, д. 24 (далее – Университет), обработку персональных данных, указанных в пункте 3 настоящего согласия, на нижеследующих условиях:

1. Субъект дает согласие на обработку Университетом своих персональных данных, то есть совершение в том числе следующих действий: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, предоставление (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных (общее описание вышеуказанных способов обработки данных приведено в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных»), а также право на передачу такой информации третьим лицам, если это необходимо для обеспечения и мониторинга учебного процесса, научной, организационной и финансово-экономической деятельности Университета, в случаях, установленных нормативными правовыми актами Российской Федерации.

2. Университет обязуется использовать данные Субъекта для обеспечения и мониторинга учебного процесса, научной, организационной и финансово-экономической деятельности Университета в соответствии с действующим законодательством Российской Федерации. Университет может раскрыть правоохранительным органам любую информацию по официальному запросу только в случаях, установленных законодательством Российской Федерации.

3. Перечень персональных данных, передаваемых Университету на обработку:
фамилия, имя и отчество;
гражданство;
пол;
дата и место рождения;
биографические сведения;
сведения о местах обучения (город, образовательное учреждение, сроки обучения);
сведения о местах работы (город, название организации, должность, сроки работы);
данные об успеваемости;
адрес регистрации;
адрес проживания;
контактная информация;
цифровая фотография и фотография на бумажном носителе;
видеозапись проведения вступительных испытаний;
сведения о родителях;
паспортные данные (номер, дата и место выдачи) и цифровая копия паспорта;
номер СНИЛС и его цифровая копия;
данные о конкурсах, на которые поданы заявления о приёме на обучение;
форма сдачи и результаты вступительных испытаний;
индивидуальные достижения и баллы, начисленные за них;
факт наличия особых или преимущественных прав;
факт подачи заявления о согласии на зачисление;
информация для работы с финансовыми организациями;
сведения об оплате (при условии поступления на обучение на договорной основе).

4. Субъект дает согласие на предоставление работникам Университета следующих персональных данных для обеспечения и мониторинга образовательного процесса, научной, организационной и финансово-экономической деятельности Университета:

фамилия, имя и отчество;
пол;
дата и место рождения;
гражданство;
сведения о местах обучения (город, образовательное учреждение, сроки обучения);
данные об успеваемости;
цифровая фотография;
контактная информация;
сведения о родителях;
данные о конкурсах, на которые поданы заявления о приёме на обучение;
форма сдачи и результаты вступительных испытаний;
индивидуальные достижения и баллы, начисленные за них;
факт наличия особых или преимущественных прав;
факт подачи заявления о согласии на зачисление;
сведения об оплате (при условии поступления на обучение на договорной основе).

5. Субъект по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных.

6. Обработка персональных данных прекращается по истечении полугода с даты завершения приемной кампании, и данные удаляются (уничтожаются) из информационных систем Университета после указанного срока (кроме сведений, хранение которых обусловлено требованиями законодательства Российской Федерации).

7. При поступлении в Университет письменного заявления Субъекта о прекращении действия настоящего Согласия (в случае отчисления) персональные данные деперсонализируются в 15-дневый срок (кроме сведений, хранение которых обусловлено требованиями законодательства Российской Федерации).

8. Настоящее согласие действует в течение срока хранения личного дела Субъекта.

Субъект:

Ф.И.О.: _____

Адрес: _____

Паспортные данные: _____

_____

_____

(подпись)

Приложение № 3
к приказу ФГБОУ ВО «ХТУ"
«31» 07 2025г.№ 1216
(п.3)

СОГЛАСИЕ
на распространение персональных данных абитуриента ФГБОУ ВО «ХТУ»

№ _____/ ____ «____»_____ 202__г.

Я, абитуриент _____ ,
(Фамилия, Имя, Отчество)

в дальнейшем – Субъект, разрешаю федеральному государственному бюджетному образовательному учреждению высшего образования «Херсонский технический университет», юридический адрес: 273003, Херсонская область, г.о. город Херсон, г. Херсон, ш. Бериславское, д. 24 (далее – Университет), распространение персональных данных, указанных в пункте 2 настоящего согласия, на нижеследующих условиях:

1. Субъект дает согласие на распространение Университетом своих персональных данных в целях информирования о ходе открытого конкурса при приёме на обучение в Университет путем размещения информации на официальном сайте Университета в сети Интернет.

2. Перечень персональных данных, передаваемых Университету для распространения:

фамилия, имя и отчество;
данные о конкурсах, на которые поданы заявления о приёме на обучение;
форма сдачи и результаты вступительных испытаний;
индивидуальные достижения и баллы, начисленные за них;
факт наличия особых или преимущественных прав;
факт подачи заявления о согласии на зачисление;
сведения об оплате (при условии поступления на обучение на договорной основе).

3. Субъект по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных.

4. Размещение персональных данных прекращается по истечении полугода с даты завершения приёмной кампании, и данные удаляются (уничтожаются) из информационных систем Университета после указанного срока (кроме сведений, хранение которых обусловлено требованиями законодательства Российской Федерации).

5. При поступлении в Университет письменного заявления Субъекта о прекращении действия настоящего Согласия персональные данные деперсонализируются в 15-дневый срок (кроме сведений, хранение которых обусловлено требованиями законодательства Российской Федерации).

6. Настоящее согласие действует в течение срока проведения приёмной кампании.

Субъект:

Ф.И.О.: _____

Адрес: _____

Паспортные данные: _____

_____

(подпись)

Приложение № 3
к приказу ФГБОУ ВО «ХТУ"
«31» 02 2025г.№ 1216
(п.3)

СОГЛАСИЕ
на распространение персональных данных абитуриента ФГБОУ ВО «ХТУ»

№ _____ / ____ «____»_____ 202__г.

Я, _____ ,
(Фамилия, Имя, Отчество)

законный представитель (_____) (далее – Представитель)

абитуриента _____,
(Фамилия, Имя, Отчество)

в дальнейшем – Субъект, разрешаю федеральному государственному бюджетному образовательному учреждению высшего образования «Херсонский технический университет», юридический адрес: 273003, Херсонская область, г.о. город Херсон, г. Херсон, ш. Бериславское, д. 24 (далее – Университет), распространение персональных данных Субъекта, указанных в пункте 2 настоящего согласия, на нижеследующих условиях:

1. Представитель дает согласие на распространение Университетом персональных данных Субъекта в целях информирования о ходе открытого конкурса при приёме на обучение в Университет путем размещения информации на официальном сайте Университета в сети Интернет.
2. Перечень персональных данных, передаваемых Университету для распространения:
фамилия, имя и отчество;
данные о конкурсах, на которые поданы заявления о приёме на обучение;
форма сдачи и результаты вступительных испытаний;
индивидуальные достижения и баллы, начисленные за них;
факт наличия особых или преимущественных прав;
факт подачи заявления о согласии на зачисление;
сведения об оплате (при условии поступления на обучение на договорной основе).
3. Представитель по письменному запросу имеет право на получение информации, касающейся обработки персональных данных Субъекта.
4. Размещение персональных данных прекращается по истечении полугода с даты завершения приёмной кампании, и данные удаляются (уничтожаются) из информационных систем Университета после указанного срока (кроме сведений, хранение которых обусловлено требованиями законодательства Российской Федерации).
5. При поступлении в Университет письменного заявления Представителя о прекращении действия настоящего Согласия персональные данные деперсонализируются в 15-дневый срок (кроме сведений, хранение которых обусловлено требованиями законодательства Российской Федерации).
6. Настоящее согласие действует до достижения Субъектом полной дееспособности или в течение срока проведения приёмной кампании (смотря что, наступит ранее).

Представитель:

Ф.И.О.:_____

Приложение № 3
к приказу ФГБОУ ВО «ХТУ"
«31» 07 2025г.№ 1216
(п.3)

СОГЛАСИЕ
на распространение персональных данных обучающегося в ФГБОУ ВО «ХТУ»

№ _____/ ____ «____»_____ 202__г.

Я, _____ ,

законный представитель (_____) (далее — Представитель)

обучающегося _____ ,
(Фамилия, Имя, Отчество)

в дальнейшем – Субъект, разрешаю федеральному государственному бюджетному образовательному учреждению высшего образования «Херсонский технический университет», юридический адрес: 273003, Херсонская область, г.о. город Херсон, г. Херсон, ш. Бериславское, д. 24 (далее – Университет), распространение персональных данных Субъекта, указанных в пункте 2 настоящего согласия, на нижеследующих условиях:

1. Представитель дает согласие на распространение Университетом персональных данных Субъекта в целях информирования о результатах его научной и учебной деятельности в Университете путем размещения информации на официальном сайте Университета в сети Интернет.
2. Перечень персональных данных, передаваемых Университету для распространения:
   фамилия, имя и отчество;
   гражданство;
   данные об обучении в Университете;
   данные об успеваемости;
   цифровая фотография.
3. Представитель по письменному запросу имеет право на получение информации, касающейся обработки персональных данных Субъекта.
4. При поступлении в Университет письменного заявления Представителя о прекращении действия настоящего Согласия персональные данные деперсонализируются в 15-дневый срок (кроме сведений, хранение которых обусловлено требованиями законодательства Российской Федерации).
5. Настоящее согласие действует до достижения Субъектом полной дееспособности или до его отзыва.

Представитель:
Ф.И.О.: _____
Адрес: _____
Паспортные данные: _____
_____

_____
(подпись)

Субъект: _____

Приложение № 3
к приказу ФГБОУ ВО «ХТУ"
«31» 07 2025г.№ 12.16
(п.3)

СОГЛАСИЕ
на обработку персональных данных абитуриента ФГБОУ ВО «ХТУ»

№ _____ / ____ «____»_____ 202__г.

Я, _____,
(Фамилия, Имя, Отчество)

законный представитель (_____) (далее – Представитель)

абитуриента _____ ,
(Фамилия, Имя, Отчество)

в дальнейшем – Субъект, разрешаю федеральному государственному бюджетному образовательному учреждению высшего образования «Херсонский технический университет», юридический адрес: 273003, Херсонская область, г.о. город Херсон, г. Херсон, ш. Бериславское, д. 24 (далее – Университет), обработку персональных данных Субъекта, указанных в пункте 3 настоящего согласия, на нижеследующих условиях:

1. Представитель дает согласие на обработку Университетом персональных данных Субъекта, то есть совершение в том числе следующих действий: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, предоставление (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных (общее описание вышеуказанных способов обработки данных приведено в Федеральном законе № 152-ФЗ от 27 июля 2006 г. «О персональных данных»), а также право на передачу такой информации третьим лицам, если это необходимо для обеспечения и мониторинга учебного процесса, научной, организационной и финансово-экономической деятельности Университета, в случаях, установленных нормативными правовыми актами Российской Федерации.

2. Университет обязуется использовать данные Субъекта для обеспечения и мониторинга учебного процесса, научной, организационной и финансово-экономической деятельности Университета в соответствии с действующим законодательством Российской Федерации. Университет может раскрыть правоохранительным органам любую информацию по официальному запросу только в случаях, установленных законодательством Российской Федерации.

3. Перечень персональных данных, передаваемых Университету на обработку:
фамилия, имя и отчество;
гражданство;
пол;
дата и место рождения;
биографические сведения;
сведения о местах обучения (город, образовательное учреждение, сроки обучения);
сведения о местах работы (город, название организации, должность, сроки работы);
данные об успеваемости;
адрес регистрации;
адрес проживания;
контактная информация;
цифровая фотография и фотография на бумажном носителе;
видеозапись проведения вступительных испытаний;
сведения о родителях;
паспортные данные (номер, дата и место выдачи) и цифровая копия паспорта;
номер СНИЛС и его цифровая копия;
данные о конкурсах, на которые поданы заявления о приёме на обучение;
форма сдачи и результаты вступительных испытаний;
индивидуальные достижения и баллы, начисленные за них;
факт наличия особых или преимущественных прав;

факт подачи заявления о согласии на зачисление;
информация для работы с финансовыми организациями;
сведения об оплате (при условии поступления на обучение на договорной основе).

4. Представитель дает согласие на предоставление работникам Университета следующих персональных данных Субъекта для обеспечения и мониторинга образовательного процесса, научной, организационной и финансово-экономической деятельности Университета:

фамилия, имя и отчество;
пол;
дата и место рождения;
гражданство;
сведения о местах обучения (город, образовательное учреждение, сроки обучения);
данные об успеваемости;
цифровая фотография;
контактная информация;
сведения о родителях;
данные о конкурсах, на которые поданы заявления о приёме на обучение;
форма сдачи и результаты вступительных испытаний;
индивидуальные достижения и баллы, начисленные за них;
факт наличия особых или преимущественных прав;
факт подачи заявления о согласии на зачисление;
информация для работы с финансовыми организациями;
сведения об оплате (при условии поступления на обучение на договорной основе).

5. Представитель по письменному запросу имеет право на получение информации, касающейся обработки персональных данных Субъекта.

6. Обработка персональных данных прекращается по истечении полугода с даты завершения приемной кампании, и данные удаляются (уничтожаются) из информационных систем Университета после указанного срока (кроме сведений, хранение которых обусловлено требованиями законодательства Российской Федерации).

7. При поступлении в Университет письменного заявления Представителя о прекращении действия настоящего Согласия (в случае отчисления) персональные данные деперсонализируются в 15-дневый срок (кроме сведений, хранение которых обусловлено требованиями законодательства Российской Федерации).

8. Настоящее согласие действует до достижения Субъектом полной дееспособности.

Представитель:

Ф.И.О.: _____
Адрес: _____
Паспортные данные: _____
_____

_____
(подпись)

Субъект: _____
(подпись)

ПРИЛОЖЕНИЕ № 3
К ПРИКАЗУ ФГБОУ ВО «ХТУ"
«31» 07 2025Г.№ 1216
(П.3)

УВЕДОМЛЕНИЕ
о последствиях отказа предоставления аспирантом ФГБОУ ВО «ХТУ»
согласия на обработку персональных данных

№ _____ / ____ «____»_____ 202__г.

Я, _____
(фамилия, имя, отчество)

аспирант (соискатель) института _____ ФГБОУ ВО «ХТУ», год поступления _____

специальность _____
уведомлен о том, что обработка моих персональных данных осуществляется на основании Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», согласно пункту 1, статьи 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и не требует письменного согласия.

Также уведомлен, что отказ от подписания согласия на обработку персональных не позволит включить мои персональные данные во внутриуниверситетские базы данных обучающихся, что в свою очередь, приведет к невозможности включения меня в списки групп, зачетно-экзаменационные ведомости и другие документы. Допуск к зачетам и экзаменам в этом случае будет возможен только при условии личного получения индивидуальных направлений-допусков. Доступ к электронным библиотечным системам, к которым подключен ФГБОУ ВО «ХТУ», аспиранту Университета будет не возможен.

Субъект:
Ф.И.О.: _____
Адрес: _____
Паспортные данные: _____
_____

_____
(подпись)

Приложение № 1
к приказу ФГБОУ ВО «ХТУ"
«31» 07 2025г.№ 1216
(п.1)

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ФГБОУ ВО «Херсонский технический университет»

г. Геническ -2025г.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

1.1. Федеральное государственное бюджетное образовательное учреждение высшего образования «Херсонский технический университет» (далее по тексту - Университет, ФГБОУ ВО «ХТУ») реализует широкий спектр образовательных программ и исследовательских проектов в области естественных, технических, гуманитарных и общественных наук, - в результате чего Университет является обладателем многочисленных информационных систем.

1.2. В информационных системах Университета обрабатывается общедоступная информация и информация ограниченного доступа (конфиденциальная информация), не содержащая сведений, составляющих государственную тайну, включая персональные данные (далее - информация ограниченного доступа).

1.3. Непрерывное функционирование информационных систем - это обязательное условие для успешной деятельности Университета, которое обеспечивается организацией мероприятий по информационной безопасности. Мероприятия по обеспечению информационной безопасности включают в себя защиту информационных систем, ресурсов, защиту поддерживающей инфраструктуры. Мероприятия охватывают все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Университет.

1.4. При современном развитии информационных технологий невозможно обеспечить требуемый уровень защищённости информационных систем Университета не только с помощью отдельного средства, но даже и с помощью простой совокупности отдельных средств. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационных систем должны рассматриваться как часть единой информационной системы Университета в защищённом исполнении при оптимальном соотношении рисков и технических, организационных мероприятий, финансовых затрат.

1.5. Меры защиты информации в информационных системах Университета, должны быть направленны на обеспечение:

- конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);
- целостности информации (исключение неправомерного уничтожения или модифицирования информации);
- доступности информации (исключение неправомерного блокирования информации).

1.6. Положения Политики информационной безопасности ФГБОУ ВО «ХТУ» служат основой для разработки локальных нормативных актов

(регламентов, инструкций и т.п.), в сфере вопросов информационной безопасности Университета.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящая Политики информационной безопасности ФГБОУ ВО «ХТУ» выражает позицию Университета в области информационной безопасности. Политика представляет собой систематизированное изложение целей и задач защиты информации и определяет мероприятия, процедуры и правила по защите информации.

2.2. Следование требованиям информационной безопасности является важным условием при осуществлении повседневной деятельности (в том числе при реализации информационных технологий, проектов, проработке цифровых инициатив и т.д.). Каждый работник Университета несёт ответственность за безопасную работу с вверенными им информационными активами, системами, компьютерным оборудованием, мобильными техническими средствами, носителями информации, предоставленной
и обрабатываемой информацией. Всем пользователям информационных систем Университета необходимо руководствоваться в своей деятельности настоящей Политикой.

2.3. Руководители структурных подразделений Университета обеспечивают выполнение требований информационной безопасности во вверенных им подразделениях. Ответственность за организацию обеспечения безопасности информации ограниченного доступа (включая персональные данные) несут уполномоченные лица - работники Университета, назначаемые приказом ректора.

2.1. Сокращения и обозначения

АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИС	Информационная система
ИСПДн	Информационная система по обработке персональных
ИТ	Информационные технологии
ИТЦ	Информационно технический центр Университета
КЭП	Квалифицированная электронная подпись
Нсд	Несанкционированный доступ
УКБ	Управление комплексной безопасности Университета
ПДн	Персональные данные

ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации

2.2. Термины и определения

В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации:

Администратор (отдел информационной безопасности УКБ): пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы (администратор системный) и (или) ее системы защиты информации (администратор безопасности) в соответствии с должностными обязанностями.

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторизация - предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Безопасность информации - защищённость информации от нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного тиражирования.

Бизнес-процесс - последовательность технологически связанных операций по предоставлению продуктов, услуг или осуществлению конкретного вида деятельности Университета.

Владелец информационных ресурсов*, информационных систем, технологии и средств их обеспечения* - субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения ими в пределах, установленных законом.

2.4. ***Государственные информационные системы*** - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

Документ - зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.

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

Защита информации - деятельность Университета по принятию правовых, организационных и технических мер, направленных на защиту информации от неправомерного доступа, уничтожения или блокирования.

Идентификация - присвоение субъектам доступа. объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность - практика предотвращения несанкционированного доступа, использования, раскрытия, искажения информационных ресурсов Университета.

Информационный процесс - процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационный ресурс (актив) - массив информации, который находится в распоряжении Университета и представляет ценность.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку технологий и технических средств.

Инцидент - непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Инцидент информационной безопасности - одно или серия нежелательных, или неожиданных событий ИБ, представляющих угрозу ИБ.

Коммерческая тайна - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Контролируемая зона - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

Конфиденциальная информация. - информация с ограниченным доступом или ПДн, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации - состояние защищённости информации, характеризуемое способностью ИС обеспечивать сохранение

в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Мобильны и код - несамостоятельное программное обеспечение или компонент программного обеспечения (скрипты, макросы, иные компоненты) получаемые из мест распространения мобильного кода, передаваемые по сети и выполняемые на компонентах ИС (в местах использования мобильного кода) без предварительной установки (инсталляции) пользователем для расширения возможностей системного и (или) прикладного программного обеспечения.

Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Политика ИБ - общие цели и указания, формально выраженные руководством Университета в отношении защиты ИС от НСД.

Привилегии - это права доверенного объекта (субъекта) на совершение каких-либо действий по отношению к объектам системы.

Риск - сочетание вероятности события и его последствий.

Система обеспечения информационной безопасности (СОИБ) - часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.

Собственник информационных ресурсов*, информационных систем, технологий и средств их обеспечения* - субъект, в полном объёме реализующий, полномочия владения, пользования, распоряжения указанными объектами.

События информационной безопасности - идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.

Угроза - опасность, предполагающая возможность потерь (ущерба).

Управление риском - процесс выбора и реализации мер по модификации (снижению) риска.

Целостность информации - устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

3. ЦЕЛИ И ЗАДАЧИ

3.1. Целями настоящей Политики являются:

3.1.1. Формирование безопасного информационного пространства для функционирования и развития Университета, чтобы Университет мог предоставлять услуги высокого качества при осуществлении образовательной, научной, административно-хозяйственной, международной и иной деятельности.

3.1.2. Защита информационных активов Университета от возможных угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации, и обеспечение нормального функционирования технологических процессов.

3.1.3. Повышение осведомлённости работников, обучение грамотности в области информационной безопасности.

3.1.4. Выполнение требований действующего законодательства Российской Федерации по защите информации.

3.2. **Для достижения целей Политики необходимо обеспечить решение следующих задач:**

3.2.1. Проведение аудита (оценки соответствия, самооценки) информационной безопасности Университета и анализ функционирования систем обеспечивающих ИБ.

3.2.2. Определение информационных ресурсов, подлежащих защите (объектов защиты), их классификация, определение ценности и степени тяжести последствий наступления инцидентов ИБ (оценка рисков).

3.2.3. Определение и актуализация списков возможных негативных воздействий на защищаемые ресурсы, способов реализации и степени вероятности реализации угроз ИБ (модель угроз безопасности).

3.2.4. Назначение и распределение функциональных прав и обязанностей между работниками Университета в части взаимодействия с ИС в том числе с ИСПДн, сетями и поддерживающей инфраструктурой (с отражением в должностных инструкциях).

3.2.5. Управление доступом к объектам информационной инфраструктуры, в соответствии с назначенными функциональными правами и обязанностями работников Университета - политика управления учетными записями (ролевая модель доступа).

3.2.6. С целью снижения рисков нарушения ИБ не рекомендуется, чтобы в рамках одной роли совмещались следующие функции:

- разработки и сопровождения системы или программного обеспечения, - разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора безопасности, выполнения операций в системе и контроля их выполнения.

3.2.7. Защита ИС на всех стадиях жизненного цикла - стадии создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры, а также хранения информации. При этом необходимо обеспечить защиту информации, представленную как в электронном, так и в бумажном виде.

3.2.8. Внедрение политики паролей, определяющей правила и процедуры идентификации и аутентификации пользователей в ИС.

3.2.9. Организация и контроль физического доступа к объектам информационной инфраструктуры, местам хранения конфиденциальных документов, документов содержащих ПДн.

3.2.10. Обеспечение антивирусной защиты от воздействий вредоносного кода (АВЗ).

3.2.11. Организация сегментации сети и защиты периметра вычислительных сетей (VLAN и межсетевое экранирование).

3.2.12. Оценка и обработка инцидентов нарушения информационной безопасности.

3.2.13. Регистрация событий безопасности связанных с изменением параметров ИС и вычислительных сетей, мониторинг и контроль содержимого сетевого трафика (выявление сетевых вторжений и атак).

3.2.14. Ввод в действие организационно-распорядительных документов в соответствии с требованиями законодательства Российской Федерации в области обеспечения безопасности информации.

3.2.15. Использование средств криптографической защиты конфиденциальной информации (СКЗИ) при ее передаче по каналам связи сетей общего пользования и (или) международного обмен.

3.2.16. В договорах с контрагентами, которым необходим доступ в информационную инфраструктуру Университета, рекомендуется предусмотреть и обозначить мероприятия по обеспечению защиты информации.

3.2.17. Организация повышения квалификации и (или) переподготовки сотрудников Университета, работающих в области обеспечения безопасности информации.

3.2.18. Организация резервирования технических средств, резервного копирования программного обеспечения, баз данных и разработка процедуры восстановления.

4. ОСНОВАНИЯ ДЛЯ РАЗРАБОТКИ

4.1. Настоящая политика разработана на основе требований законодательства Российской Федерации, накопленного в Университете опыта в области обеспечения ИБ, интересов и целей Университета. При

написании отдельных положений настоящей политики использовались следующие нормативные документы:

- приказ Федерального Агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Федеральный Закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Федеральный Закон от 14.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный Закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008;
- «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденные Постановлением Правительства Российской Федерации от 15.09.2008 № 687;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11.02.2013 № 17;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России от 18.02.2013 № 21;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11.02.2014;
- ГОСТ Р ИСО/МЭК 27001-2021 «Методы и средства обеспечения безопасности»;
- РС БР ИББС-2.5-2014 «Менеджмент инцидентов информационной безопасности».

5. ОБЛАСТЬ ДЕЙСТВИЯ

5.1. Настоящая Политика обязательна к исполнению всеми структурными подразделениями Университета и распространяется на всех ее работников (основных и совместителей), обучающихся (студентов, аспирантов, слушателей) и контрагентов Университета, и иных лиц, взявших на себя обязательства о неразглашении конфиденциальной информации, в порядке и на условиях, предусмотренных Политикой, законодательными

актами и иными нормативно правовыми документами Российской Федерации и локальными нормативными актами Университета.

5.2. Университет является правообладателем всей деловой информации и вычислительных ресурсов, приобретённых (полученных) и введённых в эксплуатацию в целях осуществления уставной деятельности в соответствии с действующим законодательством. Указанные права распространяются в том числе на голосовую и факсимильную связь, на содержание ящиков электронной почты, бумажные и электронные документы всех подразделений и работников Университета, созданные (полученные) в рамках исполнения трудовых обязанностей.

5.3. Настоящая Политика распространяется на всю информацию правообладателем которой является Университет и ресурсы её обработки, независимо от формы их представления и вида носителя (бумажный, электронный и т.п.), на котором они зафиксированы, включая охраняемую законом информацию (персональные данные, коммерческую тайну, в том числе учебную деятельность, сведения о сущности результатов интеллектуальной деятельности, выполнение научно-исследовательских работ и т.п.), за исключением государственной тайны.

6. СИТЕМА ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

6.1. Система защиты ИС Университета строится на основании:

- результатов проведения аудита ИБ;
- перечня информационных объектов Университета, подлежащих защите;
- актов классификации ИС Университета;
- модели угроз безопасности ИС;
- нормативно-правовых документов Российской Федерации.

Исходя из указанных документов определяется класс защищенности каждой ИС Университета с целью установления методов и способов защиты информации. Составляется перечень технических средствах и организационных мероприятиях для обеспечения необходимого уровня защиты ИС.

6.2. Используемые средства защиты информации должны поддерживаться в актуальном состоянии. При изменении элементов ИС, вывода из эксплуатации или ввода новых ИС, соответствующие изменения должны быть внесены в состав технических средств и организационных мероприятий защиты информации. Процессы обеспечения информационной безопасности Университета являются составной и неотъемлемой частью процессов управления информационными технологиями и осуществляются на основе циклической модели:

- «планирование - реализация - проверка - совершенствование - планирование -...».

7. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Порядок и периодичность проведения аудита ИБ Университета регламентируется внутренними организационно распорядительными документами. Проведение аудита ИБ отдельных структурных подразделений или отдельных ИС определяется на основании потребности в такой деятельности (при вводе в эксплуатацию новой ИС, в случае выявления инцидента ИБ и т.д.).

7.2. Аудит информационной безопасности Университета (проверки систем, обеспечивающих защиту информации) проводится через запланированные интервалы времени - для систем 3-его класса защищённости один раз в два года.

7.3. Основные цели проведения таких проверок:

- оценка текущего уровня защищённости ИС;
- выявление и локализация уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИС;
- оценка соответствия ИС требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию систем обеспечивающих ИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

7.4. В число задач, решаемых при проведении проверок и аудитов систем, обеспечивающих ИБ входят:

- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей политики безопасности и других организационно распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;

проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;

- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

7.5. Руководство и сотрудники Университета при проведении у них аудита ИБ обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

7.6. Внешний аудит ИБ проводится по отдельному решению руководителя. Внешний аудит ИБ проводится независимыми экспертами,

которым предоставляется доступ к ресурсам Университета и имеет целью получить более объективную оценку существующей системы управления ИБ. К внешнему аудиту допускаются эксперты, имеющие право, на проведение работ, подтверждённое наличием лицензий и сертификатов в данной области. При проведении внешнего аудита ИБ уполномоченный представитель аудитора обеспечивает документальное и, когда это необходимо, техническое подтверждение или замечания в плане того, что:

- политика ИБ отражает требования бизнеса и цели Университета;
- организационная структура управления ИБ создана;
- требования ИБ исполняются и удовлетворяют поставленным целям;
- защитные меры (например, межсетевые экраны, средства управления физическим доступом) настроены и используются правильно;
- риски оценены и остаются приемлемыми для Университета;
- система управления ИБ соответствует требованиям защиты.

8. ОБЪЕКТЫ ЗАЩИТЫ

8.1. В ИС Университета присутствует информация, содержащая:

- персональные данные (сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность);
- конфиденциальную информацию, или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Университета, информацию составляющую коммерческую тайну, информацию составляющую служебную тайну;
- сведения об учебной деятельности Университета, том числе сведения о сущности результатов интеллектуальной деятельности, сведения о выполнении научно- исследовательских, иные чувствительные по отношению к случайным и несанкционированным воздействиям сведения;
- открыто распространяемую информацию, необходимую для работы Университета.

8.2. В рамках обеспечения информационной безопасности к объектам защиты в Университете относятся все ИС, владельцем которых является Университет и содержащаяся в них информация, в том числе открытая (общедоступная), включая все элементы ИС:

- АРМ пользователей;
- сервера приложений;
- сервера СУБД;
- граница ЛВС;
- каналы передачи в сети общего пользования и (или) международного обмена, если по ним передается информация ограниченного доступа;
- различного рода носители защищаемой информации;

- в том числе документы на бумажных и машинных носителях, определенные как защищаемые нормативно-распорядительными документами Университета.

ОБЩИЕ ТРЕБОВАНИЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ УНИВЕРСИТЕТА

8.3. В Университете должен быть определен и документально зафиксирован перечень ИСПДн. В перечень ИСПДн должны быть включены все ИС в которых осуществляется обработка персональных данных.

8.4. Для каждой ИСПДн Университета должны быть определены и документально зафиксированы:

- цель обработки персональных данных в ИСПДн;
- объем и содержание персональных данных, обрабатываемых в ИСПДн;
- перечень действий с персональными данными и способы обработки персональных данных в ИСПДн.

Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать целям обработки. В том случае, если для выполнения информационного технологического процесса, реализацию которого поддерживает ИСПДн, нет необходимости в обработке определенных персональных данных, эти персональные данные должны быть удалены.

8.5. Информационные технологические процессы, в рамках которых обрабатываются персональные данные в ИСПДн, должны быть документированы.

8.6. В Университете должен быть определен и документально зафиксирован перечень (список) работников, осуществляющих обработку персональных данных в ИСПДн, без использования средств автоматизации, либо имеющих доступ к персональным данным. Доступ работников к персональным данным и обработка персональных данных работниками Университета должны осуществляться только в рамках их должностных обязанностей.

8.7. Обработка ПДн, содержащихся в ИСПДн либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПДн, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

8.8. Работники Университета, осуществляющие обработку персональных данных в ИСПДн, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также должны быть ознакомлены под роспись со всей

совокупностью требований по обработке и обеспечению безопасности персональных данных в части, касающейся их должностных обязанностей.

8.9. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются локальными нормативными актами Университета.

9. КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Для каждой ИСПДн Университета определяется класс защищенности в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

9.2. Проведение классификации информационных систем включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе;
- присвоение информационной системе соответствующего класса;
- документальное оформление.

9.3. По результатам анализа исходных данных типовой информационной системе присваивается один из четырёх классов защищенности информационной системы. Самый низкий класс - четвертый, самый высокий - первый.

9.4. При наличии специальных информационных систем - класс системы определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами, в дополнение к результатам анализа исходных данных.

9.5. Важно учитывать, что при наличии в ИСПДн подсистем (каждая из которых также является ИС) - информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

9.6. Результаты классификации информационных систем оформляются соответствующим актом:

- для объектов критической информационной инфраструктуры форма акта определена приказом ФСТЭК России от 06.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоений объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

- для ИСПДн акт классификации оформляется в соответствии с приказом ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13.02.2008 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

10. МОДЕЛЬ УГРОЗ

10.1. Модели угроз и нарушителя являются определяющими при развертывании, поддержании и совершенствовании системы обеспечения информационной безопасности Университета. Меры защиты информации, выбираемые для реализации в ИС, должны обеспечивать блокирование одной или нескольких угроз безопасности информации, включенных в модель угроз безопасности информации.

10.2. Наибольшими возможностями для нанесения ущерба Университета обладает ее собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне Университета), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

10.3. Для противодействия угрозам информационной безопасности в Университете на основе имеющегося опыта составляется модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ Университета при минимальных ресурсных затратах.

10.4. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

10.5. Стратегия обеспечения ИБ Университета заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программнотехнических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий или ошибочных действий персонала Университета и других пользователей ИС.

10.6. Источники угроз, уязвимости и объекты нападений, пригодные для реализации угрозы, типы возможных потерь, масштабы потенциального ущерба подробно определены документом «Модели угроз и нарушителей».

11. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ УНИВЕРСИТЕТА

11.1. Несмотря на то, что многие действия по защите информации производятся прозрачно для пользователей ИС, они остаются активными участниками процесса по защите конфиденциальной информации и являются вовлеченными в процессы обеспечения информационной безопасности в Университете. Поэтому все пользователи ИС Университета (работники, обучающиеся, контрагенты и т.д.) обязаны соблюдать в своей работе порядок обращения с конфиденциальными сведениями, ПДн, ключами электронной подписи и иной защищаемой информацией, соблюдать требования Политики и других документов, регламентирующих вопросы обеспечения информационной безопасности.

11.2. Общие обязанности пользователя ИС Университета:

- при работе руководствоваться документацией к программному обеспечению (руководству пользователя ПО);
- выполнять только те действия, которые необходимы для исполнения своих служебных обязанностей, любые посторонние действия в ИС запрещены;
- принимать меры по недопущению несанкционированного доступа посторонних лиц к защищаемой информации (персональным данным, информации, содержащей коммерческую тайну, информации для служебного пользования, своим учетным данным) во время работы с ИС Университета;
- знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;
- обращаться в службу поддержки пользователей ИТЦ или к специалистам, ответственным за системное администрирование, по всем техническим вопросам, связанным с работой в ИС Университета (подключения к корпоративной ИС домену, инсталляции и настройки ПО, удаления вирусов, предоставления доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонта и технического обслуживания и т.п.), а также за необходимой методологической или консультационной помощью по вопросам применения технических и программных средств ИС Университета;
- обращаться к администратору безопасности либо специалисту по информационной безопасности при возникновении у пользователя вопросов по защите информации и защите персональных данных в ИС;
- минимизировать вывод на печать обрабатываемую информацию.

Подробно обязанности пользователей ИС описаны в инструкциях, политиках, регламентах и других локальных нормативных документах Университета.

12. ОТВЕТСТВЕННОСТЬ

12.1. Общее руководство обеспечением информационной безопасности осуществляет проректор по комплексной безопасности Университета.

12.2. Руководители структурных подразделений Университета контролируют выполнение требований политики информационной безопасности во вверенных им подразделениях.

12.3. Руководители структурных подразделений несут персональную ответственность за неисполнение или ненадлежащее исполнение требований данной Политики во вверенных им подразделениях.

12.4. Каждый работник, обучающийся, контрагент и иные лица, взявшие на себя обязательства о неразглашении конфиденциальной информации - несут персональную ответственность за неисполнение обязательств, а также неисполнение или ненадлежащее исполнение требований данной Политики при выполнении договорных, должностных или функциональных обязанностей.

12.5. Возложение полномочий и определение структурного подразделения (работников) Университета, ответственных за обеспечение информационной безопасности (в том числе персональных данных) подтверждается изданием соответствующего локального правового акта - приказа ректора.

12.6. В случае установленных нарушений требований Политики, локальных нормативных актов по обеспечению информационной безопасности или законодательства Российской Федерации - работники, обучающиеся и контрагенты могут быть ограничены в правах доступа к защищаемым ресурсам информационной среды Университета, а также привлечены к уголовной, административной, гражданско-правовой или дисциплинарной ответственности согласно действующего законодательства Российской Федерации.

13. КОНТРОЛЬ И ПЕРЕСМОТР

13.1. Политика является локальным нормативным актом Университета постоянного действия, которая утверждается на Учёном совете, вводится в действие, изменяется и признаётся утратившей силу приказом ректора Университета.

13.2. Контроль за исполнением требований Политики ИБ осуществляется руководителями структурных подразделений и администратором безопасности (лицом ответственным за информационную безопасность).

13.3. Пересмотр Политики информационной безопасности производится не реже одного раза в три года и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

13.4. Пересмотр Политики осуществляется Учёным советом Университета.

13.5. Внеплановое внесение корректив в настоящую Политику может производится по результатам анализа инцидентов информационной безопасности, актуальности и эффективности используемых мер по защите информационных ресурсов, результатам проведения аудита информационной безопасности и других контрольных мероприятий.

14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

14.1. Политика является общедоступным документом.

14.2. Требования Политики могут развиваться другими внутренними нормативными документами Университета, которые её дополняют и уточняют.

14.3. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Университета, настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам.

Проректор по комплексной безопасности
ФГБОУ ВО «ХТУ» С.С. Азаркин

ЛИСТ ознакомления с приказом
от «___»_____2025 г. №_____

«ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ФГБОУ ВО «Херсонский технический университет»

№ п/п	Ф.И.О.	Должность работника	Дата	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				