Приложение 3
к приказу № 883 от «1» 08 2022 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

УТВЕРЖДАЮ
И.о. ректора
_____ Б.И. Сидлер
«__» _____ 2022 г.

ПОЛОЖЕНИЕ

Об отделе информационной безопасности

Тольятти 2022

Оглавление

1. Назначение

1.1. Отдел информационной безопасности (далее – Отдел) является структурным подразделением ФГБОУ ВО «Тольяттинский государственный университет» (далее – ТГУ, Университет).

1.2. Деятельность Отдела направлена:

а) на исключение или существенное снижение негативных последствий (ущерба) в отношении ТГУ вследствие нарушения функционирования информационных систем, информационно- телекоммуникационных сетей и автоматизированных систем управления в результате реализации угроз безопасности информации;

б) на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

в) на повышение защищенности ТГУ от возможного нанесения ему материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования;

г) на обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры ТГУ;

д) на обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем ТГУ.

2. Структура управления

2.1. Отдел создается и ликвидируется приказом ректора ТГУ.

2.2. Отдел подчиняется проректору по безопасности.

2.3. Численность сотрудников отдела определяется текущими задачами, функционалом подразделения и штатным расписанием.

3. Основные задачи

3.1. Основными задачами отдела являются:

3.1.1. Организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в Университете.

3.1.2. Выявление угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно- аппаратных средств.

3.1.3. Предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

3.1.4. Поддержание стабильной деятельности университета и его производственных процессов в случае проведения компьютерных атак.

3.1.5. Взаимодействие с Национальным координационным центром по компьютерным инцидентам.

3.1.6. Взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

3.1.7. Обеспечение нормативно-правового обеспечения использования информационных ресурсов.

4. Основные функции

4.1. Разработка концепции и политики информационной безопасности (далее - ИБ) университета, включая разработку регламентов, стандартов, руководств и должностных инструкций по ИБ.

4.2. Определение целей и постановка задач по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации.

4.3. Планирование, согласование и организация мероприятий по защите информации непосредственно на объектах информатизации.

4.4. Разработка организационно-распорядительной документации по ИБ и доведение ее до сотрудников в части их касающейся.

4.5. Контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

4.6. Организация и осуществление обработки и защиты персональных данных субъектов, состоящих в договорных и иных отношениях с университетом.

4.7. Проведение оценки соответствия объектов, помещений, технических средств, программ, алгоритмов требованиям защиты информации по соответствующим уровням безопасности.

4.8. Организация и проведения аудита информационных систем и программного обеспечения.

4.9. Согласование технических заданий, проектной и другой технической документации на вновь создаваемые информационные системы или программное обеспечение, услуги в области информационных технологий в части выполнения требований по защите информации.

4.10. Разработка моделей угроз, анализ рисков и разработка и осуществление мероприятий по их минимизации.

4.11. Проведение специальных исследований и контрольных проверок по выявлению возможных каналов утечки информации, в том числе по техническим каналам, разработка мер по их устранению и предотвращению.

4.12. Определение возможностей несанкционированного доступа к информации, ее уничтожения или искажения, разработка соответствующих мер по защите.

4.13. Определение уязвимостей информационных систем, сайтов, серверов, выработка рекомендаций по их устранению.

4.14. Разработка проектов и создание систем технической защиты информации, участие в создании систем защиты.

4.15. Установка, настройка и администрирование средств защиты информации.

4.16. Создание защищенных каналов связи, приобретение и установка и настройка средств криптографической защиты информации.

4.17. Организация и контроль резервного копирования критически важной информации.

4.18. Контроль настроек сетевого оборудования по минимально разрешенному уровню доступа.

4.19. Контроль разграничения доступа к информационным системам, базам данных, инфраструктуре сети согласно ролевой матрице доступа.

4.20. Контроль за использованием закрытых каналов связи и ключей с цифровыми

подписями.

4.21. Контроль удаленного доступа к инфраструктуре сети университета.

4.22. Контроль состояния антивирусной защиты, анализ сетевых атак, аномального трафика и сетевой активности.

4.23. Осуществление мониторинга действий пользователей в информационных системах.

4.24. Представление в Национальный координационный центр по компьютерным инцидентам информации о выявленных компьютерных инцидентах.

4.25. Исполнение указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами, Федеральной службой по техническому и экспортному контролю по результатам мониторинга защищенности информационных ресурсов, принадлежащих органу (организации) либо используемых органом (организацией), доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет».

4.26. Проведение анализа и контроля за состоянием защищенности систем и сетей и разработка предложений по модернизации (трансформации) основных процессов университета в целях обеспечения информационной безопасности.

4.27. Организация и проведение плановых проверок режима защиты информации, разработка соответствующей документации, анализ результатов, расследование нарушений.

4.28. Организация и проведение занятий по повышению осведомленности пользователей в соблюдении требований ИБ.

4.29. Обеспечение сотрудников университета информационной поддержкой по вопросам ИБ.

4.30. Выполнение иных функций, исходя из поставленных руководством университета целей и задач в рамках обеспечения информационной безопасности.

5. Права и ответственность

5.1. Отдел информационной безопасности имеет право:

5.1.1. Запрашивать и получать от институтов, кафедр, научных и иных структурных подразделений университета информацию, необходимую для выполнения функций, возложенных на структурное подразделение.

5.1.2. Готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности организаций, имеющих лицензии на соответствующий вид деятельности.

5.1.3. Контролировать деятельность любого структурного подразделения университета по выполнению требований к обеспечению информационной безопасности.

5.1.4. Постоянно повышать профессиональные компетенции, знания и навыки работников в области обеспечения информационной безопасности.

5.1.5. Участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп.

5.1.6. Вносить предложения руководству университета о приостановлении работ в случае обнаружения факта нарушения информационной безопасности.

5.1.7. Вносить на рассмотрение руководству университета предложения по вопросам деятельности подразделения.

5.1.8. Проводить плановые и внеплановые проверки;

5.1.9. Представлять Университет при проведении проверок регуляторами.

5.2. Сотрудники отдела информационной безопасности несут ответственность за:
- выполнение должностных инструкций;
- качество выполняемых работ и представляемых услуг;
- соблюдение требований настоящего Положения и Устава ТГУ, внутренних правил и инструкций, в том числе правил техники безопасности и противопожарной безопасности;
- сохранность доверенных им материальных ценностей.

6. Взаимодействие со структурными подразделениями и сторонними организациями

6.1. Для выполнения функций, задач и реализации прав Отдел взаимодействует со всеми структурными подразделениями ТГУ и сторонними организациями по вопросам осуществления текущей деятельности.

Начальник отдела информационной безопасности _____ (подпись) _____ (дата) И.А. Власов

СОГЛАСОВАНО

Проректор по безопасности _____ (подпись) _____ (дата) Б.И. Сидлер

Начальник юридического отдела _____ (подпись) _____ (дата) Т.А. Киселева

Директор центра менеджмента качества _____ (подпись) _____ (дата) Д.В. Манасян

Начальник отдела льгот и компенсаций _____ (подпись) _____ (дата) Е.В. Поликаркина

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00B0C6268C137AFEE0073B516BE919F334
Владелец: Криштал Михаил Михайлович
Действителен: с 13.09.2024 до 07.12.2025