Приложение №21 к приказу

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский химико-технологический университет имени Д.И. Менделеева»
(РХТУ им. Д.И. Менделеева)

УТВЕРЖДЕНО
приказом и.о. ректора
РХТУ им. Д.И. Менделеева
от «15» мая 2024 г. №37 ОД

ПОЛОЖЕНИЕ ОБ УПРАВЛЕНИИ ИНФОРМАТИЗАЦИОННОЙ БЕЗОПАСНОСТИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Управление информационной безопасности (далее Управление) является структурным подразделением Федерального государственного бюджетного образовательного учреждения высшего образования «Российский химико - технологический университет имени Д.И. Менделеева» (далее – РХТУ, Университет).

1.2. Настоящее Положение регулирует деятельность Управления, определяет его задачи, функции, порядок организации работы.

1.3. В своей деятельности Управление руководствуется законодательством Российской Федерации, уставом и локальными нормативными актами РХТУ, а также настоящим Положением.

1.4. Структуру и штатное расписание Управления утверждает ректор РХТУ.

1.5. Трудовые обязанности работников Управления, условия их труда определяются трудовыми договорами, заключаемыми с каждым работником, Правилами внутреннего трудового распорядка РХТУ и иными локальными нормативными актами РХТУ, а также должностными инструкциями работников Управления.

1.6. Полное наименование Управления – Управление информационной безопасности.

Сокращенное наименование Управления – Управление инф.без.

1.7. Координацию деятельности Управления осуществляет директор Департамента информационных технологий в соответствии с установленным в

Университете распределением обязанностей (далее – координирующий руководитель).

1.8. К документам Управления имеют право доступа, помимо его работников, ректор Университета, координирующий руководитель, лица, уполномоченные для проверки деятельности Управления, а также иные лица в соответствии с локальными нормативными актами Университета и законодательством Российской Федерации.

1.9. Взаимодействие Управления с другими структурными подразделениями РХТУ определяется задачами и функциями, возложенными на него настоящим Положением.

1.10. Настоящее Положение и вносимые в него изменения утверждаются приказом РХТУ.

2. ОСНОВНЫЕ ЗАДАЧИ

Основными задачами Управления являются:

2.1. реализация стратегии цифровой трансформации Университета в части обеспечения цифровой инфраструктуры Университета по направлению деятельности;

2.2. разработка единой политики (концепции) обеспечения информационной безопасности Университета, определение требований к системе защиты информации Университета;

2.3. реализация требований информационной безопасности в серверной и системно-технической инфраструктуре, информационных системах и ресурсах;

2.4. исполнение мероприятий по обеспечению информационной безопасности, защите коммерческой тайны и информации ограниченного доступа, защите персональных данных, защите детей от информации, причиняющей вред их здоровью и (или) развитию;

2.5. контроль и оценка эффективности принятых мер и применяемых средств защиты информации;

2.6. мониторинг информационной безопасности и реагирование на инциденты информационной безопасности.

3. ФУНКЦИИ

В соответствии с возложенными задачами Управление выполняет следующие функции:

3.1. в части организации и исполнения мероприятий по обеспечению информационной безопасности, защите коммерческой тайны и информации ограниченного доступа, персональных данных:

3.1.1. оценивает на наличие рисков и угроз информационной безопасности существующие, разрабатываемые и внедряемые в Университете информационные системы, ИТ-ресурсы, ПО;

3.1.2. принимает участие в проектировании, приемке, сдаче в промышленную эксплуатацию программных средств и автоматизированных систем Университета в части требований к обеспечению информационной безопасности;

3.1.3. выявляет и локализует риски и угрозы информационной безопасности Университета;

3.1.4. контролирует защищенность информационной инфраструктуры Университета, выявляет и устраняет уязвимости;

3.1.5. организует проведение профилактических работ по выявлению и устранению инцидентов информационной безопасности, в том числе связанных с незаконным доступом к информационным ресурсам, утечкой конфиденциальной информации, компьютерными атаками, распространением вредоносного программного обеспечения;

3.1.6. минимизирует и устраняет негативные последствия, материальный ущерб, явившиеся следствием инцидентов информационной безопасности;

3.1.7. организует проведение профилактических работ по выявлению и пресечению нарушений со стороны работников Университета требований законодательства РФ, локальных нормативных актов в сферах обеспечения информационной безопасности, защиты коммерческой тайны и информации ограниченного доступа, персональных данных, инсайдерской информации, соблюдения норм парольной защиты, а также правил доступа к информационным ресурсам и сервисам и хранения ключей электронной подписи;

3.1.8. внедряет в сфере обеспечения информационной безопасности современные технические средства, ПО, обновление существующих информационных систем, предназначенных для защиты информации Университета;

3.1.9. разрабатывает и совершенствует стратегию развития информационной безопасности Университета, регулирующие локально-нормативные акты и нормативно-технические документы в сфере обеспечения информационной безопасности;

3.1.10. обеспечивает снижение рисков разглашения, утечки конфиденциальной информации Университета;

3.1.11. разрабатывает и реализует меры по защите коммерческой тайны, информации ограниченного доступа Университета;

3.1.12. обеспечивает исполнение в Университете законодательства РФ, локальных нормативных актов в сфере защиты персональных данных;

3.1.13. проводит консультирование работников Университета по всему комплексу вопросов обеспечения безопасности информации;

3.1.14. обеспечивает техническое обслуживание средств защиты информации, составление рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации;

3.1.15. организует регистрацию, сбор, хранение и обработку данных со всех средств защиты информации;

3.1.16. координирует расследования инцидентов в информационно-телекоммуникационной сфере с документированием и анализом результатов расследования с использованием средств защиты информации;

3.1.17. принимает участие в рассмотрении и согласовании заявок на предоставление работникам, сторонним юридическим и физическим лицам доступа к информационным системам Университета;

3.1.18. организует и проводит служебные проверки и расследования в отношении инцидентов информационной безопасности, в том числе связанных с незаконным доступом к информационным ресурсам, утечкой, разглашением коммерческой тайны, информации ограниченного доступа, персональных данных, инсайдерской информации, компьютерными атаками, распространением вредоносных кодов, нарушениями штатного функционирования информационной инфраструктуры Университета;

3.1.19. участвует в списании и утилизации средств защиты информации.

3.2. в части реализации мер организационного и информационно-аналитического характера в сфере обеспечения информационной безопасности Университета:

3.2.1. разрабатывает ежегодные и тематические планы работ по обеспечению информационной безопасности;

3.2.2. исполняет поручения и решения руководства Университета и координирующего руководителя в сфере обеспечения информационной безопасности;

3.2.3. обеспечивает внедрение и ведение информационно-аналитических, справочных баз данных в сфере обеспечения информационной безопасности Университета.

3.3. в части информирования руководства о ходе и результатах деятельности по линии информационной безопасности:

3.3.1. информирует руководство Университета и координирующего руководителя в отношении рисков и угроз в сфере обеспечения информационной безопасности, условий и причин, способствующих утечке коммерческой и служебной информации Университета, персональных данных, нарушений штатного функционирования информационной инфраструктуры Университета, фактов несоблюдения работниками норм законодательства РФ, локальных нормативных актов в области обеспечения информационной безопасности;

3.3.2. предоставляет руководству Университета и координирующему руководителю отчетные документы, в том числе докладные и служебные записки, протоколы, заключения, акты, материалы проведенных опросов, объяснения, фото, аудио и видеоматериалы о ходе и результатах деятельности Управления в сфере обеспечения информационной безопасности Университета;

3.3.3. направляет предложения руководству Университета и координирующему руководителю о привлечении установленным законодательством РФ порядком к дисциплинарной, административной, гражданской, материальной и уголовной ответственности работников, сторонних юридических и физических лиц, виновных в нанесении ущерба Университету, допустивших нарушения положений и норм законодательства РФ, локальных нормативных актов в области информационной безопасности;

3.3.4. информирует работников Университета в рамках предупредительно-профилактической деятельности Управления о результатах работы в сфере обеспечения информационной безопасности.

3.4. в части взаимодействия с регуляторами в сфере информационной безопасности:

3.4.1. проводит проверки при получении запросов из федеральных органов исполнительной власти, осуществляющих государственный контроль в области обращения и защиты информации, законности предоставления запрашиваемых данных, направляет поручения на их исполнение в части касающейся в заинтересованные структурные подразделения Университета, обобщает, подготавливает и согласовывает в установленные законодательством РФ сроки ответов в надзорные органы РФ;

3.4.2. осуществляет подготовку в федеральные органы исполнительной власти, осуществляющих государственный контроль в области обращения и защиты информации, правоохранительные органы РФ материалов с признаками совершения преступлений в сфере информационной безопасности работниками Университета, сторонними юридическими и физическими лицами, причинившими вред интересам Университета.

3.5. в части планирования, подготовки и исполнения бюджетов, а также организации закупок в сфере обеспечения информационной безопасности:

3.5.1. осуществляет подготовку предложений в бюджет Университета в интересах информационной безопасности;

3.5.2. разрабатывает технические задания к конкурсной документации, осуществляет сопровождение договоров в части информационной безопасности;

3.5.3. осуществляет приемку и подготовку к эксплуатации средств защиты информации;

3.5.4. оптимизирует расходы на информационную безопасность.

Положение разработал:

Заместитель директора Департамента информационных технологий _____ А.В. Матасов "___" _____ 2024 г.
(подпись) (инициалы, фамилия) (дата согласования)

Согласовано:

Правовой отдел (на правах управления) _____ _____ "18" 04 2024 г.
(подпись) (инициалы, фамилия) (дата согласования)

Управление по работе с персоналом _____ _____ "27" 04 2024 г.
(подпись) (инициалы, фамилия) (дата согласования)

Финансовый департамент _____ _____ "25" 04 2024 г.
(подпись) (инициалы, фамилия) (дата согласования)

РХТУ им. Д.И. Менделеева
ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Владелец: *Иванов Александр Сергеевич*
Ведущий специалист, Отдел управления качеством образовательной деятельности
Подписан: 02:11:2024 15:20:16