Код
02069438

по ОКПО

Федеральное государственное бюджетное образовательное учреждение высшего образования
“Уфимский государственный авиационный технический университет”

ПРИКАЗ

19.07.2022 УФА № 1047-О

Об утверждении Политики ФГБОУ ВО «УГАТУ» в области информационной безопасности

В целях создания единой системы обеспечения информационной безопасности в федеральном государственном бюджетном образовательном учреждении высшего образования «Уфимский государственный авиационный технический университет» и его филиалах, принятия необходимых мер по защите информационных ресурсов, процессов обработки информации и информационной инфраструктуры университета, ПРИКАЗЫВАЮ:

1. Утвердить Политику Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский государственный авиационный технический университет» в области информационной безопасности (Приложение №1).
2. Отделу документационного обеспечения и архива обеспечить рассылку настоящего приказа во все структурные подразделения университета и его филиалы.
3. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. ректора Р.Д. Алчанова

Приложение №1
к приказу от 19.07.2022 № 1047-О

ПОЛИТИКА
Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский государственный авиационный технический университет» в области информационной безопасности

1. Общие положения

1.1. Политика Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский государственный авиационный технический университет» (далее - университет) в области информационной безопасности (далее - Политика) является локальным нормативным актом и определяет цель и задачи защиты информации, основные принципы и способы достижения требуемого уровня информационной безопасности в университете.

1.2. Положения и требования данного документа распространяются на все структурные подразделения университета, включая филиалы и являются обязательными для выполнения всеми работниками университета.

1.3. Законодательной основой настоящей Политики являются:

- Конституция Российской Федерации;
- Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 29.07.2004 №98-ФЗ «О коммерческой тайне»;
- Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федеральный закон Российской Федерации от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Закон Российской Федерации от 21.07.1993 №5485-1 «О государственной тайне»;
- Указ Президента Российской Федерации от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера»;
- Инструкция о порядке обращения со служебной информацией ограниченного распространения в Министерстве образования и науки Российской Федерации, утвержденная Приказом Министерства образования и науки Российской Федерации от 30.12.2010 №2233.

1.5. Политика является методологической основой для:

- создания единой системы управления информационной безопасностью университета;
- принятия управленческих решений, разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
- координации деятельности структурных подразделений университета при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, организационного и технического обеспечения безопасности информации.

2. Цель (назначение) Политики

2.1. Политика направлена на защиту информационных ресурсов, информационной инфраструктуры и процессов обработки информации университета от возможного нанесения им материального, физического или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи ее по каналам связи, а также минимизацию подобных рисков.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;
- целостности информации – состояние, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- конфиденциальности – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

2.2. Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается применением соответствующих мер информационной безопасности.

2.3. Для достижения цели политики и обеспечения указанных свойств должны выполняться следующие задачи:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями внутренних и внешних нарушителей, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей);
- обеспечение идентификации и аутентификации пользователей информационных ресурсов;
- защита от несанкционированной модификации используемых в информационной системе программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защита конфиденциальной информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3. Объекты защиты

3.1. Объектами, подлежащими защите в соответствии с настоящей Политикой, являются:

- информационные ресурсы содержащие конфиденциальную информацию (служебная информация ограниченного распространения, информация, составляющая коммерческую и государственную тайну, персональные данные (работников, обучающихся, аспирантов, докторантов, абитуриентов, лиц, выполняющих работы по договорам гражданско-правового характера, партнеров), открытая (общедоступная) информация, необходимая для осуществления деятельности университета и иная чувствительная информация;

- процессы обработки информации в информационных системах университета, информационные технологии (регламенты и процедуры сбора, обработки, хранения, выдачи и передачи информации);

- информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные элементы информационной среды.

4. Меры обеспечения информационной безопасности

4.1. Меры обеспечения информационной безопасности подразделяются на: правовые; организационные; технические (аппаратные, программные, криптографические).

4.2. К правовым мерам относятся выполнение норм действующего законодательства в области защиты информации.

Правовые меры устанавливают правила использования информации и определяют ответственность за нарушение этих правил.

4.3. Организационные меры – это меры организационного характера, регламентирующие процессы функционирования информационных систем, деятельность обслуживающего персонала, а также порядок действия пользователей таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

4.4. Технические меры заключаются в обеспечении безопасности объектов защиты путем применения технических, программных, аппаратных, программно-аппаратных и криптографических средств защиты информации

5. Система управления информационной безопасностью. Основные задачи и функции

5.1. Система управления информационной безопасностью является частью общей системы управления университетом и предназначена для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности.

5.2. Организация работы и эффективное функционирование системы управления информационной безопасностью в университете, возлагается на управление информационных технологий.

Управление информационных технологий, для выполнения конкретных задач в области информационной безопасности вправе привлекать кафедру вычислительной

техники и защиты информации, учебно-научный центр информационной безопасности и иные структурные подразделения университета, сторонние организации, имеющие соответствующие лицензии на данный вид деятельности, а также создавать рабочие группы и комиссии.

5.3. Основные задачи:

- проведение единой политики в области безопасности информации, организация и координация работ по защите информации;
- предотвращение угроз безопасности университета вследствие несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации или иных форм незаконного вмешательства в информационные ресурсы и информационные системы;
- принятие необходимых мер, способствующих повышению уровня информационной безопасности, в том числе обеспечению физической, инженерно-технической безопасности объектов университета;
- контроль соблюдения требований законодательства РФ в сфере информационной безопасности.

5.4. Основные функции:

- организация системы защиты информации, контроль соблюдения требований законодательства РФ в сфере информационной безопасности;
- создание единой концепции информационной безопасности, определение мероприятий, направленных на её реализацию;
- планирование и реализация задач, способствующих повышению уровня информационной безопасности;
- организация и проведение мероприятий по информационной безопасности;
- реализация, развитие и поддержка системы антивирусной защиты;
- выявление технических каналов утечки информации, в том числе за счет несанкционированного доступа к информации, а также ее разрушения (уничтожения) или искажения, разработка соответствующих мер по защите информации;
- обеспечение безопасности информационной инфраструктуры;
- обеспечение сохранности информационных ресурсов, соблюдения правильности выполнения процессов обработки информации и защите информационной инфраструктуры;
- контроль за соблюдением требований информационной безопасности подчиненными работниками;
- соблюдение порядка обращения с конфиденциальной информацией в т.ч. документами, носителями ключевой информации и другой защищаемой информации;
- выполнение требований настоящей Политики и других документов по информационной безопасности.

6. Локальные нормативные акты университета в области информационной безопасности

6.1. Реализация положений настоящей Политики в университете предусматривает принятие отдельных локальных нормативных актов: регламентов, требований, положений, инструкций и иных документов.

Принятие таких документов направлено на разъяснение и конкретизацию отдельных положений Политики, а также обеспечение безопасности информации, подлежащей защите в соответствии с законодательством Российской Федерации, информационной инфраструктуры, процессов обработки информации, порядка

обращения с конфиденциальной информацией, безопасностью персональных данных и обеспечения физической и инженерно-технической безопасности объектов университета.

7. Контроль и ответственность

7.1. Общий контроль за соблюдением требований, предписанных настоящей Политикой, возлагается на управление информационных технологий.

7.2. Контроль и профилактика нарушений информационной безопасности и защиты информации осуществляется на плановой и внеплановой основах.

7.3. Контроль (оценка) эффективности принятых технических мер по защите информации проводится управлением информационных технологий самостоятельно или привлекаемыми для этой цели организациями, имеющими соответствующие лицензии на данный вид деятельности.

7.4. Нарушение положений настоящей Политики может повлечь за собой дисциплинарную, административную, гражданско-правовую, уголовную или иную ответственность в соответствии с законодательством Российской Федерации.

ПРОЕКТ ВНОСИТ

УИТ Начальник управления Должность	**275745** 28.06.2022 15:29:32 подпись	О. Ф. Бикбулатова расшифровка подписи

СОГЛАСОВАНО

Первый проректор по науке Должность	**161504** 28.04.2022 13:55:47 подпись	Еникеев Р. Д. расшифровка подписи
Проректор по учебной работе Должность	**171908** 06.05.2022 19:46:17 подпись	Елизарьев А. Н. расшифровка подписи
Проректор по инновационной деятельности Должность	**172113** 07.05.2022 18:05:27 подпись	Агеев Г. К. расшифровка подписи
Проректор по административной и правовой деятельности Должность	**280910** 01.07.2022 08:51:29 подпись	Мифтахова А. М. расшифровка подписи
Проректор по экономике и финансам Должность	**177909** 12.05.2022 20:33:39 подпись	Алчанова Р. Д. расшифровка подписи
Проректор по хозяйственной деятельности Должность	**171981** 06.05.2022 20:42:33 подпись	Тарасюк И. В. расшифровка подписи
Проректор по безопасности Должность	**169966** 06.05.2022 11:12:45 подпись	Мишутов В. А. расшифровка подписи
ПУ Начальник управления Должность	**303133** 18.07.2022 18:17:42 подпись	Манукян Н. Г. расшифровка подписи

ИСПОЛНИТЕЛЬ

УИТ Начальник отдела Должность	**301979** 18.07.2022 10:52:03 подпись	Семенов А. Г. расшифровка подписи