Федеральное государственное бюджетное образовательное учреждение
высшего образования «Астраханский государственный медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО Астраханский ГМУ Минздрава России)

ПРИНЯТО
Ученым Советом ФГБОУ ВО
Астраханский ГМУ
Минздрава России
Протокол №_____

«___» _____ 2019 г.

«УТВЕРЖДАЮ»
Ректор ФГБОУ ВО
Астраханский ГМУ
Минздрава России
д.м.н., профессор
_____О.А. Башкина

«___» _____ 2019 г.

ПОЛОЖЕНИЕ
об отделе информационной безопасности
Федерального государственного бюджетного образовательного учреждения высшего образования «Астраханский государственный медицинский университет» Министерства здравоохранения Российской Федерации

Астрахань
2019

1. Общие положения

1.1. Настоящее Положение определяет правовое положение, задачи и функции отдела информационной безопасности (далее – Положение) федерального государственного бюджетного образовательного учреждения высшего образования «Астраханский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее - ФГБОУ ВО Астраханский ГМУ Минздрава России, Университет).

1.2. Отдел информационной безопасности (далее - отдел) в своей работе руководствуется:

- законодательством Российской Федерации;
- подзаконными и ведомственными нормативными правовыми актами;
- Уставом, локальными нормативными актами Университета, в том числе закрепляющими антикоррупционные стандарты поведения работников учреждения;
- организационно-распорядительными документами Университета; методическими рекомендациями, разработанными по вопросам, связанным с функциями отдела.

1.3. Отдел является самостоятельным структурным подразделением Университета и подчиняется непосредственно проректору по общественной и информационной безопасности Университета.

1.4. Штатное расписание отдела утверждает ректор ФГБОУ ВО Астраханский ГМУ Минздрава России.

1.5. Руководство отделом осуществляет начальник отдела в соответствии с должностной инструкцией. На время отсутствия начальника отдела его обязанности исполняет работник, назначенный в установленном порядке, который приобретает соответствующие права и несет ответственность за неисполнение или ненадлежащее исполнение обязанностей, возложенных на него в связи с замещением.

1.6. Все сотрудники отдела назначаются на должность и освобождаются от занимаемой должности приказом ректора ФГБОУ ВО Астраханский ГМУ Минздрава России по представлению проректора по общественной и информационной безопасности Университета.

1.7. Отдел в ходе своей деятельности осуществляет рабочее взаимодействие со структурными подразделениями Университета.

1.8. Реорганизация и ликвидация отдела осуществляется в соответствии с Уставом ФГБОУ ВО Астраханский ГМУ Минздрава России.

2. Задачи

Основные задачи отдела заключаются в следующем.

2.1. Разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.

2.2. Обеспечение постоянного контроля в подразделениях Университета за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.

2.3. Разработка и внесение предложений руководству ФГБОУ ВО Астраханский ГМУ Минздрава России по совершенствованию и развитию корпоративной системы обеспечения безопасности и защиты информации, в том числе персональных данных.

3. Функции

Для выполнения поставленных задач отдел осуществляет следующие функции.

3.1. Готовит и представляет на рассмотрение руководству Университета проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных.

3.2. Организует и проводит во взаимодействии с заинтересованными подразделениями классификацию информационных систем на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных в соответствии с установленными требованиями.

3.3. Разрабатывает и реализует комплекс организационных мер по обеспечению защиты информации от:

- неправомерного доступа;
- уничтожения;
- модифицирования;
- блокирования;
- копирования;
- предоставления;
- распространения;
- а также от иных неправомерных действий в отношении такой информации.

3.4. Разрабатывает инструкции по информационной безопасности:

- инструкции по организации антивирусной защиты;
- инструкции по безопасной работе в Интернете.

3.5. Для защиты информации, в том числе персональных данных от неправомерного доступа отдел обеспечивает:

- контроль за строгим соблюдением принятого Университетом Порядка доступа к конфиденциальной информации, в том числе к персональным данным;
- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

3.6. Отдел при создании и эксплуатации корпоративных информационных систем:

- самостоятельно разрабатывает и внедряет методы и способы защиты информации, соответствующие установленным требованиям;

- согласовывает с руководством Университета планируемые для использования в целях защиты информации методы и способы при условии их соответствия установленным требованиям.

3.7. Отдел:

- разрабатывает и реализует меры организационного и технического характера по недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

- организует и (или) проводит экспертизу технических средств, используемых при обработке информации на предмет соответствия возможностей защиты информации указанных средств установленным требованиям.

3.8. Отдел разрабатывает и реализует меры по информированию и обучению сотрудников Университета, в том числе вновь принимаемых на работу лиц, по вопросам защиты информации и персональных данных.

3.9. Отдел контролирует выполнение установленных требований по:

- осуществлению обмена персональными данными при их обработке в информационных системах по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств:

- размещению информационных систем, специального оборудования и охране помещений, в которых ведется работа с персональными данными, организации режима обеспечения безопасности в этих помещениях в части обеспечения сохранности носителей персональных данных и средств защиты информации, а также исключения возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

- соблюдению парольной защиты;

- соблюдению установленного регламента работы с электронной почтой;

- соблюдению требований к программному обеспечению и его использованию;

- антивирусный контроль магнитных носителей информации и файлов электронной почты, поступающих в Университет;

- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации;

- контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём;

- контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК;

- контроль пользования Интернетом.

3.10. В соответствии с установленными нормативно-правовыми актами, требованиями отдел обеспечивает:

- функционирование и поддержание работоспособности средств и систем защиты информации, в пределах, возложенных на них обязанностей;

- немедленное информирование руководства Университета о выявленных нарушениях и несанкционированных действиях пользователей, в том числе о случаях несанкционированного доступа в Интернет, а также принятие необходимых мер по устранению нарушений;

- принятие мер совместно с программистами по восстановлению работоспособности средств и систем защиты информации;

- создание и удаление учетных записей пользователей;

- администрирование работы сервера ЛВС, размещение и классифицирование информации на сервере ЛВС;

- установление по согласованию с ректором Университета критериев доступа пользователей на сервер ЛВС;

- формирование и представление паролей для новых пользователей, администрирование прав пользователей;

- отслеживание работы антивирусных программ, проведение один раз в неделю полной проверки компьютеров на наличие вирусов;

- регулярное выполнение резервного копирования данных на сервере, при необходимости восстановление потерянных или поврежденных данных;

- ежемесячная подача проректору по общественной и информационной безопасности Университета статистической информации по пользованию Интернетом;

- ведение и учет пользователей «точки доступа к Интернету». В случае необходимости, лимитирование времени работы пользователя в Интернете и объема скачиваемой информации;

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с персональными данными в информационной системе;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- разбор и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности

персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание системы защиты информации, в том числе персональных данных;
- ежегодное планирование работы по совершенствованию системы защиты информации, в том числе персональных данных;
- подготовку и предоставление отчётов руководству Университета, а также по требованию надзорных и иных уполномоченных органов об организационных и технических мероприятиях по защите информации, в том числе персональных данных;
- постоянный контроль за обеспечением уровня защищенности информации.

4. Взаимодействие

Для решения поставленных задач и осуществления предусмотренных настоящим Положением функций отдел взаимодействует:

- с ректоратом Университета;
- с любыми иными подразделениями Университета;
- с государственными, муниципальными органами, учреждениями и организациями, с надзорными органами, а также с иными органами, предприятиями и организациями.

В ходе взаимодействия руководитель и сотрудники отдела:

- в установленном порядке, получают необходимую для осуществления деятельности отдела информацию, разъяснения, уточнения, нормативные и иные документы;
- готовят и в установленном порядке вносят ректору Университета предложения по проведению организационных и технических мероприятий, изданию локальных нормативных актов, принятию иных мер по установленным направлениям деятельности в сфере защиты информации, в том числе персональных данных;
- готовят и в установленном порядке предоставляют информацию по находящимся в их компетенции вопросам в сфере защиты информации, в том числе персональных данных, по запросам подразделений Университета, государственных, муниципальных органов, учреждений и организаций, надзорных органов, а также иных органов, предприятий и организаций.

5. Ответственность

5.1 Ответственность за ненадлежащее и несвоевременное выполнение функций отдела несет начальник отдела.

5.2 Ответственность работников отдела, устанавливается действующим законодательством Российской Федерации и должностными инструкциями.