

Курс «Защита рабочих и личных данных в кризисное время (для отрасли здравоохранения)»

Актуальность курса:

С февраля 2022 года информационная инфраструктура России подвергается беспрецедентным угрозам. Более 100 тысяч человек задействованы в кибератаках на Россию. Так, с 24 февраля 2022 года были похищены персональные данные 65 миллионов россиян.

Учреждения здравоохранения особенно чувствительны к инцидентам кибербезопасности, поскольку аккумулируют в своих информационных системах большие массивы персональных данных, в том числе, данных о здоровье граждан, последствиями утечки которых могут стать не только мошеннические действия или причинение морального ущерба, но и угроза здоровью и жизни людей. Кроме того, медицинские учреждения относятся к субъектам критической информационной инфраструктуры, что подразумевает необходимость обеспечения особых мер информационной безопасности.

Ситуацию усложняет то, что в медицинских учреждениях применяется большое число разнородного программного обеспечения, слабо интегрированных между собой, специалистов по информационной безопасности недостаточно, а объем внедрения средств защиты информации в настоящий момент невелик.

Указанные проблемы отражены в Концепции информационной безопасности в сфере здравоохранения, утвержденной Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности 10.03.2022.

Также в связи с интенсификацией кибератак и учащением случаев утечек информации, приняты меры к ужесточению нормативно-правового регулирования кибербезопасности. Указы Президента, вышедшие в марте и в мае 2022 г., вменяют в обязанность субъектам критической информационной инфраструктуры принимать дополнительные организационные меры к обеспечению кибербезопасности. Кроме того, внесены изменения в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», распространяющие часть мер, применяемых к защите критической информационной инфраструктуре, на операторов персональных данных.

Считаем, что повышение цифровой грамотности сотрудников организаций здравоохранения и профильных органов власти, их уровня осведомленности об угрозах кибербезопасности, способах защиты от атак и предотвращения утечек информации, цифровой гигиены, а также обучение специалистов в области информационной безопасности современным подходам и методикам защиты информации, использованию современного инструментария, являются важными мерами предупреждения утечек данных и противодействия кибератакам.

Наша компания не только осуществляет разработку средств защиты данных, но и с 2020 года проводит бесплатные обучающие мероприятия по грамотности в сфере информационной безопасности как для широкого круга сотрудников органов власти и предприятий, так и углубленные курсы для специалистов по информационной безопасности в различных предприятиях. К настоящему моменту обучение прошли в общей сложности более 50 000 человек.

Мы разработали новый обучающий курс, предназначенный специально для сотрудников органов власти и специалистов в сфере здравоохранения. В нем отражена специфика отрасли здравоохранения и рассматривается выполнение требований нормативных правовых актов в указанной отрасли.

Курс разделен на два вебинара по критерию потенциальной целевой аудитории:

1. Вебинар по основам информационной безопасности для сотрудников органов власти в сфере здравоохранения и медицинских учреждений, который включает ознакомление с основными обязательными к выполнению нормативными требованиями и проработку основных правил цифровой безопасности и ИБ-грамотности.

2. Углубленный вебинар для специалистов информационной безопасности органов власти в сфере здравоохранения и медицинских учреждений, материалы которого охватывают различные аспекты работы ИБ-специалистов. В курс включена информация о современных рисках информационной безопасности, новеллах правового регулирования защиты информации, практических принципах обеспечения защиты данных, а также советы по пользованию средствами ИБ и повышению эффективности противодействия кибератакам и киберинцидентам в государственных и муниципальных органах и учреждениях. В обучении делается упор на реальные примеры: использование ИБ-решений, мотивы злоумышленников и варианты деструктивных действий.

В связи с принадлежностью учреждений здравоохранения к субъектам критической информационной инфраструктуры, проведение курса возможно в рамках осуществления предписаний п. 13.7 Приказа ФСТЭК от 25.12.2017 № 239 и выполнения мер ИПО.1, ИПО.2, предусмотренных Приложением к вышеуказанному Приказу.

Курс проводится бесплатно и может проходить в двух форматах:

Однодневный формат проведения. Продолжительность – 4 часа (2 вебинара по 2 часа).

Двухдневный формат проведения. Продолжительность – 4 часа (2 вебинара по 2 часа).

Точное время проведения обсуждается индивидуально.

Содержание курса «Информационная безопасность: здравоохранение»:

Вебинар 1.

- Общий обзор киберугроз и их последствий в отрасли здравоохранения. Кибератаки на медицинские организации и их последствия: основные кейсы.
- Нормативное регулирование информационной безопасности в здравоохранении.
 - Нормативная база защиты информации в здравоохранении: ст. 4, ст. 13, ст. 91.1 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Приказ Минздрава РФ от 24.12.2018 № 911Н, Концепция информационной безопасности в сфере здравоохранения.
 - Новеллы правового регулирования информационной безопасности: Федеральный закон от 14.07.2022 № 266-ФЗ, Указы Президента № 166 и № 250.
 - Нормативные требования и потребности организаций здравоохранения.
- Защита персональных данных на практике учреждений здравоохранения.
 - Что относится к персональным данным?
 - Как разграничить доступ к персональным данным в МИС и на устройствах?
 - Как предупредить и пресечь утечки информации?
 - Как нивелировать «человеческий фактор»?
 - Разбор практических примеров.

Вебинар 2.

- Общий обзор киберугроз и нормативной базы информационной безопасности в здравоохранении.
 - Основные киберугрозы и последствия инцидентов информационной безопасности в здравоохранении.
 - Нормативная база защиты информации в здравоохранении: Федеральные законы: от 27.06.2006 № 152-ФЗ, от 26.07.2017 № 187-ФЗ, Приказ Минздрава РФ от 24.12.2018 № 911Н, Концепция информационной безопасности в сфере здравоохранения, требования ФСТЭК.
- Выполнение нормативных требований по защите информации при внедрении и использовании ПО для информационной безопасности.
- Технические средства защиты информации.
 - DСАР-система: задачи, функции, механика работы.
 - SIEM-система: подключение и контроль устройств, выявление инцидентов, составление отчетности.
 - DLP-система: стадии инцидента информационной безопасности, блокировки в DLP-системе, пользовательский интерфейс DLP-системы.
- Защита от «человеческого фактора».