бюджетное профессиональное
образовательное учреждение
Вологодской области
«Великоустюгский
многопрофильный колледж»

УТВЕРЖДЕНА
приказом директора
колледжа
от 24.05.2022 г. № 236

ПОЛИТИКА

«24» 05 2022 г. № 19

г. Великий Устюг

в области обучения и повышения осведомленности работников учреждения по вопросам информационной безопасности

Общие положения

Одним из основных факторов, которые существенно влияют на состояние информационной безопасности в учреждении, являются осведомленность пользователей в области информационной безопасности и их умение применять полученные знания в повседневной деятельности, поэтому одна из важнейших задач, которую приходится решать - организация обучения пользователей по вопросам обеспечения информационной безопасности.

Под повышением осведомленности работников учреждения в области информационной безопасности понимается целенаправленный, организованный, планомерно и систематически осуществляемый процесс повышения уровня знаний работников и формирования необходимых навыков в области информационной безопасности, создание культуры в данной области и осознания необходимости соблюдения требований информационной безопасности.

Цели и основные требования к повышению осведомленности

Периодичность обучения:

- по действующей в учреждении Политике информационной безопасности;
- по применяемым защитным мерам;
- по правильному использованию защитных мер в соответствии с внутренними документами;
- по значимости и важности деятельности работников для обеспечения информационной безопасности.

В общем случае к системе повышения осведомленности работников учреждения предъявляются следующие требования:

- возможность регулярного обучения любого количества работников, независимо от их территориального местонахождения и без отрыва от рабочего процесса;

- простота и доступность учебных материалов для различных категорий работников;

- возможность оперативного внесения изменений в программы повышения осведомленности и учебные материалы.

Важным аспектом работы по повышению осведомленности работников учреждения по вопросам информационной безопасности является непрерывность этого процесса. Законодательство и требования регуляторов быстро меняются, появляются новые угрозы информационной безопасности, новые информационные системы - все это необходимо оперативно отражать в программах повышения осведомленности. Для работников учреждения непрерывность обучения заключается в повторении требований и правил информационной безопасности. Также важно информировать всех работников о произошедших изменениях в Политике информационной безопасности учреждения и процедурах обеспечения информационной безопасности.

Конечной целью реализации вышеуказанных программ является снижение ущерба и потерь (материальных, моральных, репутационных) от угроз, связанных с человеческим фактором при работе с информационными ресурсами учреждения.

Как и всякая система обучения, система повышения осведомленности подразумевает использование определенных форм, видов и методов обучения. Выбор того или иного метода или формы зависит от целого ряда факторов, таких как: цели организации, кадровая политика, характеристики обучающегося персонала, его численность и финансирование.

Обучение

В рамках повышения осведомленности работников учреждения в области информационной безопасности обучение может проходить в следующих формах:

- очного обучения;

- дистанционного обучения;

- самостоятельного изучения учебных материалов.

Наибольший эффект дает комплексное применение различных форм и методов обучения в рамках многоуровневой системы повышения осведомленности работников учреждения в области информационной безопасности, с использованием:

- очного обучения в виде инструктажа по обеспечению информационной безопасности, а также специализированных курсов для отдельных категорий работников;

- дистанционного обучения, проводимого периодически, по нескольким программам различного уровня;

- разовых рассылок, доведения информации по изменениям в законодательстве РФ в области информационной безопасности, Политике информационной безопасности учреждения, по выявленным нарушениям и другим актуальным вопросам;

- самостоятельной работы с нормативными документами;

- консультаций и проведения совещаний по отдельным вопросам обеспечения информационной безопасности.

Систему повышения осведомленности работников учреждения, как один из процессов системы менеджмента информационной безопасности, целесообразно организовывать в виде циклической модели Деминга «... планирование - реализация - проверка - совершенствование - планирование...», которая является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001 и ИБ ISO/IEC IS 27001:2005.

Особенности этапов циклической модели Деминга

Этап «планирование»

На этом этапе осуществляется постановка целей обучения, закупка/разработка и ввод в эксплуатацию системы обучения, разработка учебных программ и необходимых учебных материалов, подготовка организационно-распорядительных документов по организации обучения. Наиболее сложной и самой ответственной задачей является разработка (или приобретение у специализированных компаний) учебных программ и учебных материалов, которые должны учитывать специфику деятельности учреждения и существующий уровень осведомленности работников учреждения по вопросам информационной безопасности. Для этого предварительно проводится анализ действующей в учреждении Политики информационной безопасности, используемых защитных мер, количества, видов и последствий инцидентов информационной безопасности с целью выявления проблемных областей и уровня осведомленности работников в области информационной безопасности.

Содержание учебных программ обычно типовое, раскрывающее основные положения Политики информационной безопасности, правил использования информационных ресурсов, но с обязательным учетом специфики учреждения, особенностей обработки информации и других нюансов.

Работникам необходимо четко понимать, что такое информационная безопасность и какие последствия могут быть для учреждения в случае несоблюдения ее требований. Для правильного формирования культуры информационной безопасности работники учреждения должны понимать, почему важно защищать информацию, какие виды конфиденциальной информации используются в колледже, какие существуют угрозы, и какие защитные меры необходимо использовать и каким образом.

Особое внимание необходимо акцентировать на рассмотрении понятия и основных видов инцидентов информационной безопасности, их признаках и доведения информации о том, что необходимо делать в случае выявления инцидента информационной безопасности и к кому обращаться в этом случае.

В разрабатываемых курсах до работников учреждения должны быть доведены требования законодательства РФ и локальных нормативных актов в области информационной безопасности.

Так как повышение осведомленности в области информационной безопасности для большинства работников не является профильным обучением,

средства и материалы, используемые в учебной программе и учебных материалах, должны быть простыми для восприятия, интересными и максимально понятными.

Этап «Реализация»

Здесь реализуется разработанная программа и осуществляется контроль усвоения знаний работниками учреждения.

Прежде чем использовать систему дистанционного обучения, производится инструктаж пользователей, обучение, как правильно ее использовать, установленным порядком выдаются учебные задания и производится контроль их выполнения.

Возможно выделение отдельных групп обучаемых в соответствии с выполняемым функционалом и уровнем осведомленности.

На данном этапе важнейшим элементом является контроль обучения работников: во-первых, необходимо иметь обратную связь, чтобы оценить эффективность проведения обучения, во-вторых, некоторые подходят к обучению несерьезно, либо совсем не проходя обучение либо не сдавая тесты. Таких работников надо выявлять и добиваться успешного прохождения ими курса обучения.

Для контроля могут использоваться различные формы: тестирование, опрос на знание Политики информационной безопасности учреждения.

Этап «Проверка»

Оценка эффективности реализации учебных программ, которая включает в себя оценку полученных работниками знаний и умений, оценку действенности проведенных мероприятий, а также анализ изменений статистики инцидентов информационной безопасности, проводится на этапе проверки.

Возможно применение следующих способов оценки эффективности реализации программы:

- сбор и анализ статистики инцидентов информационной безопасности в учреждении;
- открытые проверки (тесты, опросы, интервью, анкетирование, внешний или внутренний аудит);
- скрытые проверки (телефонные звонки и электронные письма провокационного характера с использованием приемов социальной инженерии, мониторинг действий пользователей, внешний или внутренний аудит).

Этап «Совершенствование»

На данном этапе производится коррекция и улучшение работы, переработка программ и учебных материалов, их обновление.

Обычно переработка учебных программ производится после существенного изменения требований законодательства, нормативных документов, требований информационной безопасности учреждения, правил обработки информации.

В учреждении должен быть определен перечень документов, являющихся свидетельством выполнения программ обучения и повышения осведомленности в области информационной безопасности.

В частности, такими документами могут являться:

- документы (журналы), подтверждающие прохождение работниками обучения в области информационной безопасности с указанием уровня образования, навыков, опыта и квалификации обучаемых;
- документы, содержащие результаты проверок обучения работников;
- документы, содержащие результаты проверок осведомленности в области информационной безопасности.

Заключительные положения

Повышение осведомленности работников учреждения - это один из важнейших этапов внедрения системы обеспечения информационной безопасности, который направлен на обучение работников учреждения и поддержание его знаний в актуальном состоянии.

Обучение работников учреждения по вопросам информационной безопасности - залог высокой эффективности всей системы безопасности в целом. Кроме того, большую часть инцидентов информационной безопасности можно не допустить, поскольку более половины всех инцидентов порождают работники учреждения просто по незнанию требований и правил информационной безопасности.

Рассмотрено
Советом Учреждения
Протокол № 22
«24» 05 2022 г.

В дело № 01-14
«24» 05 2022 г.