

УТВЕРЖДЕН

приказом № 327 от 04.06. 2024

Директор ГАПОУ СО «ТМК»

И.А.Мочалов

П 368-2024

**ПОРЯДОК ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ
ГОСУДАРСТВЕННОГО АВТОНОМНОГО ПРОФЕССИОНАЛЬНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ САМАРСКОЙ ОБЛАСТИ
«ТОЛЬЯТТИНСКИЙ МАШИНОСТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»
ОБ УГРОЗАХ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, О ПРАВИЛАХ
ЭКСПЛУАТАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ОТДЕЛЬНЫХ
СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ ИСПДн**

Тольятти, 2024 г.

ПЕРЕЧЕНЬ ТЕРМИНОВ

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность – свойство информации сохранять конфиденциальность, целостность и доступность.

Риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба.

Угроза информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящий «Порядок повышения осведомленности работников государственного автономного профессионального образовательного учреждения Самарской области «Тольяттинский машиностроительный колледж» (далее - Учреждение) об угрозах безопасности информации, о правилах эксплуатации системы защиты информации и отдельных средствах защиты информации ИСПДн» (далее – Порядок) является локальным нормативным актом Учреждения.

1.2 Целями настоящего процесса информирования и обучения в области обеспечения безопасности информации работников Учреждения, являющихся пользователями информационных систем персональных данных (далее – ИСПДн), в области информационной безопасности (далее – ИБ) является:

- снижение рисков ИБ, связанных с человеческим фактором и появлением новых угроз ИБ ИСПДн;
- обеспечение необходимого уровня компетентности работников в области ИБ.

1.3 Задачами процесса информирования и обучения персонала в области обеспечения безопасности информации являются:

- обеспечение соответствия ИСПДн требованиям российского законодательства, нормативным документам в сфере обеспечения ИБ, локальным нормативным актам Учреждения;
- минимизация прямого или косвенного негативного воздействия, направленного на нарушение конфиденциальности, целостности и доступности информации, обрабатываемой в ИСПДн;
- снижение вероятности появления инцидентов ИБ, связанных с несанкционированным доступом к ИСПДн.

1.4 Настоящий Порядок распространяется на следующих лиц:

- системные администраторы ИСПДн;
- пользователи ИСПДн;
- администратора безопасности информации.

2 ПОРЯДОК ИНФОРМИРОВАНИЯ И ОБУЧЕНИЯ ПЕРСОНАЛА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

2.1 Принципы информирования и обучения персонала в области обеспечения безопасности информации

2.1.1 Информирование и обучение персонала в области обеспечения безопасности информации проводится:

- для снижения рисков ИБ, связанных с человеческим фактором и появлением новых угроз ИБ ИСПДн;
- для обеспечения необходимого уровня компетентности и осведомленности в области ИБ.

2.1.2 Обучение персонала в области обеспечения безопасности информации ИСПДн делится на следующие типы:

- обязательное обучение (внутреннее) – проводится для всех работников;
- дополнительное обучение (внутреннее или внешнее) – расширяет обязательное обучение знаниями, необходимыми работникам для решения специфических задач.

2.1.3 Помимо обучения Учреждение проводит следующие мероприятия:

- вводный инструктаж по ИБ – проводится для всех принимаемых на работу работников Учреждения;
- информирование персонала в области обеспечения безопасности информации в случае необходимости. Информирование проводится с целью оперативного уведомления персонала об изменениях в процессах управления и обеспечения ИБ ИСПДн.

2.2 Вводный инструктаж по обеспечению безопасности информации

2.2.1 Вводный инструктаж по обеспечению безопасности информации для всех принимаемых на работу работников Учреждения, участвующих в эксплуатации ИСПДн, проводится кадровой службой путем ознакомления с соответствующими инструкциями и порядками обеспечения ИБ в ИСПДн (в части, их касающейся).

2.2.2 Вводный инструктаж необходимо проводить до предоставления работнику прав доступа к ИСПДн. По результатам инструктажа ответственным работником кадровой службы должна быть внесена отметка в Журнал учета прохождения вводного инструктажа (форма записи представлена в приложении (Приложение А) настоящего Порядка).

2.3 Внутреннее обучение персонала в области обеспечения безопасности информации

2.3.1 Администратор безопасности информации проводит мероприятия по обучению персонала в области обеспечения безопасности информации ИСПДн (обязательное обучение, дополнительное внутреннее обучение).

2.3.2 Кадровая служба осуществляет организацию проведения мероприятий по обучению персонала:

- оповещение работников по электронной почте о дате, времени и месте проведения мероприятий.

2.3.3 Администратор безопасности информации разрабатывает и поддерживает в актуальном состоянии годовую программу мероприятий по обязательному и дополнительному внутреннему обучению (Форма годовой программы обучения персонала в области обеспечения безопасности информации представлена в приложении (Приложение Б) настоящего Порядка), согласовывает ее с кадровой службой и передает на утверждение Руководству. Программа мероприятий пересматривается не реже одного раза в год.

2.3.4 Программа общего курса по обучению персонала в области обеспечения безопасности информации должна содержать в том числе:

- базовые сведения в области обеспечения ИБ;
- защита информации ограниченного доступа, обрабатываемой в ИСПДн.

2.3.5 Программы дополнительного обучения персонала в области обеспечения безопасности информации являются адресными программами для работников. Программа курса может содержать в том числе:

- обязанности пользователей ИСПДн в части ИБ;
- теория управления и обеспечения ИБ;

- защита информации ограниченного доступа.

2.3.6 Новые работники Учреждения в период прохождения испытательного срока обязаны пройти внеочередное обязательное обучение в области обеспечения безопасности информации.

2.3.7 Работники Учреждения, получившие оповещение о необходимости пройти обучение в области обеспечения безопасности информации, проходят назначенный им курс в установленные сроки.

2.3.8 При необходимости Администратор безопасности информации инициирует повторное обучение. Причиной прохождения повторного обучения являются в том числе:

- изменение курсов обязательного обучения;
- уровень усвоения курса обучения ниже необходимого;
- не прохождение работником обучения;
- внедрение новых или внесение существенных изменений в процессы управления безопасностью информации ИСПДн и ее обеспечения;
- заявка в свободной форме от непосредственного начальника структурного подразделения работника.

2.4 Внешнее обучение персонала в области обеспечения безопасности информации

2.4.1 Внешнее обучение персонала в области обеспечения безопасности информации проводится в случаях невозможности проведения внутреннего обучения в силу отсутствия соответствующих компетенций у работников Учреждения, отсутствия необходимой технической базы (оборудования и программного обеспечения) и других причин.

2.4.2 Причиной подачи заявки на внешнее обучение персонала в области обеспечения безопасности информации являются в том числе:

- результаты аудита по ИБ (внутреннего и внешнего);
- результаты анализа состояния ИБ со стороны руководства Учреждения;
- заявка в свободной форме от непосредственного начальника структурного подразделения работника.

2.4.3 Кадровая служба Учреждения осуществляет организацию проведения внешнего обучения персонала в области обеспечения безопасности информации:

- согласование проведения внешнего обучения при необходимости;
- поиск подрядчика, осуществляющего внешнее обучение;
- оповещение работников по электронной почте о дате, времени и месте

проведения обучения.

2.5 Информирование работников в области ИБ

2.5.1 Целью информирования персонала является оперативное уведомление работников об изменениях в состоянии ИБ, о возникновении новых угроз ИБ, а также повышение общего уровня осведомленности работников в области ИБ.

2.5.2 Информирование персонала в области обеспечения безопасности информации осуществляется следующими способами:

- рассылка информационных писем по электронной почте;
- рассылка инструкций по электронной почте.

2.5.3 Информирование персонала проводится в следующих случаях:

- при утверждении разработанных/актуализированных документов в области обеспечения или управления ИБ администратор безопасности информации оповещает всех работников Учреждения об утверждении разработанных/актуализированных документов посредством электронной почты с указанием места расположения документа в локальной компьютерной сети;

- при появлении новых угроз ИБ администратор безопасности информации информирует о новых угрозах работников по электронной почте и рассылает инструкции по реагированию на новые угрозы ИБ.

3 ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ ПЕРСОНАЛА

3.1 Работники, выполняющие обязанности и/или замещающие администратора безопасности информации, осуществляющие деятельность по администрированию и контролю средств защиты информации, должны иметь высшее профессиональное образование в области технической защиты информации либо высшее техническое или среднее профессиональное (техническое) образование и сертификат о профессиональной переподготовке или повышении квалификации по вопросам технической защиты информации.

4 АКТУАЛИЗАЦИЯ

4.1 Периодическая проверка актуальности настоящего Порядка должна проводиться с интервалом не реже одного раза в год.

4.2 Решение об изменении настоящего Порядка принимает директор Учреждения на основании результатов применения настоящего Порядка, а также рекомендаций внутренних или внешних проверок.

5 КОНТРОЛЬ ИСПОЛНЕНИЯ ПОРЯДКА

5.1 Контроль исполнения Порядка возлагается на Администратора безопасности информации.

5.2 Лица, перечисленные в разделе 1 настоящего Порядка, несут ответственность за неисполнение и ненадлежащее исполнение обязанностей по информированию и обучению персонала в области обеспечения безопасности информации, предусмотренных настоящим Порядком, в соответствии с действующим законодательством Российской Федерации.

РАЗРАБОТАНО:

Ведущий специалист по кадрам



Т.О.Медяшкина

СОГЛАСОВАНО:

Заместитель директора по

учебно-производственной работе



С.А.Крюков

Юрисконсульт



Э.Н.Зайкова

Приложение А

(Форма) Журнал учета прохождения вводного инструктажа

№ п/п	ФИО инструктируемого работника	Структурное подразделение	Дата проведения вводного инструктажа	Отметка о прохождении (подпись)	ФИО проводшего вводный инструктаж	Отметка о проведении (подпись)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

Приложение Б

Форма Программы обучения персонала в области обеспечения безопасности информации

Программа годового обучения персонала в области обеспечения безопасности информации на 202_ год

№ п/п	Информация о курсе
1. Обязательное обучение	
1.N	Наименование курса:
	Дата проведения курса:
	Время начала курса:
	Продолжительность курса:
	Тренер курса:
	Цель курса:
	Целевая аудитория курса:
	Содержание курса: – Раздел курса – Раздел курса –
2. Дополнительное внутреннее обучение	
2.N	Наименование курса:
	Дата проведения курса:
	Время начала курса:
	Продолжительность курса:
	Тренер курса:
	Цель курса:
	Целевая аудитория курса:
	Содержание курса: – Раздел курса – Раздел курса –

Администратор безопасности информации»: _____

(подпись) (ФИО)

Приложение В
(Форма) Журнал результатов прохождения работниками обучения
в области обеспечения безопасности информации

№ п/п	ФИО работника	Структурное подразделение	Наименование курса	Дата начала обучения	Дата последнего посещения	Дата планируемого завершения	Уровень усвоения пройденного курса обучения (%)
1.							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							