Технический университет

УТВЕРЖДАЮ
Директор
Технического университета
_____ В.А. Лапин
(подпись)
«09» ноября 2023 г.

ПРОГРАММА

дополнительная общеобразовательная общеразвивающая

«Кибербезопасность бизнеса»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01A9B270009FB0CDA24F536A9900FD88B1
Владелец: ЛАПИН ВЯЧЕСЛАВ АЛЕКСАНДРОВИЧ
Действителен: с 18.10.2023 до 18.01.2025

г. Верхняя Пышма
2023 г.

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы

Получение новых компетенций, необходимых для профессиональной деятельности в области защиты информации, способность предотвращения утечки информации ограниченного доступа по техническим каналам в результате несанкционированного доступа к информации и специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

1.2. Планируемые результаты обучения

Слушатель должен знать:

- последствия утечки информации ограниченного доступа по техническим каналам в результате несанкционированного доступа к информации и специальных воздействий на информацию;
- методы мошенничества;
- алгоритм действий при утечке информации ограниченного доступа;
- виды кибератак;
- методы защиты информации;
- инструменты для обнаружения и предотвращения атак;
- законодательную базу РФ в области кибербезопасности.

Слушатель должен уметь:

- обнаруживать утечку информации;
- использовать инструменты и методы защиты информации в целях защиты информации ограниченного доступа;
- хранить информацию ограниченного доступа, не подвергая ее опасности;
- соблюдать законодательство в области кибербезопасности и обеспечивать соответствие требованиям регуляторов.

1.3. Требования к уровню подготовки слушателя

Слушатели, имеющие высшее или среднее профессиональное образование

1.4. Программа разработана с учетом:

профессионального стандарта «Специалист по технической защите информации», утвержденный приказом Министерства труда и социальной защиты РФ №474н от 09.08.2022

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

Наименование раздела		Трудоемкость, час	Всего, ауд. час.	в том числе, час.		
				лекции	лабораторные работы	прак. занятия, семинары
1		2	3	4	5	6
1.	*Обзор рисков и угроз для бизнеса в интернете*	2	2	0	0	2
2.	*Обсуждение законодательства в области кибербезопасности и его роли в защите данных компаний*	2	2	0	0	2
3.	*Разбор методов защиты информации и противодействия хакерам*	3	3	0	0	3
4.	Кейс-стади	4	4	0	0	4
5.	*Роль обучения в обеспечении безопасности информации*	4	4	0	0	4
Итого		**16**	**16**	**0**	**0**	**16**

2.2. Учебно-тематический план

№ п/п	Наименование раздела и тем	Трудоемкость, час	Всего, ауд. час.	в том числе, час.		
				лекции	лабораторные работы	прак. занятия, семинары
1	2	3	4	5	6	7
1	Обзор рисков и угроз для бизнеса в интернете	2	2	0	0	2
2	Обсуждение законодательства в области кибербезопасности и его роли в защите данных компаний	2	2	0	0	2
3	Разбор методов защиты информации и противодействия хакерам	3	3	0	0	3
4	Кейс-стади	4	4	0	0	4
5	Роль обучения в обеспечении безопасности информации	4	4	0	0	4
Итого		**16**	**16**	**0**	**0**	**16**

2.3. Примерный календарный учебный график

Период обучения (дни, недели)[1)]	Наименование раздела

Первый день	Обзор рисков и угроз для бизнеса в интернете Обсуждение законодательства в области кибербезопасности и его роли в защите данных компаний Разбор методов защиты информации и противодействия хакерам
Второй день	Практическая работа Роль обучения в обеспечении безопасности информации

_____

[1)] Даты обучения будут определены в расписании занятий при наборе группы на обучение

2.4. Рабочие программы разделов

№, наименование темы	Содержание лекций (количество часов)	Наименование лабораторных работ (количество часов)	Наименование практических занятий или семинаров (количество часов)	Виды СРС (количество часов)
1	2	3	4	5
Раздел I. Обзор рисков и угроз для бизнеса в интернете				
1.	-	-	Обзор рисков и угроз для бизнеса в интернете (2)	-
Раздел II. Обсуждение законодательства в области кибербезопасности и его роли в защите данных компаний				
1	-	-	Обсуждение законодательства в области кибербезопасности и его роли в защите данных компаний (2)	_
Раздел III. Разбор методов защиты информации и противодействия хакерам				
1	-	-	Разбор методов защиты информации и противодействия хакерам (3)	_
Раздел IV. Кейс-стади				
1	-	-	Кейс-стади (4)	-
Раздел V. Роль обучения в обеспечении безопасности информации				
1	-	-	Роль обучения в обеспечении безопасности информации (4)	-

2.5. Оценка качества освоения программы (формы аттестации, оценочные и методические материалы)

2.5.1. Форма(ы) промежуточной и итоговой аттестации

Промежуточная аттестация не проводится. Итоговая аттестация не проводится.

3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Материально-технические условия

Наименование специализированных учебных помещений	Вид занятий	Наименование оборудования, программного обеспечения
Аудитории ТУ УГМК и Заказчика	Практические занятия	Мультимедийное оборудование, компьютеры. Компьютер, подключенный к сети Интернет, интернет-браузер.

3.2. Учебно-методическое и информационное обеспечение*:*

1. Джафарли, В. Ф. Криминология кибербезопасности : монография / В. Ф. Джафарли ; под редакцией С. Я. Лебедева. — Москва : Проспект, 2022 — Том 5 : Криминологическая кибербезопасность: перспективы развития — 2022. — 272 с. — ISBN 978-5-392-36256-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/280301

2. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131717

3. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148383

3.3. Кадровые условия

Кадровое обеспечение программы осуществляют преподаватели-практики, имеющие опыт в области кибербезопасности бизнеса.