АНО ”СТУДЕНЧЕСКОЕ НАУЧНОЕ ОБЩЕСТВО”

ИНН 7814762360, КПП 781401001

197350, город Санкт-Петербург, проспект Королёва, дом 42 корпус 3 литер а, квартира 41

admin@snospb.ru

УТВЕРЖДЕНО

Приказом №___ от «__»_____ 2023 г.

Генеральный секретарь

АНО «Студенческое научное общество»

_____ Пуляк А.В.

РАБОЧАЯ ПРОГРАММА ДОПОЛНИТЕЛЬНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО КУРСА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Цифровая безопасность

Уровень образования: дополнительное профессиональное

Срок реализации: 0,5 года

Количество часов: 36 часов

Разработчик: Пуляк В.Д.

руководитель образовательного отдела, п.д.о.

Санкт-Петербург, 2023

Рабочая программа дополнительного профессионального образования составлена на основе требований к обеспечению информационной безопасности, изложенной в Федеральном законе "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ и постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Пояснительная записка

Дополнительная общеобразовательная программа повышения квалификации «Цифровая безопасность» (далее - Программа) разработана в рамках работы автономной некоммерческой организации «Студенческое научное общество». Данная программа направлена на повышение уровня знаний в сфере цифровой безопасности и защите информации участников, чья профессиональная деятельность связана с управлением рисками информационной безопасности, стратегиями защиты данных и управлением безопасностью информационных систем. Программа составлена с целью развития у участников навыков и знаний в области безопасного обращения с информацией и повышения профессиональной эффективности в современных условиях и с учетом Федерального Закона Российской Федерации от 29.12.2012 г. № 273 «Об образовании в Российской Федерации»; постановления Правительства РФ от 28 октября 2013 г. № 966 «О лицензировании образовательной деятельности», приказа Министерства просвещения от 09.11.2018 N 196 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»; письма Минобрнауки России от 18.11.2015 №09-3242 «О направлении информации» (вместе с «Методическими рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)»; распоряжения Комитета по образованию Санкт-Петербурга «Об утверждении Методических рекомендаций по проектированию дополнительных общеразвивающих программ в государственных образовательных организациях Санкт-Петербурга, находящихся в ведении Комитета по образованию» от 01.03.2017 №617-р.

Направленность программы: техническая

Актуальность

С каждым годом вопросы обеспечения цифровой безопасности становятся все более актуальными, поскольку увеличивается количество личной информации, размещенной в цифровой среде. Так, например, согласно отчёту, представленному главой Минцифры Максутом Шадаевым, количество

зарегистрированных пользователей на едином портале государственных и муниципальных услуг «Госуслуги» увеличилось на 15,2 миллиона.

Вместе с ростом числа пользователей, использующих цифровые ресурсы для хранения личной информации, увеличивается и количество правонарушений, связанных с нарушением конфиденциальности в цифровом пространстве. Кибератаки становятся все более распространенными и причиняющими больше вреда.

Обучение цифровой безопасности позволяет разобраться в защите персональных данных от несанкционированного доступах, методах и способах отражения кибератак. Поскольку в вопросах цифровых технологий происходит постоянное усложнение, то требуется постоянное обновление знаний и навыков для эффективной работы.

Отличительные особенности

Комплексный подход к освоению программы, с применением различных методов подачи материала и контроля отработки полученных знаний позволяет погрузиться в тему и более полно усвоить представляемую информацию. Лекции, работа со скриптами и интеллект-картами, выполнение самостоятельных заданий даёт возможность структурировать и наиболее полно разобраться в теме цифровой безопасности.

Адресат программы: специалисты, профессиональная деятельность которых связана с использованием цифровых технологий в своей работе: сотрудники административного персонала, менеджеры, специалисты по маркетингу, финансам, продажам и другим областям, которым требуется основная компьютерная грамотность для эффективного выполнения своих задач

Объем и срок реализации программы: программа рассчитана на 0,5 года (36 часов)

Цель программы:

Повысить уровень осведомлённости обучающихся о различных угрозах и рисках, с которыми они могут столкнуться в цифровой среде, развить навыки безопасного обращения с персональными данными и расширить представления о способах борьбы с кибератаками. В процессе изучения курса сформировать базовые знания об основных принципах, угрозах и методах защиты в цифровой среде.

Задачи образовательной программы:

Обучающие:

- Сформировать представления о необходимости компьютерных технологий, важности обеспечения эффективного применения современных цифровых возможностей.
- Понять основные принципы и концепции цифровой безопасности, а также угрозы и риски, связанные с использованием компьютерных технологий.
- Овладеть базовыми навыками и методами защиты в цифровой среде, включая безопасное использование паролей, защиту личных данных и информации, обнаружение и предотвращение кибератак.

Развивающие:

- Развивать у обучающихся критическое мышление и аналитические способности в процессе оценки цифровых угроз и рисков
-

Воспитательные:

- Сформировать осознанное отношение к цифровой безопасности и важности защиты персональных данных.
- Развивать этическое поведение и уважение к правам и нормам в цифровом пространстве.

Условия реализации программы

Принцип набора обучающихся:

В группы для обучения принимаются совершеннолетние обучающие, являющиеся участниками трудовых отношений и проявляющие интерес к теме курса. В зависимости от индивидуальных возможностей, знаний, умений и творческих способностей, обучающемуся могут быть предложены другие уровни и форматы обучения.

Возраст обучающихся: 18-60+ лет

Количество обучающихся: наполняемость группы не менее 5 человек

Режим занятий: продолжительность обучения – 36 часов, из них 20 часов – занятия в формате видеоконференции, 16 часов – самостоятельная работа (изучение конспекта и выполнение домашних заданий), с постоянной обратной связью от педагога в режиме онлайн, консультированием онлайн для качественного выполнения домашнего задания.

Занятия проходят в формате видеоконференций на платформе ZOOM и Discord – 2 раза в неделю по 1 часу.

Основные формы и методы программы

Обучение по программе включает в себя:

Онлайн занятия в формате видеоконференции на платформе ZOOM и Discord:

- лекции
- групповые дискуссии;
- групповую рефлексию в кругу;
- тренажеры
- мэйндмэпинг

Материально-техническое оснащение программы

Для проведения занятий по программе необходимо обеспечение возможности дистанционного подключения педагога к телекоммуникационной сети Интернет и наличие специальных материалов. Для этого помещение должно быть оснащено: стол – 1 шт, стул – 1 шт, ноутбук – 1 шт, модем – 1 шт, графический планшет – 1 шт.

Методы и приемы реализации программы

• Программа составлена из практических и теоретических занятий.

• Учащимся предоставляется теоретический материал для самостоятельного изучения (на странице курса в сети Интернет https://snospb.ru/),

• После изучения конспекта по каждой теме проходит встреча группы в формате видеоконференции на платформе ZOOM (https://zoom.us/). В ходе этой конференции педагоги подробнее останавливаются на важных аспектах теории, и проводят практические занятия.

• После занятия учащимся предоставляется доступ к домашнему заданию, которое необходимо выполнить и предоставить педагогам для проверки. Ссылка на практическое задание представлена на странице курса (https://snospb.ru/). Практически задания выполняются и хранятся в Облачном хранилище https://dropbox.com и https://drive.google.com/

• Поддержка Учащихся происходит в кросс-платформенном мессенджере https://telegram.org/

• Предоставляемые Учащимся дополнительные методические материалы, выложены на https://drive.google.com

Дидактические материалы:

Бондарев В.В. Введение в информационную безопасность автоматизированных систем (2-е издание). – М.: МГТУ им. Н.Э. Баумана. 2018. – 252с. 2)

Организационно-правовое обеспечение информационной безопасности. под редакцией А.А. Александрова, М.П. Сычева – М.: МГТУ им. Н.Э. Баумана. 2018. – 292с. 3)

Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры. – М.: Горячая линия – телеком, 2018. – 314с

Астахов А. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с.

Bayuk J., CyberForensics: Understanding Information Security Investigations, Humana Press, 2010, - 200 с. 3)

Bidgoli H., Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management Book, Wiley, - 1152 с.

Lance Hayden, IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, McGraw-Hill Osborne Media, 2010, - 396 с.

Список приложений и онлайн-инструментов:

1. ZOOM – сервис видеотелефонии, который позволяет подключать одновременно до 100 устройств (https://zoom.us)
2. Discord – бесплатный мессенджер с поддержкой айпи́-телефонии (IP-телефония, VoIP) и видеоконференций, предназначенный для использования различными сообществами по интересам (https://discord.com)
3. Google Class – бесплатный веб-сервис, разработанный Google для школ, который призван упростить создание, распространение и оценку заданий безбумажным способом (classroom.google.com)

Формы подведения итогов реализации программы

Контроль за исполнением программы осуществляется через анализ эффективности образовательной деятельности и систему мониторинга достижений учащихся.

В рамках работы по программе, педагог проводит оценку:

- процента заполнения обучающимся скриптов

-выполнения заданий: письменных и устных.

Педагог осуществляет проверку контрольных работ, тестов и выставляет оценки зачтено/не зачтено:

- Оценка «зачтено» – более 75% выполненных заданий.
- Оценка «не зачтено» – до 75% выполненных заданий.
-

Содержание программы

1. Сущность, задачи и проблемы информационной безопасности

Определение информационной безопасности и ее роль в современном обществе. Значение конфиденциальности, целостности и доступности информации. Основные угрозы и риски для информационной безопасности.

2. Методы нарушения конфиденциальности, целостности и доступности информации

Методы перехвата информации. Взлом учетных записей и паролей. Вирусы, троянские программы и другие виды вредоносного программного обеспечения. Методы препятствия передачи или получения информации.

3. Причины, виды, каналы утечки и искажения информации

Внешние атаки и взломы системы для получения доступа к информации. Утечка конфиденциальной информации через незащищенные каналы связи. Уничтожение или блокирование доступа к информации.

4. Защита персональных данных

Важность и методы защиты персональных данных. Процессы и инструменты шифрования данных. Безопасное хранения и обработка персональных данных, включая установку паролей, многофакторную аутентификацию и контроль доступа. Ознакомление с законодательством и нормативными актами, регулирующими защиту персональных данных.

5. Безопасность в сети Интернет

Изучение основных правил безопасного поведения в онлайн-среде, таких как проверка подлинности веб-сайтов, осмотрительное обращение с электронной почтой и файлами, идентификация подозрительных ссылок и вложений.

6. Организационно-правовое обеспечение защиты информации

Основные законодательные акты и нормативные документы, регулирующие защиту информации, включая законы, постановления и стандарты. Требования и обязательства, возлагаемые на организации в области защиты информации

Тематическое планирование

№	Название темы	Кол-во часов
1	Сущность, задачи и проблемы информационной безопасности	4
2	Методы нарушения конфиденциальности, целостности и доступности информации	6
3	Причины, виды, каналы утечки и искажения информации	10
4	Защита персональных данных	8
5	Безопасность в сети Интернет	6
6	Организационно-правовое обеспечение защиты информации	2

Календарный учебный график

Год обучения	Дата начала обучения по программе	Дата окончания обучения по программе	Количество учебных недель	Количество учебных часов	Режим занятий
2023/2024 учебный год	01.09.2023	По мере реализации программы	23	36	2 раза в неделю по 1 часу

Календарно-тематический план

№ п/п		Тема урока	Планируемая дата	Дата проведения
Тема 1. Сущность, задачи и проблемы информационной безопасности 4 часа				
1.	1.	Определение и роль информационной безопасности. Ключевые компоненты.		
2.	2.	Задачи и основные принципы информационной безопасности		
3.	3.	Современные угрозы и вызовы в области информационной безопасности		
4.	4.	Тренды в развитие информационной безопасности		
Тема 2. Методы нарушения конфиденциальности, целостности и доступности информации 6 часов				
5.	1.	Определение и принципы работы вирусов, червей и троянских программ		
6.	2.	Методы распространения и механизмы воздействия на информационные системы		
7.	3.	Основные принципы фишинга и его влияние на конфиденциальность информации		
8.	4.	Понятие и принципы работы ДДоС-атак		
9.	5.	Угрозы, связанные с использованием социальных сетей.		
10.	6.	Основные виды сетевых атак		
Тема 3. Причины, виды, каналы утечки и искажения информации 10 часов				
11.	1.	Методы обнаружения и предотвращения внутренних угроз		
12.	2.	Понятие социальной инженерии и ее влияние на безопасность информации.		
13.	3.	Защита информации от физического доступа и повреждений.		
14.	4.	Каналы утечки информации в сетевых средах		

15.	5.	Проверка на уязвимости и аудит безопасности сети		
16.	6.	Методы обнаружения и предотвращения технических утечек информации		
17.	7.	Виды искажения информации		
18.	8.	Методы проверки подлинности информации и предотвращения искажений		
19.	9.	Роль человеческого фактора в утечках и искажениях информации		
20.	10.	Ответственность за утечку и искажение информации		
Тема 4. Защита персональных данных 8 часов				
21.	1..	Определение персональных данных и их основные характеристики		
22.	2.	Категории персональных данных и их особенности		
23.	3.	Прозрачность и легитимность обработки персональных данных		
24.	4.	Ограничение целей обработки и минимизация данных		
25.	5.	Обеспечение конфиденциальности и безопасности персональных данных		
26.	6.	Использование средств шифрования и обезличивания данных		
27.	7.	Защита персональных данных при их передаче и хранении		
28.	8.	Особенности обработки персональных данных, относящихся к особым категориям		
Тема 5. Безопасность в сети Интернет 6 часов				
29.	1.	Основные угрозы и риски в сети Интернет		
30.	2.	Защита паролей, использование сильных паролей и двухфакторной аутентификации		
31.	3.	Определение и управление приватностью в онлайн-сервисах и социальных сетях		
32.	4.	Защита персональных данных при онлайн-транзакциях и платежах		
33.	5.	Основы безопасного использования мессенджеров и видеочатов		
34.	6.	Опасности и угрозы, связанные с публичностью профилей и публикацией личной информации		
Тема 6. Организационно-правовое обеспечение защиты информации 2 часа				
35.	1.	Законодательство и нормативные акты, регулирующие защиту информации		
36.	2.	Органы и структуры, отвечающие за обеспечение информационной безопасности		

Планируемые результаты

Обучающие:

- Сформированное понимание основных принципов и понятий цифровой безопасности.
- Усвоение основных технических и методологических средств обеспечения цифровой безопасности.
- Умение определять уязвимости и риски в информационных системах и сетях.
- Навыки использования средств защиты информации и проведения анализа рисков.
- Знание и понимание основных политик и процедур безопасности информации.

Развивающие:

- Развитие критического мышления и умения принимать обоснованные решения в области цифровой безопасности.
- Развитие интеллектуальных и творческих способностей в процессе выполнения заданий и работы с различными источниками информации.

Воспитательные:

- Развитие ответственности и осознанного использования информационных ресурсов в соответствии с принципами безопасности

В результате освоения программы обучающиеся должны

знать/понимать: основные принципы и концепции цифровой безопасности, типы угроз и риски, связанные с использованием информационных технологий, нормативные и правовые акты, регулирующие область цифровой безопасности, основные методы защиты информации и противодействия киберпреступности, принципы и методы анализа уязвимостей информационных систем и сетей, правила и процедуры безопасного поведения в сети Интернет

уметь: оценивать уровень безопасности информационных систем и сетей, проектировать и реализовывать меры по обеспечению безопасности информации, применять технические средства и методы для обнаружения и предотвращения инцидентов безопасности

владеть*:* навыками использования специализированного программного обеспечения для обеспечения цифровой безопасности, техническими навыками по настройке и администрированию систем безопасности

Критерии оценивания

Виды контроля: предварительный (входной), текущий, промежуточный, итоговый.

На основании предварительного (входного) контроля (собеседования) педагог получает представление об исходном уровне знаний и умений учащихся.

Текущий контроль фиксируется в «Журнале учета работы педагога дополнительного образования». Предполагается, что, присутствуя на занятиях, учащийся задействован в процессе раскрытия и развития собственного творческого потенциала, получает новые углубленные знания, умения и навыки по предмету.

Промежуточный контроль предусмотрен 2 раза в полгода для выявления уровня освоения программы учащимися и возможной корректировки процесса обучения. Итоговый контроль проводится для определения итогового уровня освоения программы обучающимися, включая учет их творческих достижений.

При осуществлении промежуточного и итогового контроля заполняется «Диагностическая карта оценки результатов обучающегося по дополнительной образовательной программе».

Промежуточный и итоговый контроль (аттестация) осуществляются педагогом в отношении каждого обучающегося, результаты фиксируются в «Диагностической карте оценки результатов обучающегося по дополнительной образовательной программе», количество таких карт соответствует количеству обучающихся в группе.

«Диагностическая карта оценки результатов освоения дополнительной образовательной программы, сводная по группе обучающихся» отражает результативность группы, для каждой группы такая карта заполняется в единственном количестве.

Уровни освоения программы учащимися:
I (начальный) — от 1 до 10 баллов; II (средний) — от 11 до 20 баллов; III (высокий) — от 21 до 30 баллов.