

**Индивидуальный предприниматель Титовский Александр Валерьевич  
Онлайн-школа дополнительного образования деловых навыков «Вада»**

УТВЕРЖДЕНА:  
Приказом № 3 от 18.07.2023г.

**ДОПОЛНИТЕЛЬНАЯ  
ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА  
(краткосрочная)  
технической направленности  
«ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА»**

Возраст учащихся: взрослое население  
Срок реализации: 4 ак. часа  
1 день обучения

Автор программы:  
Титовский Александр Валерьевич

г. Нарьян-Мар, 2023г.

## **СОДЕРЖАНИЕ**

1. Пояснительная записка	3
2. Категории обучающихся	3
3. Планируемые результаты	3
4. Объем программы	4
5. Учебный план	4
6. Календарный учебный график	4
7. Рабочие программы	5
8. Условия реализации образовательной программы	6
9. Кадровое обеспечение образовательного процесса	7
10. Оценка качества освоения образовательной программы	8
11. Информационно-методическое обеспечение реализации программы	8
12. Образец тестового задания для итоговой аттестации	8

## **Дополнительная общеобразовательная (общеразвивающая) программа «ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА»**

### **1. Пояснительная записка.**

#### **1.1.** По направленности – техническая.

По уровню содержания – ознакомительная.

По срокам реализации – краткосрочная.

**1.2. Форма обучения:** заочная, образовательная программа реализуется с применением исключительно электронного обучения, дистанционных образовательных технологий.

Целью изучения программы является формирование общих представлений о безопасности в информационном пространстве, формирование на основе полученных знаний понимания технологий информационной безопасности и умения применять правила защиты данных и кибербезопасности во всех сферах деятельности.

#### **1.3. Язык обучения:** русский.

**1.4. Документ об обучении:** сертификат о прохождении дополнительной общеобразовательной (общеразвивающей) программы «Защита информации от несанкционированного доступа».

**1.5. Срок обучения:** 4 ак. часа, 1 день.

**1.6. Объем программы:** 4 часа трудоёмкости, в том числе 4 ак. часа.

**1.7. Категории обучающихся:** взрослое население, без требований к образованию.

### **2. Цель и задачи программы.**

**2.1.** Целью изучения программы является понимание общих принципы организации защиты информации от несанкционированного доступа, обучение навыкам защиты информации и организации безопасного пространства для хранения информации.

**2.2.** К задачам программы относятся:

- Формирование общих представлений о безопасности в информационном пространстве;
- Изучение общих принципов, технологий, применяемых в информационной безопасности;
- Изучение способов защиты информации, необходимых мероприятий и действий для недопущения несанкционированного доступа;
- Развитие навыков защиты информации и данных, применение полученных навыков во всех сферах деятельности.

### **3. Планируемые результаты обучения.**

По результат обучения Обучающийся должен знать:

- Основные понятия информационной безопасности;
- Понятие и виды угроз информационной безопасности и способов несанкционированного доступа;
- Методы защиты от несанкционированного доступа;
- Законодательное регулирование безопасности данных и ответственность за нарушения в сфере защиты информации;
- Возможные меры защиты данных и их применение.

По результат обучения Обучающийся должен уметь:

- Ориентироваться в информационном поле;
- Выявлять элементы информационного пространства, представляющие угрозу защите данных;
- Ставить цели, формулировать задачи, связанные с обеспечением защиты данных от несанкционированного доступа;

- Применять знания о защите данных в решении возникающих задач в различных сферах деятельности;
- Применять методы проведения анализа в области обеспечения безопасности и защиты данных в информационном пространстве.

#### 4. Учебный план.

Образовательная программа состоит из текстовых материалов для самостоятельного изучения, видеоуроков, тестового задания итоговой аттестации.

Режим занятий определяется договором об образовании: групповые занятия или предоставление индивидуального доступа обучающегося к программе курса.

№ п/п	Название модуля	Количество часов			Форма аттестации/контроля
		Всего	Теория	Практика	
1.	Защита информации от несанкционированного доступа.	3	3	-	Текущий контроль
2.	Итоговая аттестация. Самостоятельная работа.	1	1	-	Тестовое задание.
	Итого	4	4	-	

#### 5. Календарный учебный график.

№ п/п	Наименование модуля	Количество ак. часов	Период обучения
1.	Защита информации от несанкционированного доступа.	3	Первый день обучения
2.	Итоговая аттестация. Тестовое задание. Самостоятельная работа.	1	
	Итого:	4	Один день обучения

Для освоения дополнительной общеобразовательной (общеразвивающей) программы обучающиеся принимаются в течение всего календарного года.

В случае предоставления индивидуального доступа обучающегося к программе курса график освоения программы определяется обучающимся самостоятельно, но в сроки, определенные договором об образовании.

#### 6. Рабочие программы. Защита данных от несанкционированного доступа.

##### Тема 1. Введение в тему защиты информации от несанкционированного доступа.

##### 1.1. Понятие информационной безопасности.

Понятие информационной безопасности. Цели информационной безопасности. Принципы информационной безопасности. Объекты защиты информационной безопасности. Основные виды конфиденциальной безопасности.

## **Тема 2. Угрозы информационной безопасности. Способы несанкционированного доступа посторонних к сведениям.**

Понятие угрозы информационной безопасности. Виды угроз информационной безопасности.

## **Тема 3. Способы несанкционированного доступа посторонних к сведениям.**

Перечень возможных способов несанкционированного доступа. Возможные способы использования полученных данных.

## **Тема 4. Служба информационной безопасности.**

Основные цели работы СИБ. Функции СИБ, Состав СИБ. Политика информационной безопасности.

## **Тема 5. Методы защиты от несанкционированного доступа.**

Виды защиты информации. Законодательные меры защиты информации. Нормативно-правовое обеспечение информационной безопасности и защиты информации в РФ. Ответственность за правонарушения в сфере защиты информации. Административно-организационные меры защиты информации. Программно-технические меры защиты информации. Антивирусное обеспечение.

## **Тема 6. Заключение.**

## **7. Условия реализации образовательной программы.**

Дополнительная общеобразовательная (общеразвивающая) программа реализуется исключительно с применением дистанционных образовательных технологий и электронного обучения. Образовательный курс размещен на образовательной платформе <https://in.wada.su/>. Вход на платформу осуществляется обучающимся посредством авторизации путем введения логина и пароля для доступа в личный кабинет на платформе.

Под электронным обучением понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательной программы информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников.

Под дистанционными образовательными технологиями понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Для реализации образовательной программы с применением исключительно электронного обучения, дистанционных образовательных технологий в организации созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся.

Для эффективного внедрения дистанционных образовательных технологий и использования электронных образовательных ресурсов имеется качественный доступ педагогических работников и обучающихся к информационно-телекоммуникационной сети Интернет (далее - сеть Интернет) с использованием установленных программно-технических средств для обучающихся и педагогических работников на скорости не ниже 512 Кбит/с; обеспечен порт доступа в сеть Интернет со скоростью не ниже 10 Мбит/с и возможностью установления не менее 20 одновременных сессий по 512 Кбит/с. Услуга подключения к сети Интернет предоставляется в режиме 24 часа в сутки 7 дней в неделю без учета объемов потребляемого трафика.

Для использования дистанционных образовательных технологий каждому обучающемуся и педагогическому работнику предоставляется свободный доступ к средствам информационных и коммуникационных технологий. Рабочее место педагогического работника и обучающегося оборудовано персональным компьютером и компьютерной периферией (аудиоколонками и(или) наушниками). Также

используются принтер, сканер (или многофункциональное устройство). В состав программно-аппаратных комплексов включено (установлено) программное обеспечение, необходимое для осуществления учебного процесса общего назначения (операционная система (операционные системы), офисные приложения, средства обеспечения информационной безопасности, архиваторы, графический, видео- и аудио-редакторы).

Формирование информационной среды осуществляется с помощью программной системы дистанционного обучения:

- разработчики образовательных программ: авторы и программист совместно разрабатывают и размещают содержательный контент;
- педагогический работник планирует свою педагогическую деятельность: выбирает из имеющихся или создает нужные для обучающихся ресурсы и задания;
- онлайн-школа, педагогические работники, обучающиеся обеспечиваются доступом к полной и достоверной информации о ходе учебного процесса, результатах обучения благодаря автоматическому фиксированию указанных позиций в информационной среде;
- обучающиеся выполняют задания, предусмотренные образовательной программой, при необходимости имеют возможность обратиться к педагогическим работникам за помощью;
- все результаты обучения сохраняются в информационной среде, на их основании формируются портфолио обучающихся.

## **8. Кадровое обеспечение образовательного процесса.**

Реализация дополнительной общеобразовательной (общеразвивающей) программы обеспечивается педагогическими работниками онлайн-школы, а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора.

Квалификация руководящих и педагогических работников должна соответствовать квалификационным характеристикам, установленным в Едином квалификационном справочнике должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей работников образования», утвержденном приказом Минздравсоцразвития России от 26.08.2010 N 761н и профессиональным стандартам (при наличии). Уровень компетентности педагогических работников онлайн-школы, реализующей образовательные программы с применением электронного обучения, дистанционных образовательных технологий, в вопросах использования новых информационно-коммуникационных технологий соответствует требованиям Методических рекомендаций по реализации дополнительных общеобразовательных программ с использованием электронного обучения, дистанционных образовательных технологий (Письмо Минпросвещения России от 31.01.2022 N ДГ-245/06 «О направлении методических рекомендаций»).

## **9. Оценка качества освоения образовательной программы.**

Текущий контроль осуществляется для обеспечения оперативной связи между обучающимся и преподавателем, а также контроля качества, информативности образовательной программы, методов и средств обучения в процессе освоения обучающимся образовательной программы или ее части.

Текущий контроль осуществляется через Платформу, путем дистанционного взаимодействия в следующих формах:

- контроль посещаемости Платформы обучающимися, выполнения действий;
- через обсуждение изучаемых вопросов в чате с преподавателем;

Оценка качества освоения образовательной программы включает итоговую аттестацию в форме зачета в виде тестового задания. Оценивание ответов на итоговой аттестации осуществляется следующим образом: «зачет»- правильных ответов по тесту 80% и более, «незачет» - правильных ответов по тесту менее 80%.

Обучающийся считается успешно освоившим дополнительную общеобразовательную (общеразвивающую) программу при условии выполнения на оценку «зачет» заданий итоговой

аттестации. Обучающимся, успешно окончившим дополнительную общеобразовательную (общеразвивающую) программу выдается сертификат о прохождении дополнительной общеобразовательной (общеразвивающей) программы «Защита информации от несанкционированного доступа».

## **10. Учебно-методическое обеспечение образовательной программы.**

**10.1.** Реализация образовательной программы осуществляется путем предоставления доступа к образовательной программе <https://in.wada.su/>. Обучение по программе осуществляется путем изучения текстовых и графических материалов (таблиц и схем), просмотра видеоуроков, размещенных на образовательной платформе.

**10.2.** Перечень электронных образовательных ресурсов:

Национальная электронная библиотека <https://rusneb.ru/>

Российская государственная библиотека для молодежи <https://rgub.ru/>

Официальный интернет – портал правовой информации <http://pravo.gov.ru/>

**10.3.** Список использованной литературы.

1. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ.

2. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ.

3. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ.

4. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ.

5. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.

6. Белоус А.И., Солодуха В. А. Кибероружие и кибербезопасность. О сложных вещах простыми словами. -Москва: Инфа-Инженерия, 2020.

7. Белоус А.И., Солодуха В. А. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. - Москва: ТЕХНОСФЕРА, 2021.

8. Диогенез Ю., Озкайя Э. Кибербезопасность: стратегия атак и обороны. / Перевод Д.А. Беликова. - Москва: ДМК пресс, 2020.

9. Колисниченко Д. Н. Секреты безопасности и анонимности в интернете. - Санкт-Петербург: БХВ-Петербург, 2020.

10. Мартиросян А. Формирование системы обеспечения безопасности киберпространства. Монография. - Москва: Проспект, 2022.

11. Масалков А.С. Особенности киберпреступлений. Инструменты нападения и защиты информации. - Москва: ДМК Пресс 2018.

12. Сафронов Е. В. Азы кибергигиены. Методологические и правовые аспекты. - Москва: Проспект, 2018.

13. Ярошенко А. В. ХАКИНГ на примерах. Уязвимости, взлом, защита. - Москва: Наука и Техника, 2021.

## **11. Образец тестового задания для итоговой аттестации.**

Вопрос 1. Выберите один или несколько ответов.

Комплекс принципов, правил, процедур и руководящих инструкций для защиты информационных активов компании от рисков, возникающих в результате реализации угроз информационной безопасности — это:

- a. Политика
- b. Контроль доступа
- c. Авторизация

- d. Идентификация
- e. Аутентификация

Вопрос 2. Выберите один или несколько ответов.

Какую информацию можно включить в коммерческую тайну?

- a. Потребительская информация о товаре — из чего состоит, когда произведен, условия использования и другое
- b. Имя генерального директора
- c. Стратегические планы

Вопрос 3. Выберите один или несколько ответов.

Процесс преобразования данных в секретный код для предотвращения несанкционированного доступа — это:

- a. Анализ рисков
- b. Шифрование
- c. Контроль доступа

Вопрос 4. Выберите один или несколько ответов.

Какие уровни документации включает в себя политика информационной безопасности компании:

- a. Верхний, средний (основной) и технический уровни
- b. Экспертный, базовый, низший уровни

Вопрос 5. Выберите один или несколько ответов.

Что подразумевается под конфиденциальностью информации?

- a. Это гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена
- b. Гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений
- c. Это гарантия получения требуемой информации или информационной услуги пользователем за определенное время

Вопрос 6. Выберите несколько вариантов.

Основными принципами информационной безопасности являются:

- a. Учет
- b. Неотрекаемость
- c. Доступность
- d. Конфиденциальность
- e. Целостность

Вопрос 7. Выберите один или несколько ответов.

Защита информации — это:

- a. Пошаговые инструкции по выполнению задач безопасности
- b. Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
- c. Детализированные документы по обработке инцидентов безопасности

Вопрос 8. Выберите один или несколько ответов.

Как называется состояние информации, при котором она существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений?

- a. Конфиденциальность
- b. Доступность
- c. Целостность

Вопрос 9. Выберите один или несколько ответов.

Какие из нижеперечисленных мер относятся к административно-организационным мерам защиты информации? возможно несколько ответов.

- a. Организация работы с документами и документированной информацией
- b. Резервное копирование и восстановление данных
- c. Введение режима коммерческой тайны
- d. Защита физических активов, таких как серверы, центры обработки данных и другая критически важная инфраструктура, от несанкционированного доступа, кражи или повреждения
- e. Организация режима и охраны, пропускной режим, режим видеонаблюдения
- f. Внедрение механизма аутентификации и авторизации пользователей

Вопрос 10. Выберите верный вариант ответа.

Информационная безопасность — это:

- a. Процесс разработки структуры базы данных в соответствии с требованиями пользователей
- b. Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.
- c. Получение определенных информационных услуг