ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ 2024/2025 гг.
ШКОЛЬНЫЙ ЭТАП
ТРУД (ТЕХНОЛОГИЯ)
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
5-6 КЛАСС

МАТЕРИАЛЫ ДЛЯ ЧЛЕНОВ ЖЮРИ (КЛЮЧИ, КРИТЕРИИ ОЦЕНИВАНИЯ)
Максимальное количество баллов - 60 баллов

Общая часть (5 баллов)

1. **(1 балл)** Как называется оборудование, которое позволяет изготавливать изделия, изображённые на рисунках?

1. Лазерный резак
2. Швейная машина
3. 3D-принтер
4. гравировальный станок

Ответ: 3

2. **(1 балл)** Компьютерная графика - это...?

1. Разные виды документов, создаваемых или обрабатываемых с помощью компьютера
2. Разные виды графических изображений, создаваемых или обрабатываемых с помощью компьютера
3. Разные виды графических изображений

Ответ: 2

3. **(1 балл)** Установите соответствие между старинными и современными приборами, выполняющими одну и ту же функцию

Ответ: БВА

4. (1 балл) Исследованием мусора, его состава и способов утилизации занимается целая наука. Как она называется?
1. Урбоэкология;
2. Гарбология;
3. Микология;
4. Аутоэкология.
Ответ: 2

5. (1 балл). Из использованных алюминиевых банок в результате переработки можно изготовить много полезных вещей, например, рамы для велосипедов.

Узнать алюминиевые изделия, пригодные для переработки, можно по специальной экомаркировке (см. маркнровку).

При переработке 800 алюминиевых банок получают достаточное количество металла для создания одной рамы для велосипеда.

Сколько таких банок потребуется переработать, чтобы изготовить 15 рам?
Ответ: 12000

Специальная часть (45 баллов)

1. (2 балла) Предоставление определенному лицу или группе лиц прав на выполнение определенных действий называется:
1. Идентификация.
2. Аутентификация.
3. Авторизация.
4. Модификация.
Ответ: 3

2. (2 балла) Персональные данные состоят из:
1. ФИО, возраст, домашний адрес и номер телефона.
2. Паспортные данные.
3. Группа крови, отпечатки пальцев.
4. Все вышеперечисленное.
Ответ: 4

3. (2 балла) Метод защиты информации, связанный с регулированием использования всех ресурсов информационной системы, называется:
1. управление доступом
2. маскировка
3. регламентация
4. побуждение
Ответ: 1

4. (2 балла) Какое из утверждений верно:
А. Любое сообщение об ошибке компьютера указывает на заражение вирусом.
Б. Компьютерные вирусы и вредоносные программы могут исполнять музыкальные произведения, издавать странные и неожиданные звуки, а также шум.
1. Верно утверждение А.

2. Верно утверждение Б.
3. Верны оба утверждения.
4. Оба утверждения неверны.
Ответ: 2

5. (2 балла) К компьютерным вирусам не относятся следующие программы:
1. Windows
2. Word
3. Win32
4. Chameleon
* Допускается несколько вариантов ответа
Ответ: 1,2

6. (2 балла) Какие данные не стоит указывать при заполнении онлайн-формы для ввода данных, которые будут опубликованы на сайте?
1. Никнэйм или псевдоним.
2. ФИО.
3. Адрес, где ты живешь.
4. Адрес, где ты учишься.
* Допускается несколько вариантов ответа
Ответ: 2,3

7. (4 балла, по 1 баллу за пару). Соотнесите вид компьютерного вируса с его описанием

Вид компьютерного вируса	**Описание компьютерного вируса**
1. Файловые вирусы	А. Внедряются в загрузочный сектор диска. Операционная система при этом загружается с ошибками и сбоями.
2. Загрузочные вирусы	Б. Внедряются в исполняемые файлы (программы) и активизируются при их запуске.
3. Макровирусы	В. Заражают компьютер после открытия вложенного файла (вируса) в почтовое сообщение
4. Сетевые вирусы	Г. Заражают документы Word, Excel и других прикладных программ операционной системы Windows.

Ответ: 1-Б , 2-А, 3-Г, 4-В

8. (4 балла, по 2 балла за слово) Игорь, чтобы не скучать во время долгой поездки, стал зашифровывать названия разных городов, заменяя буквы их порядковыми номерами в алфавите. Расшифруйте пункты прибытия и отправления поезда, каждое из которых записывается с помощью всего лишь трех цифр.

Пункт отправления поезда: 12112115

Пункт прибытия поезда: 1151171

Русский алфавит:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ъ	Ю	Я
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Ответ: Абакан-Анапа

9. (25 баллов, по 2 балла за слово+1 балл за верное написание всех слов) Разгадайте кроссворд:

Вопросы:

По горизонтали:

1. Устройство для обмена информацией между компьютерами через телефонные, оптоволоконные и другие сети.
5. Хранилище данных о пользователе на разных сайтах или устройствах.
6. Фамилия разработчика одной из антивирусных программ.
8. Программа, осуществляющая несанкционированные действия по сбору и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию.
10. Наука о методах и процессах сбора, хранения, обработки и анализа и оценки информации, обеспечивающих ее использование для принятия решений.
11. Программа, предназначенная для локализации и уничтожения вируса на конкретных компьютерах.

По вертикали:

2. Программа для мгновенного обмена сообщениями через Интернет.
3. Распознавание объекта по его идентификатору.
4. Нежелательные сообщения в любой форме, которые отправляются в большом количестве.
5. Последовательность определенных действий или шагов для решения поставленной задачи.
7. Секретное слово или набор символов, применяемое для конфиденциальности.
9. Информация, представленная в определенной форме и предназначенная для передачи.

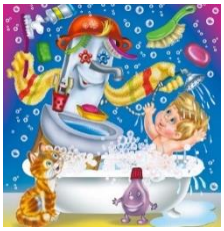
Ответ:

1. модем	**2. мессенджер**
5. аккаунт	**3. идентификация**
6. Касперский	**4. спам**
8. вирус	**5. алгоритм**
10. информатика	**7. пароль**
11. антивирус	**9. сообщение**

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ 2024/2025 гг.
ШКОЛЬНЫЙ ЭТАП
ТРУД (ТЕХНОЛОГИЯ)
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
5-6 КЛАСС

Кейс-задание (10 баллов)

10. (10 баллов, по 2 за правило) Сформулируйте основные правила безопасного поведения в Интернете, используя сюжеты известных сказок:

1 	2 	3 
Русская народная сказка «Волк и семеро козлят»	**А.Н. Толстой «Золотой ключик, или Приключения Буратино»**	**К.И. Чуковский «Мойдодыр»**
4 	5 	
Русская народная сказка «Коза-дереза»	**Русская народная сказка «Морозко»**	

Ответ:

№ иллюстрации	**Правила безопасного поведения в Интернете**
1	Под маской виртуального друга может скрываться злой человек
2	Опасайся мошенников. Не сообщай никому свои пароли, не посылай СМС в ответ на письма от неизвестных людей
3	Проверяй компьютер на вирусы, пользуйся антивирусными программами
4	Используй, скачивай информацию только с проверенных сайтов.
5	Будь вежливым при общении в сети, не груби, тогда и к тебе будут относиться так же).

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ 2024/2025 гг.
ШКОЛЬНЫЙ ЭТАП
ТЕХНОЛОГИЯ
7-8 КЛАСС

МАТЕРИАЛЫ ДЛЯ ЧЛЕНОВ ЖЮРИ (КЛЮЧИ, КРИТЕРИИ)

МАКСИМАЛЬНОЕ КОЛИЧЕСТВО БАЛЛОВ - 60.

Общая часть (5 баллов)

1. **(1 балл)** Определите, к каким основным типам профессий относится профессия «графический дизайнер».

1) человек – знак
2) человек – природа
3) человек – техника
4) человек – человек
5) человек – художественный образ

2. **(1 балл)** Назовите составной элемент FFF (Fused Filament Fabrication) 3Dпринтера, предназначенный для нагрева и выдавливания термопластика через специальное сопло в зону печати.

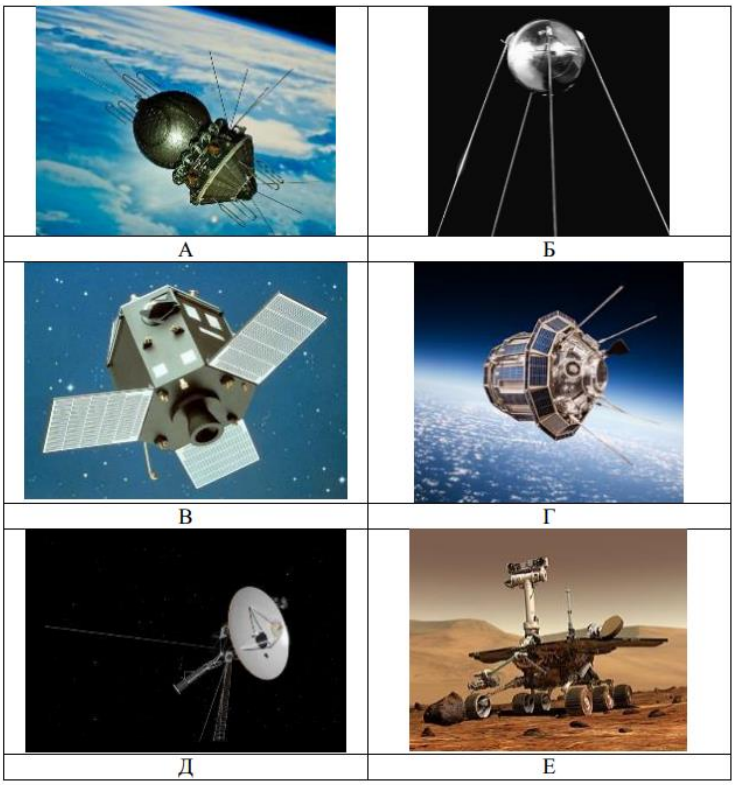
1) воронка
2) комбайн
3) цилиндр
4) филамент
5) экструдер
6) эксцентрик

3. **(1 балл)** Из предложенных изображений выберите два, на которых изображены инструменты, основанные на рычаге первого рода

Ответ: Б, З

4. (1 балл) 4 октября 1957 года на орбиту Земли был выведен первый искусственный спутник Земли, советский космический аппарат, который назывался «Спутник-1». Он получил кодовое обозначение — «ПС-1» («Простейший Спутник-1»).

Рассмотрите предложенные изображения. Среди них выберите то, на котором изображён ПС-1.



Ответ: Б

5. (1 балл) При благоустройстве парка было решено посыпать несколько тропинок песком. Длины тропинок равны 45 м 5 см, 12 м 6 дм 9 см, 707 дм и 314 см. Определите общую длину тропинок, которые решили посыпать песком. Ответ дайте в сантиметрах.

Ответ: 13158

Специальная часть (45 баллов)

1. (2 балла, по 1 баллу за каждую расшифрованную аудиторию)

Расшифруйте аббревиатуры:

АСОД Автоматизированная система обработки данных

КСЗИ Комплексная система защиты информации

2. (2 балла) Вставьте пропущенное слово/словосочетание в следующем утверждении:

Аутентификация – это процесс подтверждения ***ЛИЧНОСТИ ПОЛЬЗОВАТЕЛЯ,*** *часто используется в сочетании с паролями, биометрическими данными или одноразовыми кодами.*

3. (2 балла) Вставьте пропущенные слова/словосочетания в следующее утверждение

Под субъектами системы информационной безопасности понимают активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения системы. В качестве субъектов могут выступать ***ПОЛЬЗОВАТЕЛИ****, активные программы и процессы.*

4. (2 балла) Примером двухфакторной аутентификации является запрос пользователю:

1) ввести пароль и ответить на секретный вопрос;
2) приложить электронную карту к сканеру и ввести PIN-код;
3) пройти распознавание лица и затем отсканировать отпечаток пальца;
4) подключить электронный ключ (токен) и отсканировать штрихкод пропуска.

Ответ: 2

5. (2 балла) В мандатной модели разграничения доступа определение того, имеет липользователь право доступа к файлу, определяется на основе

1) наличия или отсутствия у данного пользователя прав доступа к данному файлу;
2) соотношения метки (уровня) секретности файла и уровня допуска пользователя;
3) установленного для файла режима доступа;
4) роли (уровня) пользователя в системе.

Ответ: 2

6. (2 балла) Стеганография – это категория мер защиты информации:

1) основанных на сохранении в секрете факта передачи и хранения информации;
2) предназначенных для усиления криптографии;
3) предназначенных для передачи секретной информации из системы;
4) основанных на криптографии, но не требующих от пользователей использовать секретные ключи;

Ответ: 1

7. (2 балла) Среди вредоносных программ различных классов создавать собственныекопии могут:

1) троянские программы;
2) сетевые черви;
3) руткиты;
4) шифровальщики;

Ответ: 2

8. (2 балла) Укажите, что из перечисленного может составлять коммерческую тайну:

1) Сведения о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке.

2) Сведения об устройстве или компонентном составе некоторого изделия.

3) Сведения, содержащиеся в учредительных документах юридического лица.

4) Сведения об использовании государственным или муниципальным предприятием средств соответствующих бюджетов.

5) Сведения о задолженности организации по заработной плате.

Ответ: 3

9. (5 баллов) Авиакомпания N для облегчения пилотирования самолётов устанавливает на них системы автоматического управления (автопилот). Для запуска работы такой системы пилот должен ввести координаты пунктов отправления и назначения, параметры самолёта, а также авторизационные данные для связи с наземными диспетчерскими службами по пути следования. Далее система осуществляет пилотирование по указаниям наземных служб, передавая управление пилоту в случае необходимости принятия решений, возникновении внештатных ситуаций и в иных предусмотренных случаях.

Оцените, какие из утверждений являются верными, а какие нет.

1) Для обеспечения корректного исполнения поступающих от наземных служб указаний требуется обеспечить, в первую очередь, их конфиденциальность.

2) Для того, чтобы наземные службы могли постоянно следить за координатами самолёта, требуется обеспечить доступность этих данных.

3) Для корректного принятия решений системой пилотирования с учётом параметров самолёта необходимо обеспечить целостность этих данных в памяти программы.

4) Пилоты в момент пилотирования могут рассматриваться в качестве потенциальных нарушителей безопасности информации в системе.

5) Во время полёта пассажирам может быть запрещено использовать коммуникационные устройства из-за возможности нарушения доступности сигналов от наземных служб при случайном совпадении частот сигналов и внесения искажений.

Ответ: Верные утверждения: 2,3,4 Неверные утверждения: 1,5

10. (4 балла) Сопоставьте категории вредоносного программного обеспечения с их характерными особенностями.

11.

Категория вредоносного программного обеспечения	**Характерные особенности**
1) вирус	А) может создавать собственные копии
2) руткит	Б) маскируется под легальную программу
3) троянская программа	В) блокирует доступ к пользовательским данным
4) шифровальщик	Г) позволяет нарушителю скрывать активность в системе

Ответ: 1- А, 2-Г, 3-Б, 4-В

Задания 10-11

С помощью шифра Цезаря осуществляется шифрование сдвигом. Каждая из букв алфавита заменяется на букву, находящуюся от неё на определённом расстоянии слева или справа.

Если в качестве ключа взять пару «Ё – Я», то часть таблицы замены будет выглядеть следующим образом:

Исходный текст	**А**	**Б**	**В**	**Г**	**Д**	**Е**	**Ё**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**
Зашифрованный текст						Ю	Я	А	Б	В	Г	Д					

Исходный текст	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**	**Ю**	**Я**
Зашифрованный текст																

12. (4 балла) С помощью данного шифра зашифруйте слово ПАРАЛЛЕЛОГРАММ.

В ответ запишите последовательность букв без кавычек и пробелов.

Ответ: ИЩЙЩЕЕЮОЕЗЬЙЩЁЁ

13. (4 балла) С помощью данного шифра расшифруйте слово ДЗЭВНВДЩЛЗЙ.

В ответ запишите последовательность букв без кавычек и пробелов.

Ответ: КОДИФИКАТОР

12. (12 баллов, по 1,5 балла за каждое слово и знак препинания) Шифр, известный как «квадрат Полибия», устроен следующим образом. В квадратную или прямоугольную таблицу вписываются буквы алфавита (для кодирования – в алфавитном порядке, для шифрования – в произвольном, при этом расположение букв в таблице является ключом), строки и столбцы таблицы обозначаются цифрами. При зашифровании буквы открытого текста заменяются на пары цифр, которыми отмечены, соответственно, строка и столбец, в которых стоит данная буква.

Например, на иллюстрации ниже буква «О» зашифрована сочетанием цифр «34», а слово «ОКО» – «34 26 34».

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	.	,	?

Таким шифром зашифрован некоторый текст (без пробелов, но с сохранением знаков препинания – точки и запятой):

51 16 32 41 31 34 22 33 16 16 32 16 42 34 15 65 42 16 32 32 16 33 56 52 16 41 13 34 12 34 15 55 64

Напишите слова из зашифрованного сообщения.

Ответ: ЧЕМ СЛОЖНЕЕ МЕТОД, ТЕМ МЕНЬШЕ СВОБОДЫ.

Кейс-задание (10 баллов)

Сформулируйте 10 основных правил безопасности в Интернете (Участник может дать близкие по смыслу формулировки). **По 1 баллу за каждое правило**

1) Используйте надежный пароль.

2) Заходите в интернет с компьютера, на котором установлен антивирус.

3) Заведите один основной почтовый адрес и придумайте к нему сложный пароль.

4) Если Вы хотите скачать какой-то материал из интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес своей электронной почты, то, скорее всего, на Ваш адрес будут высылать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.

5) Скачивайте программы либо с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников.

6) Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были.

7) Если Вы работаете за компьютером, к которому имеют доступ другие люди

(на роботе или в интернет кафе), не сохраняйте пароли в браузере.

8) Не открывайте письма от неизвестных Вам пользователей (адресов) или письма с оповещением о выигрыше в лотереи, в которой Вы просто не участвовали.

9) Не нажимайте на вплывающие окна, в которых написано, что Ваша учетная запись в социальной сети заблокирована.

10) Периодическим меняйте пароли на самых важных сайтах.

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ 2024/2025 гг.
ШКОЛЬНЫЙ ЭТАП
ТРУД (ТЕХНОЛОГИЯ)
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
9-11 КЛАСС

МАТЕРИАЛЫ ДЛЯ ЧЛЕНОВ ЖЮРИ (КЛЮЧИ, КРИТЕРИИ) МАКСИМАЛЬНОЕ КОЛИЧЕСТВО БАЛЛОВ - 60.

Общая часть (5 баллов)

Номер вопроса	Max балл	Правильный ответ
Общая часть		
1	1	5
2	1	2,1,3
3	1	13158
4	1	1-В, 2-А, 3-Г, 4-Б, 5-Е, 6-Д
5	1	2175

Специальная часть (45 баллов)

1	2	Федеральное Агентство Правительственной Связи и Информации Комплексная система защиты информации
2	2	ПРИНЦИПАМИ
3	5	Верно: 1,2,4. Неверно: 3,5
4	2	1
5	2	2
6	2	3
7	2	3
8	2	2
9	2	2
10	4	1,3
11	6	1-Б,В,Е 2-А,Г,Д
12	5	Ключ сдвига: 5 (1 балл) Расшифрованный текст: Стеганография, криптография-отличные способы сохранить пароль в секрете. Для базы данных я применяю пароль слово гарантия. (по 0,25 балла за слово)
13	9	Везде исследуйте всечасно, Что есть велико и прекрасно. (по 1 баллу за слово, по 0,25 баллов за знак препинания)

Кейс-задание (10 баллов)

Какие действия могли предпринять работники NASA, чтобы выявить причину заражения и как обезвредить? Укажите два основных действия с обоснованием **(5 баллов, по 2,5 балла за каждое действие с обоснованием).**

С какими угрозами информационной безопасности можно столкнуться в наши дни и как с ними бороться? Укажите две основные угрозы и обоснуйте их выбор **(5 баллов, по 2,5 балла за каждое действие с обоснованием).**

Примерные варианты ответов:

1. Какие действия могли предпринять работника NASA, чтобы выявить причину заражения и как обезвредить?

Причины заражения:

*Для быстрого и своевременного выявления причины необходимо было обратиться незамедлительно в Центр национальной компьютерной безопасности США.

*Чтобы выявить причину заражения нужно просканировать систему антивирусом или антивирусным сканером

*Антивирусная система CHK4BOMB позволяла проанализировать текст загрузочного модуля и выявлять все текстовые сообщения и «подозрительные» участки кода.

Действия:

*Единственным способом остановить червя было полное отключение компьютера от сети.

*Буквально за два дня были определены и заблокированы «лазейки», через которые червь проникал в систему, а код заразы был целиком дизассемблирован. За 12 часов активной работы и изучения кода программисты смогли написать закрывающую дыры заплатку и начать распространять её по сети.

*Вредоносную активность сразу же обнаружили администраторы сети. Они привлекли большое количество разработчиков для борьбы с нею. Решением проблемы занимались специалисты Центра национальной компьютерной безопасности, Национального института науки и технологий, Агентства военной связи, Министерства энергетики США, ЦРУ, ФБР и других организаций США.

2. С какими угрозами информационной безопасности можно столкнуться в наши дни т как с ними бороться?

Угрозы информационной безопасности:

*Вирусы, черви и трояны — вредоносные программы, которые проникают в компьютер или сеть и наносят различный вред. С их помощью киберпреступники крадут, портят и уничтожают данные.

*Перехват паролей — процесс получения доступа к чужому аккаунту путем кражи учетных данных.

*Фишинг — мошенническая практика, когда киберпреступники выдают себя за надежные источники для получения личной информации. Одна из разновидностей фишинга — использование подменных доменных имен, которые похожи на настоящие.

*Социальная инженерия — манипуляции людьми с целью получения личной информации или выполнения определенных действий. Например, злоумышленник может различными способами втираться в доверие к жертве, ведя с ней переписку в социальных сетях или мессенджерах.

Методы борьбы:

* Антивирусное и антишпионское ПО. Предназначено для обнаружения и удаления вредоносных программ, таких как вирусы, трояны, шпионские программы.

*Криптография. Обязательно шифруйте данные, это играет важнейшую роль в их защите. Шифрование информации при передаче и хранении помогает предотвратить утечки, причем даже при компрометации системы в целом. Это процесс преобразования исходных данных в зашифрованные с помощью специального алгоритма, который называют ключом. Таким образом, криптографическая защита делает информацию непонятной для всех, кто таким ключом не владеет.

*Управление доступом. Разграничьте права и используйте дополнительную защиту. Речь прежде всего о программных ограничениях доступа — разграничении пользователей при помощи аутентификации с различными правами.

*Программная защита. Установите дополнительное ПО. Программная защита включает использование антивирусов и антишпионских программ, брандмауэров (межсетевых экранов) и других средств для обнаружения и предотвращения киберугроз. Такие программы защитят корпоративную сеть от вирусов, червей, троянов, руткитов, кейлоггеров, шпионского и рекламного ПО (adware), программ-вымогателей. А брандмауэры снижают риск несанкционированного доступа и DDoS-атак.

*VPN и прокси. VPN (виртуальные частные сети) и прокси-серверы обеспечивают безопасное соединение с сетью через шифрование трафика, что позволяет защитить информацию при передаче через открытые сети.

*Сканеры уязвимостей. Используются для поиска уязвимостей в сетях, приложениях и устройствах, чтобы предотвратить возможные кибератаки.