ИННОВАТИКУМ

Всероссийский форум школьников

для учащихся 8–11 классов и молодых педагогов

КЕЙС

«КИБЕРБЕЗОПАСНОСТЬ»

2024

Дорогие участники Форума! Предлагаем вам познакомиться с кейсом, раскрывающим некоторые особенности работы по направлению «Кибербезопасность».

Изучите предлагаемые материалы, найдите дополнительную информацию и выполните задания, приведенные в конце кейса.

В тексте и заданиях кейса будут встречаться понятия «профессия» и «специальность». Поясним разницу между ними.

Профессия – это род деятельности, для освоения которой нужно приобрести специальные знания и умения.

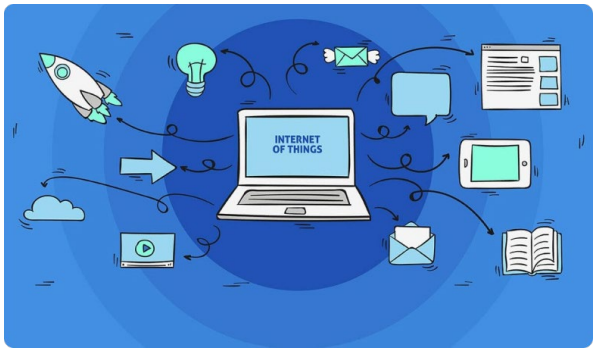
Специальность приобретается в рамках выбранной профессии. Одна профессия может включать несколько специальностей. Например:

- ✓ юрист – это профессия, а юрисконсульт, нотариус – ее специальности;
- ✓ учитель – это профессия, а учитель математики – специальность;
- ✓ врач – это профессия, а хирург, кардиолог – специальности врача.

В нашем кейсе мы рассмотрим профессии в сфере кибербезопасности.

Интернет во многом упростил нашу жизнь. Но также стал источником опасности для всех, кто им пользуется: утечки персональных данных, вредоносные программные обеспечения и многое другое. В этом кейсе мы разберем направление «Кибербезопасность». Поговорим, с какими проблемами сталкиваются профессионалы, какие есть специальности и какое будущее нас ждет!

Только представьте, что в 2023 году в мире было зафиксировано более 16,7 млрд устройств, у которых есть выход в Интернет. По некоторым прогнозам, к 2030 году количество устройств **интернета вещей** будет превышать отметку в 29 млрд. **Интернет вещей** – это сеть физических устройств, которые подключены к другим устройствам и службам через Интернет или другую сеть и обмениваются с ними данными.



В кейсе вы встретите некоторые профессиональные термины направления «Кибербезопасность». Для удобства работы с заданиями мы собрали для вас словарь терминов. Его вы найдете в приложении к кейсу.

Давайте вернемся к кибербезопасности. Вы уже поняли, что количество устройств в мире сейчас превышает количество людей примерно в два раза. Конечно же, все эти устройства

потенциально могут стать объектом атаки киберпреступников. И чтобы такого не происходило, нужны специалисты по кибербезопасности.

Кибербезопасность – это совокупность методов и практик защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от атак злоумышленников. Она включает множество аспектов, таких как защита компьютеров и сетей от вирусов и других вредоносных программ, обеспечение безопасности личных данных в интернете, защита от хакеров и многое другое.

«Мир сейчас живет в состоянии постоянной кибервойны. По известным данным, в мире сейчас действуют более 130 кибергруппировок, но в реальности их уже больше. В 2023 году мировой ущерб от кибератак достиг примерно $8 трлн – это в два раза больше убытка, принесенного эпидемией коронавируса за два года. К 2025 году цифры вырастут до $10,5 трлн».

Алексей Марков,
президент группы компаний НПО «Эшелон»,
профессор МГТУ им. Н. Э. Баумана

Современный мир сегодня приближается к **Индустрии 4.0**. Фокус внимания специалистов по кибербезопасности уже нацелен не только на защиту компаний, но на каждого человека. Ведь современные кибератаки все чаще направлены на конкретного человека и его личные данные.

Индустрия 4.0 – четвертая промышленная революция. Она предполагает новый подход к производству, основанный на массовом внедрении информационных технологий в промышленность, масштабной автоматизации бизнес-процессов и распространении искусственного интеллекта.

Подробнее об Индустрии 4.0 и ее трендах вы можете узнать из статей РБК: Что такое Индустрия 4.0? Индустрия 4.0 в 40 цифрах и фактах.

Но подобные изменения произойдут не только на производствах, но и в нашей обычной жизни. В домах все чаще начнут появляться умные устройства, которые потенциально могут стать объектами кибератак. Цифровизация приведет к развитию целых «умных» городов.

У вас может возникнуть вопрос, как устройства умного дома (робот-пылесос, умная колонка и другие еще более простые устройства) могут помочь преступникам получить личную информацию.

Чтобы вы смогли ответить на этот вопрос, мы предлагаем ознакомиться со статьей, где рассказывается про получение информации через датчики освещенности. Статью можно прочитать по ссылке.

Важно сказать, что очень часто под кибербезопасностью подразумевают сохранность данных, но работа специалистов по кибербезопасности намного сложнее. Давайте сначала разберем виды киберугроз:

Киберпреступление – действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.

Кибератака – действия, нацеленные на сбор информации.

Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

И все эти угрозы могут быть направлены как на компанию, так и на конкретного человека! По данным Positive Technologies (ведущий российский разработчик продуктов, решений и сервисов для результативной кибербезопасности) самыми атакуемыми отраслями в России в следующем году станут:

— Государственный сектор экономики;
— Медицинский сектор;
— Наука и образование.

Подробнее со статистикой вы можете ознакомиться на сайте компании по ссылке.

Именно поэтому востребованность в специалистах по кибербезопасности постоянно растет. Давайте разберем подробнее, какие есть специалисты в области кибербезопасности.

СПЕЦИАЛИСТЫ ПО КИБЕРБЕЗОПАСНОСТИ

Сейчас буквально для каждой компании или организации важно иметь специалиста по кибербезопасности или иметь подключение к системе, которая может обеспечить подобную защиту. Больницы, школы, банки, организации, которые занимаются инфраструктурой города и многие другие, – все они могут быть в опасности. Важность появления специалистов этой области обусловлена еще и следующими факторами:

1. Снижение рисков. Количество специалистов снижает риски, связанные с кибератаками, которые могут привести к финансовым потерям, нарушению работы бизнеса или инфраструктуры города.
2. Соблюдение законодательства. Многие страны, в том числе и Россия, имеют строгие законы, касающиеся кибербезопасности и защиты личных данных. Увеличение специалистов в этой области и появление их в каждой компании помогает организациям соблюдать законодательство, особенно если наши компании выходят на международный рынок.
3. Обучение людей информационной грамотности. Граждане учатся защищать себя от киберугроз и правильно использовать технологии.
4. Конкурентоспособность. В современном мире, где информация является ключевым активом, компании, которые уделяют внимание кибербезопасности, имеют конкурентное преимущество перед теми, кто этого не делает. Это также влияет и на репутацию компании в глазах пользователей. Если компания производит какой-то продукт, то пользователям важно знать, что компания позаботилась о защите этого продукта от взломов и атак.

Разработчики программного обеспечения в области кибербезопасности занимаются созданием и поддержкой программного обеспечения, предназначенного для защиты информационных систем от кибератак и обеспечения безопасности данных. Они занимаются разработкой и улучшением систем защиты, таких как антивирусы, брандмауэры, системы обнаружения вторжений. Для каждого вида угроз существуют свои специалисты, но в рамках этого кейса мы рассмотрим только нескольких.

Разработчик программного обеспечения в сфере кибербезопасности.

Специалисты такого рода могут заниматься созданием специализированного программного обеспечения или связанных с безопасностью решений. Они могут разрабатывать стратегию безопасности программного обеспечения в масштабах компании, участвовать в каждом этапе жизненного цикла создания и эксплуатации программных систем, тестировать ПО на наличие уязвимостей и т. д.

Этичный хакер, или пентестер.

Этичные хакеры получают от работодателей разрешение на попытку проникновения в информационные системы. Прежде чем злоумышленник сможет причинить реальный вред, пентестер найдет проблемы с сервисами и приложениями, ошибки в настройках и многое другое. По их рекомендациям будут созданы и внедрены улучшения.

Компьютерный криминалист.

Компьютерные криминалисты определяют, как произошел инцидент, кто в нем виноват, какие данные и системы были скомпрометированы и т. д. При необходимости они сотрудничают с правоохранительными органами и решают широкий круг задач, включая восстановление потерянных файлов, интерпретацию данных и анализ записей в системных журналах.

С более подробным списком специальностей в сфере кибербезопасности вы можете ознакомиться по ссылке.

Как и во многих других технических специальностях, специалист по кибербезопасности должен обладать значительными техническими знаниями. У такого человека должны быть отличная теоретическая подготовка и опыт. Он должен неплохо разбираться в законодательных нормах и требованиях в области защиты информации и информационной безопасности в целом.

НОВЫЕ НАПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Сегодня активно обсуждается тема нейросетей и развития искусственного интеллекта. Она актуальна и для кибербезопасности. С появлением нейросетей у специалистов, которые занимаются защитой от киберугроз, появился повод изменить подход в своей работе. Как и любая другая технология, искусственный интеллект может стать как защитником, так и вредителем. Все сильно зависит от того, кто и как его использует.

Эксперты считают, что 80% технологий, которые будут разработаны в ближайшие годы, будут основаны на ИИ-алгоритмах. Количество и разнообразие приложений искусственного интеллекта продолжает расти, а исследователи и ученые постоянно находят новые способы их использования. Согласно исследованиям, уже сегодня 77% устройств, которые мы используем в жизни, имеют встроенный искусственный интеллект. Для примера расскажем о технологии дипфейк, которая появилась буквально несколько лет назад.

Вред и проблемы	Польза в применении
Слово deepfake объединяет два понятия: «глубокое обучение» (deep learning) и «подделка» (fake). Это фальшивый аудио- и видеоконтент, созданный с помощью нейросетей, практически неотличимый от подлинного.	Технология дипфейка активно используется в кинематографе, когда нужно изменить возраст актера на экране или воспроизвести опасный трюк.
Дипфейки несут угрозу не только для компаний и финансовых организаций, но и для репутации публичных людей, которые рискуют стать жертвами шантажа и ложных обвинений.	Интерактивное обучение. Представьте, что в будущем появится возможность посмотреть обучающие видео с известным писателем или ученым в качестве лектора.

Но как дипфейк влияет на развитие кибербезопасности? Специалисты начали активно развивать алгоритмы распознавания поддельного голоса и изображения, а также использовать программу, вставляющую в видеоконтент специальные цифровые артефакты, маскирующие

группы пикселей, по которым ориентируются программы для распознавания лиц. Этот прием замедляет работу дипфейк-алгоритмов, и в результате качество подделки будет ниже.

ИИ помогает определять разновидности атак и принимать целесообразные решения о защите. Алгоритмы машинного обучения постоянно изучают среду и адаптируются к новым угрозам, чтобы своевременно выявлять аномалии. ИИ-решения также умеют отслеживать и анализировать действия пользователей в режиме реального времени. В случае обнаружения нетипичных ситуаций они срабатывают: применяют один из сценариев защиты. Алгоритмы учитывают такую информацию, как географическое положение, рабочие часы сотрудников, идентификаторы устройств и многие другие.

ПОЛЕЗНЫЕ ИСТОЧНИКИ ДЛЯ РАБОТЫ

Подходит ли вам карьера в кибербезопасности: http://ja-russia.ru/obrazovanie/top-proekty/tsifrovye-navyki/testy-i-viktoriny/1506-karera-v-kiberbezopasnosti.html

5 самых востребованных профессий в области кибербезопасности: https://dzen.ru/a/Y6K0rVWZwB7V8Pxe

Словарь терминов информационной безопасности: https://www.ptsecurity.com/ru-ru/research/glossary/ru/a/

Подробный разбор на тему «Что такое кибербезопасность»: https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-kiberbezopasnost/

Кибербезопасность будущего: https://www.youtube.com/watch?v=sDKMplX6_R0

ЗАДАНИЯ КЕЙСА

Для дальнейшей работы на Форуме предлагаем выполнить задания кейса. Это поможет лучше разобраться в направлении «Кибербезопасность».

1. Составьте список основных современных профессий и специальностей по направлению «Кибербезопасность».

2. Выберите одну из перечисленных профессий/специальностей для дальнейшей работы на Форуме. Обоснуйте выбор.

3. Укажите особенности этой профессии/специальности с учетом вызовов времени. Объем текста не должен превышать 300 знаков без пробелов.

4. Определите сферы взаимодействия выбранного вами специалиста в области освоения новейших методов и технологий. Создайте интеллект-карту, на которой укажите, с какими специалистами он входит во взаимодействие и каков предмет каждого взаимодействия (подробнее про интеллект-карты можно посмотреть здесь: https://clck.ru/ZybYw).

5. Укажите пять «плюсов» и пять «минусов» выбранной профессии/специальности.

6. Определите пять профессиональных характеристик, которыми должен обладать выбранный специалист.

7. Определите пять личных качеств, которыми должен обладать выбранный специалист.

8. Проведите сравнительный анализ программ подготовки специалистов в вузах РФ и на основании его результатов укажите, в каких именно вузах страны ведется подготовка выбранных вами специалистов.

9. Укажите пять инноваций, которые были внедрены за последние 5-10 лет в отрасль энергетики. Укажите инновации в выбранной профессии/специальности, определяющие современный технологический/экономический прорыв России.

10. Составьте пять вопросов выбранному специалисту, которые хотели бы задать ему лично на пресс-конференции.

11. Составьте список дополнительных источников информации по выбранной профессии/специальности.

12. Обоснуйте, почему вы готовы выбрать в будущем эту профессию/специальность, а также почему не хотите ее выбирать.

13. Предложите слоган про выбранную вами профессию/специальность.

14. Напишите 15 ассоциаций к выбранной профессии.

15. Предложите сюжет фильма, книги или игры, через который вы могли бы рассказать об этой профессии своим друзьям.