- средствами индивидуальной защиты» / Контур Норматив [Электронный ресурс] – Режим доступа: <https://normativ.kontur.ru/document?moduleId=1&documentId=233654>.
3. Приказ Минтруда России от 09.12.2014 №997Н «Об утверждении Типовых норм бесплатной выдачи специальной одежды, специальной обуви и других средств индивидуальной защиты работникам сквозных профессий и должностей всех видов экономической деятельности, занятым на работах с вредными и (или) опасными условиями труда, а также на работах, выполняемых в особых температурных условиях или связанных с загрязнением» / Контур Норматив [Электронный ресурс] – Режим доступа: <https://normativ.kontur.ru/document?moduleId=1&documentId=247205>.
4. РД 5.0496 – 87 ССБТ Средства индивидуальной защиты работающих. Порядок обеспечения, хранения и ухода / Электронный фонд правовых и нормативно – технических документов [Электронный ресурс] – Режим доступа: <https://docs.cntd.ru/document/1200000277>.

Умархаджиев М.-Х.Р.

Кибербезопасность: угрозы, вызовы

*ФГБОУ ВО Чеченский государственный университет им А.А.Кадырова
(Россия, Грозный)*

doi: 10.18411/trnio-12-2021-105

Аннотация

Кибербезопасность - необходимое соображение для информационных технологий, а также интернет-услуги. Нам нужно признать важность различных типов рисков, которые существуют в онлайн-мире. Повышение кибербезопасности и защита критически важной информации имеет важное значение для национальной безопасности и экономической сущности. Всякий раз, когда мы думаем о кибербезопасности мы думаем о «киберпреступности», которая растет день ото дня. Различные правительства и компании принимают меры по предотвращению киберпреступности. Эта статья в основном фокусируется на тенденциях, проблемах и киберэтике в области компьютерной безопасности. Киберинциденты подчеркивают важность быть в курсе мировых тенденций киберпреступности, особенно относительно использования мобильных и персональных вычислительных устройств.

Ключевые слова: кибербезопасность, киберинциденты, киберэтика, киберпреступление, компьютерная безопасность.

Abstract

Cybersecurity is a necessary consideration for information technology as well as internet services. We need to recognize the importance of the different types of risks that exist in the online world. Enhancing cybersecurity and protecting critical information is essential to national security and economic substance. Whenever we think about cybersecurity we think about "cybercrime", which is growing day by day. Various governments and companies are taking action to prevent cybercrime. This article mainly focuses on trends, issues, and cyber ethics in the field of computer security. Cyber incidents highlight the importance of keeping abreast of global cybercrime trends, especially regarding the use of mobile and personal computing devices.

Keywords: cybersecurity, cyber incidents, cyber ethics, cyber crime, computer security.

Технологии развивались в разные эпохи. Интернет позволил людям отправлять и получать любую форму данных с большей скоростью. Но насколько безопасно данные передаются другому человеку без какой-либо утечки информация? — это один из важных вопросов. Сегодня Интернет - одна из самых быстрорастущих инфраструктур. В сегодняшней технической окружающей среды многие новейшие технологии меняют облик человечества. Заглядывая вперед, ясно одно: сегодня технологии не будут выглядеть так, как они выглядят. Но из-за этих новых технологий мы не можем эффективно защищать нашу личную информацию. Несмотря на технологические меры, принятые организаций и частных лиц, киберпреступность растет день ото дня. Большинство коммерческих сделок происходят

онлайн, поэтому это поле требует высокого качества безопасности. Следовательно, кибербезопасность стала одним из важных вопросов.

Чтобы общество продолжало пользоваться преимуществами информационных технологий, уязвимостями, угрозами и рисками нужно управлять с помощью кибербезопасности. Повышение кибербезопасности и защита критически важных информационных инфраструктур необходимы для безопасности и экономического благополучия каждой страны.

Киберпреступность — это совершение преступного деяния с использованием компьютера или сети Интернет. Все виды киберпреступлений включают в себя как компьютер и человек, стоящий за ним, как жертвы. Киберпреступность может включать в себя все, что угодно, например, скачивание незаконные музыкальные файлы, чтобы украсть миллионы долларов с банковских счетов в Интернете.

Мы живем в мире, где информация хранится в виде нулей и единиц. Конфиденциальность и безопасность данных — это первоочередное внимание большинства организаций. Сайты социальных сетей предоставляют пространство, где пользователи чувствуют себя в безопасности, поскольку они общаются с друзьями и семьей. Способность обнаруживать, исследовать, анализировать и реагировать на кибернетические угрозы и атаки - незаменимый компонент кибербезопасности.

Информационные технологии произвели революцию в функционировании экономики, общества и правительств вокруг Земли. Некоторые из технологических тенденций в области кибербезопасности объясняются ниже.

Мобильные технологии проникают на мировой рынок, и ожидается, что количество мобильных устройств превысит количество людей на Земле к концу 2022 года. Уже сейчас насчитывается почти шесть миллиардов мобильных абонентов. Мобильные технологии сами по себе создают огромные проблемы кибербезопасности. Смартфоны, оснащенные внутренними камерами, и Интернет может быть «лучшим шпионским инструментом», позволяющим хакерам прослушивать звонки, сделанные на устройстве, контролировать сообщения на мобильный и с мобильного, а также для отслеживания местоположения устройства. Хакеры могут использовать взломанный телефон «как скрытая камера, тайно записывать видео, подслушивать или делать аудиозаписи, а также отслеживать ваши движения с помощью геолокации.

Веб-серверы - одна из лучших платформ для киберпреступников для кражи данных. Угроза атак в сети приложений для извлечения данных или распространения вредоносного кода. Киберпреступники распространяют свой вирус через терминалы, которые они взломали. Но атаки с кражей данных, многие из которых привлекают внимание СМИ, также являются большой угрозой. Мы должны использовать безопасный браузер, чтобы не стать жертвой киберпреступности.

Облачные вычисления означают, что ваши данные хранятся на чужом компьютере. Мир медленно движется к облакам. Эта последняя тенденция представляет собой серьезную проблему для кибербезопасности, поскольку трафик может перемещаться по сторонам. Количество приложений, доступных в облаке, растет, облачные сервисы также должны развиваться, чтобы предотвратить угрозу, исходящую от киберпреступников. Облако может предоставить огромные возможности, но всегда следует учитывать, что по мере развития облака возникают проблемы с безопасностью.

Расширенная постоянная угроза (РПУ) — это сетевая атака, при которой неавторизованный человек получает доступ к сети и остается там незамеченным в течение длительного периода времени. Злоумышленник РПУ часто использует фишинг для доступа к сети законными способами. Как только доступ получен, злоумышленник открывает черный ход. В качестве злоумышленники становятся смелее и используют более расплывчатые методы, сетевая безопасность должна интегрироваться с другими средствами защиты, сервисами для обнаружения атак. Мы должны улучшить наши методы безопасности, чтобы предотвратить эти угрозы.

Рост социальных сетей также ставит новые задачи в области кибербезопасности. Хакеры давно полагаются на «социальный инжиниринг», убеждая людей раскрывать информацию, которую они не должны, чтобы завоевать доверие целей и компрометируют их сети. По мере того, как мы становимся более социальными через эти социальные сети, компании должны найти новые способы защиты личной информации. Социальные сети играют огромную роль в кибербезопасности и способствуют киберугрозе.

По мере повышения уровня корпоративной безопасности злоумышленники все больше полагаются на «социальную инженерию», чтобы завоевать доверие целей, убедить людей раскрыть информацию, которую они не должны, и впоследствии скомпрометировать цель сети. Почти сорок процентов записей, скомпрометированных в результате кибернетических данных, были скомпрометированы как результат инцидентов с применением социальной тактики. Более того, отраслевые данные показывают, что целевой фишинг лежит в основе наиболее целенаправленных атак. Следовательно, люди должны принимать соответствующие меры, особенно при работе с социальными сетями, чтобы предотвратить потерю своей информации. Способность людей делиться информацией с многомиллионной аудиторией лежит в основе вызова, который социальные сети представляют для бизнеса. Хотя социальные сети могут использоваться для киберпреступлений, эти компании не могут позволить себе прекратить использование социальных сетей, поскольку они играют важную роль в рекламе компании. Однако компании должны понимать это и осознавать важность анализа информации. Особенно в социальных сетях, и предлагать соответствующие решения по безопасности, чтобы избежать рисков. Нужно обращаться с социальными сетями, используя определенные политики и правильные технологии.

Многие хакеры рассматривают Интернет как публичное пространство для всех и не считают свои действия преступными. Компьютерная безопасность - обширная тема, которая становится все более важной, потому что мир становится все более взаимосвязанным. Новейшие и прорывные технологии, а также новые кибер-инструменты и угрозы, которые обнаруживаются каждый день, бросают вызов организациям не только в том, как они защищают свою инфраструктуру, но и в том, как им требуются новые платформы и разведки для этого. Все мы должны принимать определенные меры предосторожности при использовании Интернета, который поможет противостоять этой серьезной угрозе «Киберпреступность».

1. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны // Стратегия обороны., 2020. С. 148 – 160.
2. Чيو К., Фримэн Д. Машинное обучение и безопасность // Анализ вредоносного программного обеспечения., 2019. С. 145 – 202.
3. Коллинз М. Защита сетей. Подход на основе анализа данных // Сетевые сенсоры., 2019. С. 33 – 51.
4. Прутяну Э. Как стать хакером // Сетевая инженерия., 2020, С. – 120.

Умархаджиев М-Х.Р.

TinyML в IoT: Что в нем такого важного?

*ФГБОУ ВО Чеченский государственный университет им А.А.Кадырова
(Россия, Грозный)*

doi: 10.18411/trnio-12-2021-106

Аннотация

Быстрый рост миниатюризации маломощных встраиваемых устройств и прогресс в оптимизации алгоритмов машинного обучения, открыли новую перспективу Интернета вещей (IoT), крошечное машинное обучение (TinyML), которое требует реализации Алгоритм машинного обучения в устройстве IoT. Фреймворк TinyML в IoT нацелен на