kaspersky

Информационная безопасность

Учебное пособие для средней и старшей школы

kaspersky

Информационная безопасность

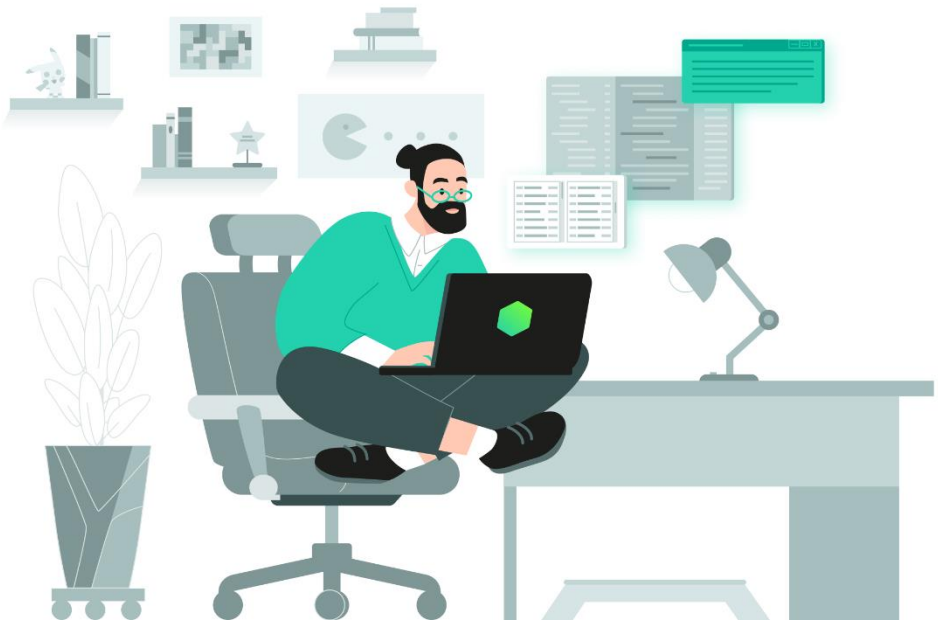
Аннотация

Учебное пособие «Информационная безопасность» предназначено для учащихся средней и старшей школы и рассчитано на формирование у них умений и знаний по обеспечению безопасности своего личного информационного пространства. А также будет актуальным и для учителей информатики, так как многие рассматриваемые темы включены в ФГОС. Учебное пособие может быть использовано в организации образовательного процесса в независимости от выбранного учебно-методического комплекса в учебном году.

В пособии рассматриваются основные аспекты информационной безопасности, такие как защита персональных данных, предотвращение кибератак, безопасное поведение в сети. Отдельные главы позволят учащимся познакомиться с фундаментальными основами криптографии и цифровой криминалистикой, что приведет к формированию понятийного аппарата о возможных карьерных путях в сфере информационной безопасности и дальнейшего выбора профессии.

Учебное пособие содержит понятные и доступные объяснения проблем информационной безопасности и конкретные примеры киберугроз.

В конце пособия приведены полезные ссылки на порталы, разработанные Лабораторией Касперского, и список используемой литературы, который будет полезен как для ознакомления учащимся, так и для учителей информатики.



kaspersky

Оглавление

kaspersky

Глава 1. Представление об информационной безопасности

§1. Понятие информационной безопасности

Ключевые слова: информационная безопасность, защита информации, инсайдеры, федеральный закон

На сегодняшний момент информационные технологии переживают активный рост в развитии, что влечет за собой как положительные, так и отрицательные стороны. То, что может облегчить рутинную работу конкретного человека, с другой стороны, сможет подвергнуть его какой-либо опасности, связанной с личной информацией. Поэтому актуальным является вопрос информационной безопасности.

Информационная безопасность – состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам).

В защите нуждаются государственная, военная, коммерческая, юридическая и врачебная тайны, помимо этого, все чаще возникают проблемы по защите своих личных данных, которыми мошенники могут пользоваться для проведения различных манипуляций (шантаж, вымогательства и т.д.).

Защита информации – это меры, направленные на то, чтобы не потерять информацию, не допустить ее искажения, не допустить, чтобы к ней получили доступ люди, не имеющие на это право.

То есть, информация будет считаться защищенной, если выполняются условия доступности, целостности и конфиденциальности. Нарушение безопасности информации в конечном итоге наносит ущерб ее собственнику.

Защитить информацию возможно различными методами и средствами:

- **Технические.** Защита помещения, где непосредственно находится та или иная информация (системы сигнализации, видеонаблюдение, надежные замки на входные группы).
- **Программные.** Защита информации за счет различного уровня ПО (личные аккаунты, шифрование данных, защита от вредоносного ПО).
- **Организационные.** Защита процесса работы с информацией и ее передача за счет политики безопасности организации.

В РФ вопросы, связанные с защитой информации, регулирует Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.06 №149-ФЗ.

Слабым звеном любой системы защиты является человеческий фактор. Некоторые пользователи могут небрежно хранить свои пароли и передавать их другим. Многие утечки информации в различных организациях связаны с инсайдерами – недобросовестными сотрудниками, которые распространяют информацию из секретного источника.

kaspersky

Вопросы к параграфу:

1. Что такое «информационная безопасность»?
2. Для чего необходимо защищать информацию?
3. Какими методами и средствами можно защитить информацию?
4. Как влияет человеческий фактор на защиту личного информационного пространства организации, в которой он работает?

Задание:

Ознакомьтесь с нормативным документом:

ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

§2. Необходимость в информационной безопасности

Ключевые слова: информационная безопасность, защита информации, конфиденциальность, целостность, доступность

Глобально информацию можно разделить на конфиденциальную и общедоступную. Но необходимость защиты информации не зависит от ее вида. Чаще всего мы слышим о защите конфиденциальных данных, к которым относятся персональные данные, коммерческие тайны, интеллектуальная собственность, профессиональная тайна, служебная тайна, государственная тайна и т.д. Каждая из этих категорий предъявляет разные требования к подходу и стандартам обеспечения информационной безопасности.

Информационная безопасность является актуальной при работе с информацией и ее хранением. И зачастую информация подвергается различным видам угроз, таких как вирусы, взломы, фишинг, кибершпионаж, утечки данных и т.д. Поэтому основное направление защиты информации – предотвращение несанкционированного доступа, сохранение целостности данных и обеспечение их доступности.

Три принципа информационной безопасности:

- Конфиденциальность: информация доступна только тем, кому это разрешено.
- Целостность: информация сохраняется в неизменном виде и доступна в полном объеме.
- Доступность: информация доступна тем, кто имеет на это право, в любое необходимое время.

Информационная безопасность является ключевым аспектом во многих сферах, таких как бизнес, медицина, финансы, государственные учреждения, личная информация. Защита финансовых данных, медицинских записей и критической инфраструктуры, как правило, требует особенного внимания и соблюдения наиболее строгих стандартов и протоколов.

Если посторонние каким-либо образом получат доступ к инфраструктуре организации, то ущерб можно минимизировать, если заранее продумать, какие активы могут интересовать злоумышленников в первую очередь, и приложить дополнительные усилия к их защите.

kaspersky

К основным направлениям, которыми интересуются злоумышленники, относятся:

- **Персональные данные.** Используются в качестве рычага давления для вымогательства. Помимо этого, в Интернете есть достаточно обширный рынок персональных данных – в некоторых случаях хакеры могут попробовать монетизировать их там.
- **Финансовые приложения.** Целый класс вредоносных программ служит для охоты на устройства, где установлены системы электронных платежей и прочие финансовые приложения. Это прямой доступ к деньгам компании и пользователей – одна успешная подмена адресата транзакции может обернуться катастрофой.
- **Пароли к различным аккаунтам.** Злоумышленникам не очень интересно добраться до одного устройства, зачастую они начинают охотиться за учетными данными для доступа к сетевым ресурсам, корпоративным сервисам или средствам удаленного доступа. Их могут интересовать доступы к рабочей почте и социальным сетям.
- **Резервные копии информации.** Такую информацию следует хранить на носителях, не подключенных к основной сети или же в специализированных облачных сервисах.
- **Среда разработки.** Если фирма занимается разработкой ПО, то рекомендуется обратить особое внимание на защиту среды разработки. Дело в том, что в наше время необязательно быть крупной компанией, чтобы стать жертвой целевой атаки. Достаточно делать приложение, которым пользуются крупные компании или большое количество пользователей. Преступники могут попробовать проникнуть в среду разработки и сделать компанию звеном в атаке через цепочку поставок. А методы в таких атаках, как правило, используются достаточно хитроумные.

В сфере информационной безопасности задействовано множество специалистов. А в зависимости от структуры организации и процессов работы с информацией могут возникать различные вопросы ее защиты и использования для этого разнообразных инструментов: антивирусы, файрволы, шифрование данных, системы контроля доступа, системы мониторинга и обнаружения вторжений, инструменты анализа угроз, менеджеры паролей, приложения по блокировке спам-звонков, приложения родительского контроля и т.д.

Конфиденциальность информационных ресурсов может быть подвергнута угрозам, таким как кибератаки, утечки данных, внутренние угрозы, социальная инженерия и другие. Защита от таких угроз требует комплексного подхода, включая технические, организационные и человеческие меры безопасности.

Информационная безопасность играет критическую роль в современном мире, обеспечивая защиту данных, сохранность частной жизни и устойчивость различных процессов. В условиях постоянно меняющихся и развивающихся угроз поддержание надежной системы информационной безопасности становится неотъемлемой частью успешной деятельности организаций и личной безопасности.

Вопросы к параграфу:

1. Существует ли необходимость защищать общедоступную информацию?
2. Какие существуют принципы информационной безопасности?
3. Почему злоумышленников интересуют персональные данные пользователей?
4. Какие инструменты ПО можно использовать для защиты личного информационного пространства?

Ситуация:

Вы является главным системным администратором крупной компании. Директор этой компании требует предоставить ему доступ ко всем информационным ресурсам – администраторские права к сайту, серверам и т.д. Какими будут ваши действия?

kaspersky

§3. История становления теории информационной безопасности

Ключевые слова: информационная безопасность, история, шифр, Энигма

Методы и средства защиты информации в каждую историческую эпоху тесно связаны с уровнем развития науки и техники. Категории защищаемой информации определялись экономическими, политическими и военными интересами государства.

Элементы защиты информации использовались с древнейших времён. Известно, что тайнопись применяли ещё в Древнем Египте и Древнем Риме. Классическим примером одного из первых применений криптографии является шифр Цезаря. Хотя, по большей части, защита передаваемой информации обеспечивалась контролем за самой процедурой обращения с секретной корреспонденцией.

С развитием почты стали возникать правительственные организации для перехвата, расшифровки, чтения и повторного запечатывания писем. А в военные времена защита информации несет первостепенную роль.

Во время Первой мировой войны системы шифрования использовались для защиты передаваемой информации всеми воюющими сторонами, что способствовало появлению и интенсивному использованию подразделений шифрования и криптоанализа.

В межвоенный период системы шифрования всё более усложнялись, для зашифровывания и расшифровки секретных сообщений стали использовать специальные машины, из которых наиболее известной является Энигма.

Объём информации, которой обменивались страны антигитлеровской коалиции в ходе Второй мировой войны потребовал формального согласования национальных систем классификации и процедур контроля и управления. Сформировался доступный лишь посвящённым набор грифов секретности, определяющих, кто может обращаться с документами и где их следует хранить. Воюющими сторонами были разработаны процедуры гарантированного уничтожения секретных документов. В Великобритании криптоанализом сообщений противника, зашифрованных с помощью Энигмы, успешно занималась группа под руководством А. Тьюринга. Разработанная ими машина для расшифровки оказала значительную помощь антигитлеровской коалиции.

Начиная с 90-х гг. XX в. исследованиями в области информационной безопасности активно занимаются российские ученые.

Как естественно-научная дисциплина теория информационной безопасности развивается в направлении формализации и использования математического аппарата в описании основных положений, выработки комплексных подходов к решению задач защиты информации.

Теория информационной безопасности постоянно претерпевает изменения, так как в связи с прогрессом технологий обработки и передачи информации возникают новые задачи по обеспечению информационной безопасности. Поэтому в настоящее время это одна из самых развивающихся естественных наук. Постоянно появляются новые перспективные направления исследований, а уже имеющиеся получают еще более глубокую научную проработку.

К числу перспективных направлений следует отнести следующие:

- Формализация положений теории информационной безопасности.
- Разработка моделей безопасности, более точно отражающих существующий уровень развития информационных технологий.
- Разработка средств и методов противодействия угрозам информационной войны.
- Вопросы обеспечения безопасности в глобальных информационных сетях.
- Вопросы безопасности обработки информации мобильными пользователями.

Особую роль в развитии теории информационной безопасности как науки и отрасли промышленности играют центры информационной безопасности. К ним относятся государственные, общественные и коммерческие организации, а также неформальные объединения, основные направления деятельности которых – координация усилий, направленных на актуализацию проблем защиты информации, проведение теоретических исследований и разработка конкретных практических решений в области безопасности, аналитическая деятельность и прогнозирование.

Приоритетными направлениями деятельности центров информационной безопасности являются:

- **Информационно-аналитическое.** Занимаются сбором и распространением информации об известных уязвимых местах систем, атаках и вторжениях, программных и аппаратных средствах профилактики и защиты. Регулярно публикуются и рассылаются аналитические обзоры, проводятся интернет-конференции, посвященные защите информации.
- **Оперативного реагирования.** Ключевым аспектом деятельности является оказание практической помощи.
- **Консультационное.** Оказание консалтинговых услуг организациям, испытывающим трудности с выбором или внедрением программных, аппаратных или комплексных мер защиты, разработкой политики безопасности или использованием нормативно-правовой базы, регламентирующей вопросы применения мер защиты.
- **Научно-исследовательское.** В таких случаях функционирование осуществляется на базе факультетов крупных учебных заведений или подразделений государственных организаций. Такие центры сосредоточены на изучении и совершенствовании теоретических основ информационной безопасности, исследовании и разработке моделей безопасных систем, синтезе и анализе защитных механизмов, совершенствовании законодательной базы.
- **Центры сертификации.** Реализуют программы тестирования, сравнения и сертификации средств защиты, а также разрабатывают подходы к сертификации и методики тестирования.

Вопросы к параграфу:

1. Как вы считаете, что является стимулом для развития методов информационной безопасности?
2. Почему теория информационной безопасности развивается в направлении использования математического аппарата?
3. Для чего необходимы центры информационной безопасности?

Задание:

Посмотрите фильм «Игра в имитацию», 2014г.

Биографический фильм о криптографе военного времени Алане Тьюринге.

kaspersky

§4. Карьера в сфере информационной безопасности

Ключевые слова: специальность, образование, аналитика, цифровая криминалистика, форензика, спам, контент, вредоносное ПО

На сегодняшний момент работа в IT-сфере становится все более привлекательной. Но на вопрос «кем работать в этой сфере?» ответ «программистом» является очень размытым, так как такая формулировка не дает никакой конкретики. В силу того, что IT-технологии находятся в постоянном развитии, то конкретная профессия в этой сфере строится не только на базовых знаниях, но и на специфических знаниях конкретной отрасли (языки программирования, архитектура компьютера, администрирование ОС и т.д.).

Мировой рынок труда давно испытывает нехватку специалистов в области кибербезопасности. Зачастую компании, которые сталкиваются с необходимостью найма специалистов по информационной безопасности, не могут найти достаточно экспертов с профильным образованием и нужным опытом. Для того, чтобы понять, насколько для обеспечения безопасности компании важно наличие у сотрудников формального образования в этой области и насколько такое образование отвечает современным потребностям рынка, Лаборатория Касперского собрала статистику у более 1000 человек из 29 стран различных регионов мира. Среди опрошенных специалисты разного уровня. По ответам респондентов становится понятно, что классическое образование не успевает за трендами информационных технологий, в частности информационной безопасности.

Во-первых, далеко не все специалисты имеют высшее образование. Но даже из тех, кто его имеет, каждый второй сомневается в том, что их формальное образование реально помогает выполнять должностные обязанности. Дело в том, что кибербезопасность – быстро меняющаяся отрасль. Ландшафт угроз меняется настолько стремительно, что даже отставание в пару месяцев может быть критично, не говоря уж о четырех-пяти годах, которые могут уйти на получение ученого звания. За это время злоумышленники могут модернизировать свои тактики и методы таким образом, что начинающему специалисту по информационной безопасности в случае реальной атаки придется спешно читать свежие статьи об угрозах и методах защиты.

Зачастую учебные заведения не предоставляют достаточно практических знаний, не имеют доступа к современным технологиям и оборудованию, да и в целом для работы и борьбы с реальными киберугрозами требуется дополнительное образование.

Это все, разумеется, не означает, что кибербезопасники с профессиональным или высшим образованием менее компетентны, чем их коллеги со школьными аттестатами. В конечном итоге важнейшую роль в профессиональном развитии играет энтузиазм и способность постоянно развиваться. Многие опрошенные отметили, что получили в традиционных учебных заведениях скорее теоретические знания, нежели практические. Этим и полезно академическое образование, потому что без должной теоретической базы обучение может продвигаться медленнее. С другой стороны, специалисты, не имеющие послешкольного образования вообще или пришедшие в информационную безопасность из другой IT-отрасли, точно так же могут стать эффективными специалистами по защите от киберугроз.

Рассмотрим некоторые направления рабочих специальностей в сфере информационной безопасности:

- **Вирусный аналитик.** Это специалист, который занимается анализом программного кода или ПО с целью обнаружения вредоносного кода, его анализа и борьбы с ними. К основным функциям вирусного аналитика относится: обнаружение вирусов, анализ вредоносного кода, разработка сигнатур, разработка методов защиты, исследование новых угроз.
- **Аналитик киберугроз.** Это направление в кибербезопасности, которое фокусируется на структурированном сборе, анализе и распространении данных о потенциальных или существующих киберугрозах, что дает организациям информацию, необходимую для прогнозирования,

предотвращения кибератак и реагирования на них, благодаря пониманию поведения участников угроз, их тактики и уязвимостей, которые они используют. В последние годы аналитика угроз стала важной частью стратегии компаний в области кибербезопасности, поскольку она позволяет компаниям применять более упреждающий подход и определять, какие угрозы представляют наибольший риск для бизнеса, что позволяет им действовать на опережение.

- **Спам аналитик.** Это специалист, который занимается подготовкой данных для линейки антиспам-продуктов. Он анализирует структурный и тематический состав спама, выявляет новые спамерские трюки и тенденции, разрабатывает способы борьбы с новыми видами спама.
- **Контент аналитик.** Это эксперт, который изучает и оценивает различные формы контента, такие как статьи, посты в блогах, контент социальных сетей, видео и копии веб-сайтов. Их основная цель – понять, насколько эффективно контент достигает определенных результатов. В частности, в сфере информационной безопасности, специалисты этой области анализируют контент на наличие нарушений безопасности пользователей в сети.
- **Тестировщик ПО.** Это специалист, который помогает делать продукты (приложения, сайты, программы) такими, чтобы ими можно было пользоваться. Тестировщики определяют, какие элементы системы функционируют некорректно или не так удобны, как хотелось бы, находят причины этого (ошибки в коде, дизайне или логике) и отдают на исправление. Все это делается для того, чтобы конечные пользователи получили стабильный, надежный и удобный продукт.
- **SOC (Security Operations Center) аналитик.** Отвечает за мониторинг и анализ сетевых событий, выявление киберугроз и реагирование на инциденты безопасности. В его задачи входит отслеживание подозрительной активности в реальном времени, анализ журналов безопасности, использование специализированных инструментов для идентификации и устранения угроз. В работе такие специалисты используют SIEM (Security Information and Event Management) системы для сбора и анализа данных, инструменты для поиска уязвимостей, а также средства для реагирования на инциденты. Одним из ключевых аспектов работы является постоянная бдительность и быстрая реакция на возникающие угрозы.
- **Pentest специалист.** Это тестировщики на проникновение. Цель пентестера – понять, может ли гипотетический злоумышленник взломать систему. Для этого тестировщики сами пытаются ее взломать или получить контроль над данными. Пентестинг проводится на физическом и программном уровнях. Основная задача — проникнуть в систему или сеть, получить контроль над устройством или ПО, собрать информацию. Конкретные действия зависят от того, что именно тестируется.
- **Detection инженер.** Это эксперт в области кибербезопасности, который разрабатывает системы и процессы для обнаружения вредоносной активности и поведения. В рамках своей работы Detection инженеры пишут правила обнаружения в различных продуктах безопасности для выявления киберугроз в системах, настраивают и поддерживают структуры, которые генерируют сигналы безопасности, отслеживают информацию об угрозах, необходимую для обнаружения кибератак, и используют эту информацию для укрепления механизмов киберзащиты.
- **Threat Hunting специалист.** Это специалист, занимающийся проактивным поиском следов взлома или функционирования вредоносного ПО, которое не обнаружено стандартными средствами защиты.
- **Цифровой криминалист.** Это специалист, который занимается анализом и расследованием событий кибербезопасности, поиском доказательств совершения преступлений в цифровой среде. Перед экспертом в этой области стоят задачи по восстановлению хронологии инцидентов, сбора и изучения следов киберпреступлений, подготовки отчётов и официальных заключений. Цифровая (компьютерная) криминалистика еще называется **форензикой** – является прикладной наукой о раскрытии и расследовании преступлений, связанных с компьютерной информацией, о методах получения и исследования доказательств, имеющих форму компьютерной информации (так называемых цифровых доказательств), о применяемых для этого технических средствах. Предметами форензики являются: криминальная практика – способы, инструменты совершения соответствующих преступлений, их последствия, оставляемые следы, личность преступника; оперативная, следственная и судебная практика по компьютерным преступлениям; методы экспертного исследования компьютерной информации и, в частности, ПО; достижения отраслей связи и информационных технологий, их влияние на общество, а также возможности их использования как для совершения преступлений, так и для их предотвращения и раскрытия.

kaspersky

Задание:

1. Проведите анализ открытых вакансий на специалистов в области информационной безопасности.
2. Сформулируйте ключевые требования к таким специалистам.

§5. Аутентификации

Ключевые слова: аутентификация, однофакторная аутентификация, двухфакторная аутентификация, пароль, токен, биометрия, одноразовый код, SMS

Аутентификация – это процесс определения, является ли кто-то (или что-то) тем, за кого пытается себя выдать. В контексте IT-процессов это значит, что учетные данные, предоставленные лицом, запрашивающим доступ к ресурсу, сравниваются с данными, имеющимися у ресурса. Если информация совпадает, пользователю предоставляется доступ.

Процедура аутентификации может строиться на основе того, что вы знаете (пароль), что у вас есть (токен) или кем вы являетесь (биометрические данные). Методы могут быть объединены, чтобы обеспечить более высокий уровень безопасности – двухфакторную или многофакторную аутентификацию.

При однофакторной аутентификации необходимо указать только один вид авторизационных данных, например, имя и пароль. Такой способ менее надежен по сравнению с двухфакторной аутентификацией, требующей ввода дополнительных сведений или выполнения подтверждающих действий на других устройствах.

Метод двухфакторной аутентификации заключается в использовании информации из двух источников для идентификации личности. При этом обычный пароль «объединяется» с внешним устройством проверки подлинности, например с аппаратным токеном, который генерирует случайный одноразовый пароль, со смарт-картой, SMS-сообщением (где мобильный телефон является токеном) или уникальным физическим атрибутом, например, отпечатком пальца.

Чаще всего цифровые сервисы работают с двухфакторной аутентификацией. На сегодняшний момент двухфакторная аутентификация обеспечивает оптимальный баланс между надежностью защиты аккаунта и удобством входа в него.

К наиболее популярным вариантам факторов, подтверждающих право пользователя, относятся:

- **Знание.** Аутентификация возможна, если вы знаете пароль, секретную фразу, цифровой код, графический паттерн, ответ на секретный вопрос и так далее.
- **Обладание.** Если у вас есть некий предмет (USB-токен, телефон, банковская карта), который является подтверждением вашего права доступа.
- **Неотъемлемое свойство.** Также часто есть возможность аутентифицироваться по какому-то неотъемлемому и достаточно уникальному свойству самого пользователя – отпечатку пальца, голосу, лицу, ДНК, рисунку радужной оболочки, характерной манере печати на клавиатуре и так далее.
- **Местоположение.** В этом варианте подтверждением права на доступ является факт нахождения пользователя в каком-то определенном месте – например, если речь идет о корпоративных ресурсах, внутри офиса компании.

Важно понимать, что для многофакторной аутентификации методы, которыми пользователь подтверждает свои права, должны быть действительно разными. То есть в том случае, если некий сервис просит

пользователя вводить два пароля, а не один (или, например, пароль и ответ на секретный вопрос), это нельзя считать двухфакторной аутентификацией, поскольку тут дважды использован один и тот же метод подтверждения прав – знание некой информации.

Многофакторную аутентификацию используют, потому что по отдельности все методы подтверждения права доступа имеют те или иные изъяны. Скажем, знание некой информации могло бы быть действительно надежным способом подтверждения лишь в том случае, если эта информация известна только самому пользователю и не может быть получена из каких-то других источников.

Это отлично работало бы в идеальном мире, но в реальности все гораздо менее радужно. Скажем, тот же пароль пользователю приходится набирать на клавиатуре, передавать через Интернет и, вероятно, каким-то образом хранить. Это дает массу возможностей для перехвата и кражи. Кроме того, этот же пароль обязательно будет храниться на стороне сервиса, и рано или поздно он оттуда может утечь.

Пожалуй, только неотъемлемое свойство можно считать более-менее надежным вариантом – и поэтому иногда его действительно используют в качестве единственного фактора аутентификации.

Из этого и вытекает основная идея многофакторной аутентификации: чем больше разных факторов используется одновременно, тем больше вероятность, что доступ к аккаунту пытается получить человек, который действительно имеет на это право.

Таким образом, ответ на вопрос «зачем нужна многофакторная аутентификация?» – это чтобы сервис мог уверенно понимать, что вы – это вы, и благодаря этому аккаунт было труднее украсть.

Рассмотрим популярные виды двухфакторной аутентификации:

- **Одноразовые коды из SMS, на электронную почту или голосом по телефону.** Один из наиболее распространенных вариантов двухфакторной аутентификации – это отправка одноразового кода для подтверждения входа. Чаще всего такие одноразовые коды отправляют в текстовом сообщении на указанный при регистрации номер телефона. Несколько реже для тех же целей используется электронная почта. В крупных сервисах обычно также предусмотрена возможность получить такой код голосовым звонком на все тот же указанный при регистрации телефон. Куда бы ни приходил код, основная идея остается неизменной: проверка возможности получить доступ к какому-то другому аккаунту или номеру телефона, который был указан при регистрации. И если пароль был утерян или украден мошенниками, но нет доступа к вашему телефону, то такая защита вполне сработает.
- **Пароль.** Иногда пароль становится вторым фактором, а не первым. Это часто практикуют мессенджеры: по умолчанию для регистрации в сервисе обмена сообщениями обычно достаточно ввести только одноразовый код, который отправляется по SMS. Поэтому недостаток аутентификации такого вида заключается в смене основного телефонного номера.
- **Одноразовый код из заранее сгенерированного списка.** Зачастую такие списки выдают своим клиентам банки для подтверждения транзакций, а некоторые интернет-сервисы (например, Google) позволяют применять их для восстановления доступа к аккаунту. Этот вариант можно считать надежным, так как такие коды передаются пользователю крайне редко, поэтому возможностей для перехвата минимум. Коды создаются случайными, то есть они уникальны и угадать их едва ли получится. Однако возникает проблема хранения: если преступник сможет каким-то образом выкрасть этот список, то далее заранее сгенерированные коды будет легко использовать для угона учетной записи или кражи денег со счета. Главное неудобство этого способа аутентификации состоит в том, что если часто необходимо что-то подтверждать, то списки заранее сгенерированных кодов быстро заканчиваются. В результате придется постоянно создавать и сохранять новые. И если речь идет о множестве аккаунтов, то в этом массиве списков будет легко запутаться. Поэтому заранее сгенерированным кодам, как основному методу аутентификации, пришли на смену коды, генерируемые «по требованию» – в тот момент, когда этот код нужен пользователю.
- **Одноразовые коды из приложения-аутентификатора.** Генерацией одноразовых кодов занимаются специальные приложения-аутентификаторы, которые устанавливаются на смартфон. Такие приложения предлагают оптимальный баланс между удобством и безопасностью, поэтому они приобретают все большую популярность.

- **Биометрия.** В большинстве смартфонов сейчас есть возможность аутентификации либо по отпечатку пальца, либо с помощью распознавания лица, и это уже давно никого не удивляет. Из более специфичных вариантов биометрии можно отметить аутентификацию с помощью голоса, рисунка радужной оболочки глаза. У биометрической аутентификации есть пара серьезных недостатков. Любые используемые для нее характеристики пользователя являются его постоянными свойствами. Пароль в случае утечки легко поменять, а вот сменить зарегистрированный отпечаток пальца получится лишь ограниченное число раз. Вторая важная проблема состоит в том, что биометрические данные являются крайне чувствительной информацией – как из-за своей неизменности, так и потому, что позволяют не только аутентифицировать пользователя, но и идентифицировать человека. Так что к сбору и передаче этих данных цифровым сервисам стоит относиться крайне осторожно. По этой причине биометрические данные обычно используются для локальной аутентификации – они хранятся и обрабатываются прямо на устройстве, так, чтобы не приходилось кому-то их передавать. Полноценно работающий механизм дистанционной биометрической аутентификации есть только у компании Apple, которая полностью контролирует свою экосистему, от разработки ПО до производства устройств.
- **Местоположение.** Обычно эта проверка происходит незаметно, и о ее результатах человек узнает только в том случае, если она оказывается неуспешной. В этом случае сервис может попросить дополнительно подтвердить вход каким-то другим способом. Этот способ аутентификации не нужно подключать самому, он работает по умолчанию. Конечно же, местоположение является не очень надежным способом проверки аутентичности пользователя, так как оно не слишком уникально, да и его достаточно легко подделать (если речь идет об определении местоположения по IP-адресу, а не о полноценной геолокации по GPS).

Вопросы к параграфу:

1. Что такое аутентификация?
2. Как строится процедура аутентификации?
3. Какие виды многофакторной аутентификации вам известны?
4. Каким видом двухфакторной аутентификации пользуетесь лично вы?

Задание:

1. Составьте сравнительную таблицу положительных и отрицательных сторон популярных видов двухфакторной аутентификации.
2. Подготовьте информацию об использовании аппаратных ключей FIDO U2F в качестве двухфакторной аутентификации.
3. Проанализируйте возможности приложений по генерации надежных паролей и их хранению.

Ситуация:

На ваш смартфон приходит SMS с одноразовым паролем для входа в аккаунт распространенной социальной сети. Какими будут ваши действия?

kaspersky

§6. Надёжность пароля

Ключевые слова: пароль, аутентификация, эмодзи, стандарт аутентификации и контроль цифровых аккаунтов

Пароль – условное слово или произвольный набор знаков, состоящий из букв, цифр и других символов и предназначенный для подтверждения личности или полномочий. Пароли используются для защиты информации от несанкционированного доступа.

Исследования показывают, что около 40% всех пользователей выбирают пароли, которые легко угадать автоматически. Пароли, которые очень трудно или почти невозможно угадать, считаются более стойкими.

В 2013 году компания Google опубликовала список широко используемых категорий паролей, которые считаются ненадёжными из-за того, что их легко подобрать (особенно после изучения профиля пользователя в социальной сети): кличка домашнего животного, имя родственника, даты рождения и важных событий, место рождения, что-либо, связанное с любимой спортивной командой, слово «password».

Надежность пароля – это показатель эффективности пароля против угадывания или атак методом перебора. Осуществляется оценка количества попыток, которые потребуются злоумышленникам, не имеющим прямого доступа к паролю, чтобы правильно его подобрать. Надежность пароля зависит от длины, сложности и непредсказуемости.

Эффективность пароля заданной надежности в значительной степени определяется конструкцией и реализацией факторов аутентификации. Скорость, с которой злоумышленник может передавать системе угаданные пароли, является ключевым фактором в определении безопасности системы. Некоторые системы вводят тайм-аут продолжительностью в несколько секунд после небольшого количества неудачных попыток ввода пароля.

К паролям есть два требования, которые могут показаться несовместимыми. С одной стороны, чтобы надежно защитить учетную запись, нужно придумать пароль, который будет трудно подобрать. С другой стороны, этот пароль должно быть легко запомнить, иначе им невозможно будет пользоваться. Регулярная смена паролей отчасти помогает с первым требованием, но второе делает трудновыполнимым. Но, на самом деле, постоянно менять пароли не так уж эффективно. Гораздо лучше использовать надежные и уникальные комбинации символов.

Утечки данных случаются регулярно, и пароли попадают в руки злоумышленников – как пользователь вы ничего не можете с этим поделать. Если же везде используется один и тот же пароль, то всего одна утечка – и все личные аккаунты будут под угрозой.

Каким должен быть пароль, чтобы его можно было назвать «надежным»? Принципиально важны два простых правила. Во-первых, в нем нужно использовать как можно более разнообразные символы. Во-вторых, пароль должен быть длинным – и чем длиннее, тем лучше.

Надежный пароль вовсе не должен быть случайным набором символов. Случайные комбинации, несомненно, хороши с точки зрения безопасности, но запоминать их – проблема. Лучше придумать легко запоминающийся пароль, минимум 12 символов.

К примеру, пароли

12345-vyshel-zaychik-naprimer

?Y]G9gWJ48zYkFBc@{nKw!'q

обладают близкой надежностью, так как первый пароль компенсирует все свои недостатки большей длиной.

kaspersky

Некоторые сайты, сервисы и приложения поддерживают возможность использования эмодзи при создании пароля как альтернативу классическим символам. Эмодзи очень много, поэтому пароль может быть вдвое короче. И когда злоумышленники пытаются подобрать пароль из букв, цифр и знаков пунктуации, для каждого символа пароля им нужно перепробовать менее сотни вариантов. Но стандартизованных эмодзи в Unicode более 3600, и, если в пароль добавить смайлик, то для каждого знака придется перебрать уже около 3700 вариантов. Так что по сложности подбора пароль из пяти разных смайлов эквивалентен обычному паролю из девяти символов. Да и многие злоумышленники не учитывают, что пароль вообще может содержать эмодзи. Пользователю же эмодзи проще запоминать, чем бессмысленную мешанину букв и цифр.

Говоря о минусах использования эмодзи в паролях, следует отметить, что не все сервисы принимают пароли с эмодзи. Если говорить о конкретных гаджетах, где необходимо вводить такой пароль, то на смартфонах ввести эмодзи очень просто, а вот на настольных компьютерах с этим могут возникнуть небольшие сложности. Да и недавние эмодзи выдают секрет. На многих клавиатурах смартфонов часто используемые эмодзи выводятся в начале списка. Для хакеров из Интернета эта информация вряд ли полезна, а вот знакомые или родственники вполне могут угадать или подсмотреть ваш пароль.

Многие считают, что киберпреступники смогут заполучить пароль, только если пользователь совершит ошибку – скачает и запустит непроверенный файл, откроет документ от неизвестного отправителя или введет свои учетные данные на сомнительном сайте. Да, все это действительно упрощает жизнь злоумышленникам, но на самом деле в их арсенале гораздо больше способов для захвата учетных записей.

Самые распространенные схемы:

- **Вредоносное ПО.** Существенную часть активных зловредов составляют трояны-стилеры. Они ждут, когда пользователь зайдет на какой-нибудь сайт или сервис, копируют введенный им пароль и отправляют своему владельцу. Если не пользоваться защитными решениями, то такие трояны могут годами скрываться в системе. Их трудно заметить, поскольку они тихо занимаются своим делом, не причиняя видимого вреда. Иногда киберпреступники внедряют в сайты веб-скиммеры, которые собирают всю информацию, вводимую пользователями (имена, данные учетных записей и банковских карт и т.д.).
- **Публичный Wi-Fi.** Злоумышленники могут перехватить данные (в том числе пароли), отправляемые по сети, если использовать сеть Wi-Fi без шифрования или защищенную старым протоколом WEP. Другой вариант кражи: хакер создает точку Wi-Fi с открытым доступом, используя название, похожее на существующую сеть. Не замечая разницы, пользователи подключаются к фальшивой точке – и весь их интернет-трафик оказывается под контролем злоумышленника. Избежать таких утечек можно, если внимательно проверять названия сетей, не пользоваться сомнительными точками доступа и не позволять устройствам подключаться к беспроводным сетям автоматически.
- **Фишинговое письмо.** Это один из тех подходов к краже чужих учетных данных, которые действительно рассчитаны на ошибку пользователя. В сети ежедневно появляются сотни фишинговых сайтов и тысячи рассылок, призванных заманить туда будущих жертв. У киберпреступников была масса времени, чтобы изобрести множество уловок, основанных на социальной инженерии, и трюков, позволяющих им мимикрировать под легитимных отправителей.
- **Уязвимость браузера.** Нередко пароли крадут через уязвимости браузеров или через браузерные расширения. В первом случае специально созданный вредоносный код на веб-странице позволяет подсадить шпиона. А во втором случае пользователь самостоятельно устанавливает себе шпионский скрипт под видом полезного браузерного плагина или расширения. После этого, когда пользователь заходит, например, на сайт банка, этот скрипт будет перенаправлять трафик через хакерский прокси-сервер и таким образом «сливать» учетные данные.
- **Пароли где попало.** Многие до сих пор записывают пароли на стикерах и других бумажках, оставляя в местах, где их легко может увидеть посторонний. Не менее опасно записывать пароли в незащищенных текстовых файлах на своем компьютере или смартфоне, а также не рекомендуется сохранять пароли в браузере для автоматической подстановки.
- **Внешние утечки.** Все, что сказано выше, касается потери пароля на пользовательской стороне. Но утечки часто происходят и в удаленных интернет-сервисах. Это может быть интернет-магазин, социальная сеть, криптобиржа или любой другой ресурс, где при входе используется

аутентификация. В результате взлома такого сайта хакеры могут получить огромную базу пользователей вместе с их паролями и другими персональными данными. При этом владельцы сайтов не всегда спешат сообщать о таких взломах. А злоумышленники тем временем обмениваются украденными базами или выставляют их на продажу в дарквебе. Специалисты по безопасности отслеживают публикации таких баз и предупреждают пользователей. Правда, иногда под видом таких специалистов высока вероятность наткнуться на мошенников.

В 2024 году вышел новый стандарт NIST SP 800-63 аутентификации и контроля цифровых аккаунтов. В документе описаны новые требования к паролям:

- Запрещены пароли короче 8 символов, рекомендованный минимум – 15 символов.
- Запрещено использовать в парольной политике требование регулярно менять пароли по графику, это признано устаревшей практикой.
- Запрещено предъявлять требования к составу пароля («ваш пароль должен содержать букву, цифру и значок»).
- Рекомендовано разрешить к применению в паролях любые видимые значки ASCII, пробелы и большинство символов Unicode (смайлики и прочее).
- Ограничение на максимальную длину пароля, если оно установлено, должно быть хотя бы 64 символа.
- Запрещено обрезать пароли при проверке, но разрешается убирать пробелы в начале и конце пароля, если они могут помешать успешной аутентификации.
- Запрещено использовать и хранить в системах подсказки к паролям, а также «проверочные вопросы».
- Обязательно предотвращать установку часто используемых паролей, то есть иметь стоп-лист популярных паролей или паролей из утечек.
- При обнаружении компрометации паролей (например, появление пароля в утечках) их нужно немедленно сбрасывать.
- При вводе паролей обязательно ограничивать частоту попыток ввода и число неудачных попыток.

Для обычных пользователей к общим рекомендациям по выбору и использованию надежного пароля можно отнести:

- Не используйте один и тот же пароль для нескольких учетных записей.
- Создавайте длинные и надежные пароли.
- Храните пароли в защищенном месте.
- Если имеется информация об утечке данных из сервисов или с сайтов, которыми пользуетесь, то сразу же меняйте пароль для доступа к ним.
- Пользуйтесь менеджером паролей.
- Используйте двухфакторную аутентификацию везде, где она доступна.

Вопросы к параграфу:

1. Что такое пароль?
2. Какой пароль можно назвать надёжным?
3. В чём преимущество и недостатки использования эмодзи в создании пароля?
4. Какие распространенные мошеннические схемы по краже пароля вам известны?

Задание:

1. Проанализируйте данные пароли:
   123456789QQ
   qwerty1239
   Iklad78!q@14STT
   paRoLL2024@@
   LOL123456789$QWERTY
   Sgu_12$WXLPt_2025
   Какие вы считаете надежными, а какие нет? Ответ обоснуйте. Проверку паролей можно осуществить через сервис: https://password.kaspersky.com/ru/
2. Разработайте алгоритм по генерации надежного пароля. Проверку результатов можно осуществить через сервис: https://password.kaspersky.com/ru/

Ситуация:

Приложение менеджер-паролей показывает уведомление, что пароль от учетной записи числится украденным. Какими будут ваши действия?

§7. Мессенджеры

Ключевые слова: мессенджеры, e-mail, Telegram, WhatsApp, двухфакторная аутентификация

Мессенджер – это ПО для мгновенного обмена сообщениями и файлами различного формата (изображениями, видео и аудио) через сеть. На сегодняшний момент многие мессенджеры дают возможность осуществлять коммуникацию между двумя и более собеседниками.

В отличие от электронной почты, мессенджеры не разделяют коммуникацию на отдельные письма, а предоставляют пользователям возможность общаться друг с другом в формате последовательного живого диалога. Чат как форма общения в мессенджерах аналогичен традиционным чатам на веб-страницах или в других приложениях, существовавшим на ранних этапах развития Интернета. Однако каждый мессенджер предоставляет собственные возможности для работы.

В настоящий момент одними из популярных мессенджеров в нашей стране являются Telegram и WhatsApp. Рассмотрим использование данных мессенджеров со стороны основного функционала и политики информационной безопасности.

WhatsApp по-прежнему остается самым популярным мессенджером в мире. При этом, он один из самых безопасных – вся переписка в нем защищена сквозным шифрованием. Signal Protocol.

Заметим, что это открытый протокол, так что любой желающий (при наличии соответствующих знаний и навыков) может изучить его исходный код на предмет ошибок или бэкдоров.

На практике это означает, что все текстовые и голосовые сообщения (причем как в личной переписке, так и в групповых чатах), изображения, видео и другие документы, а также звонки шифруются на устройстве отправителя и расшифровываются только на устройстве получателя.

Использование сквозного шифрования для всех сообщений выгодно отличает WhatsApp от Telegram. Несмотря на то, что последний позиционируется как безопасный мессенджер, сквозное шифрование в нем по умолчанию не включено. Оно используется только в секретных чатах, которые надо специально создавать. Если вы вели в Telegram конфиденциальную переписку без использования секретных чатов, считайте ее скомпрометированной.

На практике мало кто знает, как устроена серверная часть Telegram, но известно, что основная часть переписки хранится на серверах в минимально зашифрованном виде, то есть ключи для расшифровки хранятся в той же инфраструктуре Telegram. Создатели заявляют, что чаты хранятся в одной стране, а ключи их расшифровки – в другой, но насколько серьезно это препятствие на практике, учитывая, что все серверы постоянно коммуницируют друг с другом, – не очевидно.

Стандартное для других мессенджеров (WhatsApp, Signal, Viber) сквозное шифрование называется в Telegram «секретным чатом», его довольно трудно найти в глубинах интерфейса, и оно доступно только для ручной активации в индивидуальной переписке. Все групповые чаты, все каналы, а также стандартная личная переписка лишены сквозного шифрования и могут быть прочитаны как минимум на серверах Telegram.

Telegram использует как для секретных чатов, так и для всего остального свой собственный не стандартный протокол MTProto, в котором не раз находили серьезные криптографические уязвимости.

Не всем хватает стандартных функций официальных приложений WhatsApp и Telegram: кому-то нужны дополнительные возможности кастомизации интерфейса или что-то специфическое (скрывать чаты, автоматически переводить сообщения, просматривать удаленные собеседником сообщения и т.д.). На помощь пользователям приходят приложения от сторонних разработчиков – модификации или моды мессенджеров. Таких модификаций существует огромное количество.

Проблема в том, что, устанавливая такое приложение, пользователям приходится доверять свою переписку не только оригинальным разработчикам мессенджера, но и третьим лицам. Во-первых, разработчикам модов, которые нередко прячут в них какие-то зловредные модули, а во-вторых, их распространителям, так как они способны добавить в код программы что-то от себя.

Если говорить о защите личного аккаунта в мессенджерах, то первое, что следует сделать – защитить аккаунт от угона. В мессенджере учетные записи привязаны к телефонным номерам, соответственно, если кто-то завладеет номером, то он сможет войти и в личный аккаунт мессенджера. Это может произойти намеренно, в ходе атаки с подменой SIM-карты. Чтобы защититься от этой угрозы, следует включить двухфакторную аутентификацию.

Помимо этого, в настройках конфиденциальности мессенджера имеются пункты, которые позволяют настроить, кому будет доступна та или иная информация о пользователе. Следует продумать, каким пользователям будет отображаться та или иная личная информация о владельце аккаунта.

Пользуйтесь официальными версиями мессенджеров, устанавливая их из официальных источников.

Вопросы к параграфу:

1. Что такое мессенджер?
2. В чем преимущества использования мессенджера в сравнении с электронной почтой?
3. Для чего необходима функция шифрования передаваемых данных у мессенджеров?
4. Для чего необходимы моды мессенджеров?

kaspersky

Задание: Сделайте сравнительный анализ количества пользователей, географии использования и функционала востребованных мессенджеров: Telegram, WhatsApp, Signal, Viber, Snapchat.

§8. Браузеры

Ключевые слова: браузер, расширения, пароль, стилеры, обновление ПО, режим инкогнито, куки-файлы

Браузер – прикладное ПО для просмотра страниц, содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями; а также для решения других задач. В глобальной сети браузеры используют для запроса, обработки, манипулирования и отображения содержания веб-сайтов.

Многие современные браузеры также могут использоваться для непосредственного просмотра содержания файлов многих графических форматов, аудио- и видеоформатов, текстовых форматов и других файлов. Функциональные возможности браузеров постоянно расширяются и улучшаются благодаря конкуренции между их разработчиками и высоким темпам развития и внедрения информационных технологий.

Браузеры распространяются, как правило, бесплатно. Потребителям браузер может быть поставлен в форме самостоятельного приложения или в составе комплектного ПО.

К примеру, браузеры Internet Explorer и Microsoft Edge поставляются в составе ОС Microsoft Windows; Mozilla Firefox – отдельно или в составе дистрибутивов Linux; Safari – в составе Mac OS; Google Chrome, Opera и другие браузеры – самостоятельные приложения во множестве вариантов для различных ОС.

Зачастую браузеры имеют различные расширения – компьютерные программы, которые расширяют функциональные возможности браузера. Например, с их помощью на отображаемых веб-страницах можно блокировать рекламу, проверять орфографию, делать заметки и многое другое.

Для популярных браузеров существуют официальные магазины расширений, которые помогают выбрать, сравнить и установить интересующие плагины. Но можно устанавливать расширения также из сторонних источников.

Возникает вопрос, насколько безопасно пользоваться браузером и его расширениями?

Одно из распространенных расширений браузеров – **хранение логинов и паролей** от учетных записей пользователя.

Главная проблема хранения паролей в браузерах в том, что браузеры приносят безопасность в жертву удобству использования. Это справедливо как минимум для тройки самых популярных браузеров, которые использует подавляющее большинство людей: Google Chrome, Mozilla Firefox и Microsoft Edge – эти браузеры хранят пароли пользователя крайне небезопасно.

Все браузеры записывают пароли в очень предсказуемом месте – в папке, путь до которой всем прекрасно известен. И хотя пароли зашифрованы, недалеко от них хранится и ключ шифрования, доступ к которому может получить кто угодно. Используя этот ключ, пароли можно расшифровать и украсть. Получается смешная ситуация: дверь вроде бы достаточно надежно заперта, вот только ключ лежит под половичком, и все об этом прекрасно знают.

Этим фактом пользуются и сами браузеры для конкуренции друг с другом: чтобы упростить пользователю переход от использования одного браузера к другому, они часто предлагают импортировать все его сохраненные данные из старого браузера (включая и запомненные этим старым браузером пароли).

Целый класс вредоносного ПО используют данную особенность работы браузеров, который называется стилерами и специализируется на поиске и краже учетных данных. Такие зловреды анализируют хорошо известные папки, в которых лежат сохраненные браузером пользовательские пароли, ищут ключи шифрования и расшифровывают пароли. После этого загружают все найденное на сервер злоумышленников. Дальше эти пароли обычно собирают в базу и оптом продают в даркнете, а уже какие-нибудь другие жулики используют их для угона аккаунтов.

То же самое может проделать не только специальное вредоносное ПО, но и любой человек, получивший физический доступ к чужому компьютеру. Великим хакером для этого быть необязательно – скрипты, необходимые для извлечения паролей из браузера, можно без особых проблем найти в Интернете, останется лишь их запустить.

Еще один из функционалов браузеров – **режим инкогнито**. Этот режим есть во всех популярных браузерах, хотя называется по-разному: в Chrome – Incognito, в Edge – InPrivate, в Firefox – Private Window/Tab, в Safari – Private Browsing. Все эти названия создают чувство защищенности, даже невидимости. Кажется, что можно бродить по Интернету безопасно и анонимно. Увы, на практике этот режим далеко не «инкогнито», хотя все равно полезен, если понимать его особенности и дополнить защитой.

В приватном режиме браузер не сохраняет историю посещенных сайтов, не запоминает информацию, вводимую на сайтах в веб-формах, не сохраняет на диске компьютера графику и код посещаемых веб-страниц в браузерном кэше. Маленькие текстовые файлы куки (cookie), в которых сайты сохраняют настройки и предпочтения пользователя, хранятся до тех пор, пока открыто окно в режиме инкогнито, и удаляются при его закрытии. Таким образом, на компьютере пользователя не остается следов от посещения сайтов.

Но действия пользователя по-прежнему видны извне. За ними могут следить посещаемые сайты, сам браузер пользователя и браузерные дополнения, провайдер пользователя, системный администратор в офисе или учебном заведении, а также разнообразные системы рекламы и аналитики.

Некоторые браузеры, в частности, Firefox, в приватном режиме включают дополнительные меры защиты: отключение браузерных дополнений, блокировку известных сайтов аналитики, отслеживающих пользователей, и сторонних куки, установленных не тем сайтом, на который заходит пользователь. Все это, впрочем, тоже не дает полной «невидимости».

Как сайты следят за инкогнито-посетителями:

- **По логину.** Если пользователь ввел на сайте свои e-mail, телефон, имя и пароль, настройка браузера уже не играет роли – пользователь представился сайту сам.
- **Через куки.** Хотя сайт не может прочитать «обычные» куки из браузера пользователя, когда тот находится в режиме инкогнито, сайт может установить новые. Если пользователь сидит в окошке «инкогнито» целыми днями, не закрывая его, информации о его перемещениях по сети наберется достаточно.
- **По IP-адресу.** Режим инкогнито его никак не скрывает.
- **По «цифровым отпечаткам».** Комбинируя информацию, передаваемую из браузера в HTTP-заголовках, и данные, которые может собрать веб-страница при помощи JavaScript (например, разрешение экрана, заряд батареи для мобильных устройств, список установленных шрифтов), сайт может создать «цифровой отпечаток» конкретного браузера на определенном устройстве и использовать его для идентификации пользователя. Режим инкогнито на это никак не влияет.
- **Комбинируя все перечисленное.** Продвинутые системы аналитики и отслеживания стараются следить за пользователем несколькими способами, поэтому, даже если в режиме инкогнито недоступны старые куки, пользователя можно «вспомнить» по вспомогательному способу, например по «цифровому отпечатку». В результате может оказаться, что, посетив интернет-магазин в режиме инкогнито и не входя в систему, пользователь почему-то видит в истории поиска товары, которыми интересовался в прошлом.

Браузерные расширения – это полезный инструмент, но важно относиться к ним с осторожностью и помнить, что они совсем не так безобидны, как может показаться. Поэтому рекомендуется скачивать расширения только из официальных магазинов, не устанавливать слишком много расширений и регулярно проверять их список, использовать надежное защитное решение. Всегда обновляйте браузер, когда доступно обновление из официальных источников.

Следует помнить, что полной гарантии безопасности это не дает. Время от времени зловредным расширениям удается проникать и в официальные магазины. Но обычно в них все же заботятся о безопасности пользователей и вредоносные расширения в конце концов удаляют. Если видите в списке установленных расширений что-то, чего сами не устанавливали – это повод насторожиться.

Вопросы к параграфу:

1. Что такое браузер?
2. Какие расширения для браузеров вам известны?
3. В чем плюсы и минусы использования расширений браузеров?
4. Надежно ли хранить пароль от учетной записи в браузере?
5. В чем особенность использования в браузере режима инкогнито?
6. Для чего необходимы куки-файлы?

Задание:

Сделайте сравнительный анализ количества пользователей, географии использования и функционала востребованных браузеров: Google Chrome, Safari, Microsoft Edge, Mozilla Firefox, Vivaldi, DuckDuckGo.

§9. Интернет вещей

Ключевые слова:

интернет вещей, умный дом, умный город, телемедицина, конфиденциальность

Интернет вещей – это система взаимосвязанных вычислительных устройств, которые могут собирать и передавать данные по беспроводной сети без участия человека.

Система интернета вещей включает в себя датчики и устройства, взаимодействие которых осуществляется через облачное соединение. Как только данные попадают в облако, осуществляется их обработка программными средствами и принимается решение о необходимости выполнения определенных действий, например, настройки датчиков и устройств без необходимости ввода данных пользователем или отправки уведомлений.

Полная система интернета вещей состоит из четырех отдельных компонентов:

- **Датчики устройств.** Собирают данные в определенной среде. Устройство может иметь несколько датчиков, например, смартфон оснащен GPS, камерой, акселерометром и другими датчиками. Датчики собирают данные из окружающей среды для решения определенных задач.
- **Средства подключения.** После сбора данных устройство должно отправить их в облако. Это делается по-разному: по Wi-Fi или Bluetooth, средствами спутниковой связи, через

энергоэффективные сети дальнего радиуса действия (LPWAN) или при подключении напрямую к интернету через Ethernet. Вариант подключения зависит от области применения конкретного устройства интернета вещей.

- **Инструменты обработки данных.** Как только данные попадают в облако, осуществляется их программная обработка с целью последующего решения о выполнении определенных действий. Эти действия могут включать отправку предупреждений или автоматическую настройку датчиков устройства без участия пользователя. Иногда требуется ввод данных со стороны пользователя. В этом случае требуется пользовательский интерфейс.
- **Пользовательский интерфейс.** Позволяет осуществить ввод данных со стороны пользователя или выполнить проверку работоспособности системы. Все действия пользователя передаются через систему: от пользовательского интерфейса в облако, а затем к датчикам устройств для внесения запрошенных изменений.

Существует множество областей применения интернета вещей:

- **Носимые устройства.** Это, пожалуй, самый заметный для простого обывателя тип устройств интернета вещей. К ним относятся фитнес-трекеры, умные часы, умные очки, гарнитуры виртуальной реальности и многое другое.
- **Умные дома.** В систему «умный дом» входит бытовая техника. Система используется для автоматизации определенных задач и обычно управляется дистанционно. Устройства интернета вещей, входящие в состав умного дома, включают беспроводные кухонные приборы, музыкальные системы, определяющие настроение, интеллектуальные системы освещения, жалюзи с электрическим приводом, автоматические окна и двери, интеллектуальные счетчики коммунальных услуг и прочие устройства.
- **Умные города.** В умных городах используются такие устройства интернета вещей, как датчики и счетчики для сбора и анализа данных. Затем эти данные могут использоваться для улучшения инфраструктуры, коммунального обслуживания и других сервисов.
- **Беспилотные автомобили.** В беспилотных автомобилях обычно используется технологическая система на основе интернета вещей, передающая данные как о самом автомобиле, так и о дороге, по которой он движется. Самостоятельное движение автомобиля достигается благодаря тому, что данные о дорожном движении, навигации, внешней среде и многом другом собираются и анализируются компьютерными системами автомобиля.
- **Розничная торговля.** Интернет вещей все чаще используется в розничной торговле. Он позволяет обеспечить персонализированные скидки, а также реализовать автоматизированные кассы и умные полки (предупреждающие продавца о том, что заканчиваются запасы), роботизацию рабочих мест и оптимизированное управление цепочками поставок.
- **Телемедицина.** Телемедицина подразумевает использование компьютерных и телекоммуникационных технологий для оказания медицинских услуг. Интернет вещей является важным аспектом телемедицины. Примеры его применения включают удаленную медицинскую диагностику, цифровую передачу медицинских изображений, видеоконсультации со специалистами и т.д.
- **Умное сельское хозяйство.** Умное сельское хозяйство предполагает использование цифровых технологий для оптимизации сельскохозяйственных работ. Фермеры могут использовать подключенные датчики, камеры и другие устройства для получения общих данных о ферме и корректировки действий для повышения урожайности.

Этот список не является исчерпывающим: интернет вещей меняет образ действий и способы работы во многих сферах жизни. Примеры устройств интернета вещей включают умные мобильные телефоны, умные холодильники, умные часы, фитнес-трекеры, умные пожарные сигнализации, умные дверные замки, умные велосипеды, медицинские датчики, умные системы безопасности, а также виртуальные помощники, такие как Alexa, Алиса и т.д.

Интернет вещей имеет как преимущества, так и недостатки. К плюсам относятся:

- **Эффективность.** Взаимодействие между устройствами повышает эффективность процессов и экономит время людей, позволяя им работать над другими задачами.

- **Автоматизация.** Автоматизированное выполнение единообразных задач может повысить качество обслуживания и снизить потребность в человеческом вмешательстве.
- **Снижение издержек.** Повышение эффективности и автоматизация процессов может позволить сократить как отходы, так и трудозатраты, что удешевляет производство и доставку товаров.
- **Контроль качества.** Интернет вещей улучшает обмен данными между устройствами и обеспечивает лучший контроль качества.
- **Прозрачность.** Возможность доступа к информации из любого места, в любое время, с любого устройства упрощает принятие решений и увеличивает прозрачность.

Минусы интернета вещей:

- **Совместимость.** Отсутствие международных стандартов совместимости может привести к возникновению проблем при взаимодействии устройств разных производителей.
- **Снижение количества рабочих мест.** Интернет вещей ускоряет автоматизацию, в результате чего может сократиться количество требуемых рабочих мест.
- **Сложность.** В огромной сети интернета вещей всего один сбой в программном или аппаратном обеспечении может привести к катастрофическим последствиям.
- **Конфиденциальность и безопасность.** Значительное количество ежедневно используемых подключенных к интернету устройств ведет к тому, что в сети хранится существенный объем информации. Это создает риски конфиденциальности и безопасности, которые описаны ниже более подробно.

Безопасность интернета вещей подразумевает защиту устройств и сетей, к которым они подключены, от онлайн-угроз и взломов. Это достигается путем выявления, мониторинга и устранения потенциальных уязвимостей безопасности на устройствах. Таким образом, безопасность интернета вещей – это набор технологий, обеспечивающий безопасность систем интернета вещей.

Учитывая масштаб и сложность интернета вещей, устройства интернета вещей, как правило, подвержены кибератакам и утечкам данных. Производители серьезно относятся к этой проблеме и работают над обеспечением безопасности пользователей. В будущем для устройств интернета вещей ожидается рост использования встроенных систем защиты и решений по обеспечению безопасности данных в процессе передачи, а также элементы искусственного интеллекта, блокчейна и граничных вычислений.

Интеллектуальные технологии будут все чаще применяться в городах по всему миру для повышения эксплуатационной эффективности, информирования населения и обеспечения более высокого качества государственных услуг и благосостояния граждан.

Рассмотрим примеры нарушений безопасности интернета вещей. В последние годы имел место ряд громких случаев компрометации устройств интернета вещей киберпреступниками. Среди них:

- В 2016 году сотни тысяч скомпрометированных подключаемых устройств были вовлечены в ботнет Mirai. Ботнет – это сеть компьютеров, специально зараженных вредоносным ПО с целью выполнения автоматических задач в Интернете без разрешения и ведома владельцев этих компьютеров. В результате атаки ботнета Mirai наблюдались сбои в работе таких крупных сервисов и сайтов, как Spotify, Netflix и PayPal.
- В 2018 году вредоносная программа VPNFilter заразила более полумиллиона маршрутизаторов в более 50 странах. Вредоносная программа VPNFilter может устанавливать на устройства, подключенные к роутеру, вредоносное ПО, которое собирает проходящую информацию, блокирует сетевой трафик и крадет пароли.
- В 2020 году эксперт по кибербезопасности взломал Tesla Model X менее чем за две минуты, воспользовавшись уязвимостью Bluetooth. Аналогичным атакам также подверглись другие автомобили, для открытия и запуска которых используются беспроводные ключи.
- В 2021 году был осуществлен взлом камеры Verkada (компания по производству камер наблюдения). Швейцарские хакеры получили доступ к 150 000 прямых трансляций с камер этой компании. Это были камеры наблюдения внутри зданий государственных организаций, таких как школы, больницы, тюрьмы, и частных компаний.

Вопрос защиты интернета вещей являются актуальными для их пользователей. Необходимо задумываться о методах защиты устройств, относящихся к данной группе, и защищенности сети, на основе которой функционируют умные устройства. Следует выбирать производителей устройств с хорошим «послужным списком» в сферах приватности и безопасности. При выходе обновлений прошивки – в самое ближайшее время устанавливать их на устройства.

Вопросы к параграфу:

1. Что такое интернет вещей?
2. Почему в последнее время популярен умный дом?
3. Какие преимущества и недостатки телемедицины?
4. В чем заключаются плюсы и минусы использования интернета вещей?
5. Каких рекомендаций следует придерживаться при использовании интернета вещей?

§10. Вредоносное программное обеспечение

Ключевые слова: вредоносное ПО, троянские программы, вирусы, черви, шпионское ПО, бот, ботнет, логическая бомба, бэкдор, уязвимость нулевого дня

Вредоносное программное обеспечение – это программы, намеренно разработанные и внедряемые для нанесения ущерба компьютерам и компьютерным системам. Наиболее часто вредоносное ПО распространяется через почтовые вложения, физические носители, всплывающие окна в браузере, уязвимости ПО, бэкдоры (преднамеренно или непреднамеренно встроенные дефекты ПО, оборудования, сетей).

Рассмотрим типы вредоносного ПО:

- **Рекламные программы.** Отображают нежелательную, а иногда и вредоносную рекламу на экране устройств, перенаправляют результаты поиска на рекламные сайты и собирают данные пользователей, которые затем можно продать рекламодателям без согласия самих пользователей. Не все рекламные программы являются вредоносными, некоторые из них легальны и безопасны в использовании. В большинстве случаев пользователи могут влиять на частоту показа рекламных программ и на разрешенные виды загрузок с помощью элементов управления во всплывающих окнах, настроек браузеров, а также, используя блокировщик рекламы.
- **Шпионские программы.** Это разновидность вредоносных программ, скрывающихся на устройстве, отслеживающих активность и осуществляющих кражу конфиденциальной информации: финансовых данных, учетных записей, данных для входа и прочих данных.
- **Программы-вымогатели и программы-шифровальщики.** Это вредоносные программы, осуществляющие блокировку или отказ доступа пользователей к системе или данным до момента выплаты выкупа. Программы-шифровальщики – это тип программ-вымогателей, выполняющих шифрование пользовательских файлов и требующих оплаты в определенный срок и часто в цифровой валюте, например, в биткойнах. Программы-вымогатели уже много лет представляют угрозу для компаний всех отраслей. По мере того, как все больше компаний переходят на цифровые технологии, вероятность стать жертвой атак программ-вымогателей значительно возрастает.
- **Троянские программы.** Маскируются под легальное программное обеспечение, чтобы обманом заставить пользователей запустить вредоносные программы на компьютере. Поскольку они выглядят достаточно надежными, пользователи загружают их, непреднамеренно заражая свои устройства

вредоносными программами. Троянские программы – это, своего рода, точки входа злоумышленников в систему. После установки троянской программы на устройство злоумышленники могут использовать ее для удаления, изменения и сбора данных с устройства в рамках ботнета, а также для слежки за устройством и получения доступа к сети.

- **Черви.** Это один из наиболее часто встречающихся типов вредоносных программ, распространяющихся по компьютерным сетям, используя уязвимости операционной системы. Черви представляют собой отдельные программы, распространяющиеся путем самокопирования с целью заражения других компьютеров, при этом никаких действий со стороны пользователей или злоумышленников не требуется. Благодаря способности быстро распространяться, черви часто используются для выполнения фрагментов кода, созданного для повреждения системы, например, они могут удалять файлы в системе, шифровать данные для атаки программы-вымогателя, красть информацию.
- **Вирусы.** Это фрагмент кода, который вставляется в приложение и запускается при его запуске. Обычно вирус распространяется через зараженные веб-сайты, при совместном доступе к файлам, при загрузке зараженных вложений электронной почты. Вирус бездействует до момента активации зараженного файла или программы. После этого вирус начинает распространяться в системе.
- **Клавиатурные шпионы.** Это разновидность шпионских программ, отслеживающих активность пользователей. Они могут использоваться в законных целях, например, родители могут с их помощью контролировать действия детей в Интернете, а компании отслеживать активность сотрудников. Однако злоумышленники могут использовать клавиатурные шпионы для кражи паролей, банковских данных и прочей конфиденциальной информации.
- **Боты и ботнеты.** Бот – это компьютер, зараженный вредоносной программой, которым злоумышленники могут управлять удаленно. Боты, иногда называемые зомби-компьютерами, могут использоваться для запуска атак, а также стать частью ботнета – набора ботов, объединенных в сеть. Ботнеты могут включать миллионы устройств, как правило, они распространяются незаметно.
- **Потенциально нежелательные программы.** Это программы, которые могут включать рекламу, панели инструментов и всплывающие окна, не имеющие отношения к самой загруженной программе.
- **Гибридные вредоносные программы.** Большинство современных вредоносных программ представляет собой комбинацию различных типов, часто включая элементы троянских программ, червей, а иногда и вирусов. Часто вредоносные программы сначала выглядят как троянские, но после запуска распространяются по сети как черви.
- **Бесфайловые вредоносные программы.** Используются легальные программы для заражения компьютера. Они не используют файлы и не оставляют следов, что затрудняет их обнаружение и удаление. Бесфайловые программы не хранятся в файлах и не устанавливаются на устройство, они попадают непосредственно в память, а вредоносный контент никогда не затрагивает жесткий диск. Киберпреступники все чаще используют бесфайловые вредоносные программы. Они позволяют осуществлять эффективные атаки, поскольку их обнаружение традиционными антивирусами затрудняется вследствие небольшого размера и отсутствия файлов для проверки.
- **Логические бомбы.** Это тип вредоносных программ, которые активируются только при определенном условии. Вирусы и черви часто содержат логические бомбы для исполнения вредоносного кода в заранее определенное время или при выполнении определенного условия. Ущерб, причиняемый логическими бомбами, варьируется от изменения всего нескольких байтов данных до запрета на чтение жестких дисков.

Зараженные компьютеры, подключенные к сети Интернет, могут объединяться в ботнет. Такая сеть часто состоит из сотен тысяч компьютеров, обладающих в сумме огромной вычислительной мощностью. По команде злоумышленников ботнет может организовать атаку на какой-либо сайт. В результате огромного количества запросов сервер не справляется с нагрузкой и сайт становится недоступен. Такая атака называется **DoS-атакой**. Если атака выполняется одновременно с большого числа компьютеров, говорят о **DDoS-атаке** (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). Такая атака проводится в том случае, если требуется вызвать отказ в обслуживании хорошо защищённой крупной компании или правительственной организации.

В последнее время коммерческое шпионское программное обеспечение все чаще попадает в заголовки. Причем речь не о специализированных ресурсах про информационные технологии или кибербезопасность.

Коммерческое шпионское ПО – это создаваемые частными компаниями легальные вредоносные программы, предназначенные для точечной слежки и сбора важных данных с устройств пользователей. Стандартный круг задач коммерческих шпионских программ: кража переписки, подслушивание звонков и слежка за местоположением.

Часто для установки коммерческого шпионского ПО на устройства жертвы злоумышленники используют **уязвимости нулевого дня** (англ. zero day) – неустранённые уязвимости, а также вредоносное ПО, против которых ещё не разработаны защитные механизмы.

В коммерческом шпионском ПО зачастую предусмотрены инструменты для удаления следов заражения, чтобы атакуемые даже постфактум не могли заподозрить, что за ними кто-либо следил.

Хотя коммерческое шпионское ПО разрабатывают частные компании, продают они его, как правило, тем или иным государственным организациям – в первую очередь правоохранительным органам и прочим силовым ведомствам. В итоге коммерческое шпионское ПО используется в том числе для слежки за гражданскими активистами, журналистами и другими некриминальными лицами. Поэтому программы-шпионы регулярно попадают в новостные ленты.

Обнаружение каких-либо из перечисленных признаков может свидетельствовать о заражении персонального компьютера вредоносным ПО:

- Медленная работа, сбои и зависание компьютера.
- «Синий экран смерти».
- Автоматическое открытие и закрытие или самостоятельное изменение программ.
- Отсутствие места для хранения.
- Увеличение количества всплывающих окон, панелей инструментов и нежелательных программ.
- Отправка электронных писем и сообщений без ведома пользователя.

Лучший способ защититься от атак вредоносных и потенциально нежелательных программ – использовать комплексное антивирусное решение, которое может обеспечить постоянную надежную защиту данных и устройств от злоумышленников и вредоносного ПО.

Вопросы к параграфу:

1. Что такое вредоносное программное обеспечение?
2. Какие типы вредоносного программного обеспечения Вам известны?
3. Для чего злоумышленники организовывают DDoS-атаки?
4. Почему гибридное вредоносное программное обеспечение встречается всё чаще?
5. Что может являться показателем заражения компьютера вредоносным ПО?
6. Какими способами и методами можно защитить персональный компьютер и смартфон от заражения вредоносным ПО?

kaspersky

§11. Атака нулевого дня

Ключевые слова: нулевой день, уязвимость нулевого дня, эксплойт нулевого дня

В программном обеспечении часто есть уязвимости безопасности, которые злоумышленники могут использовать для причинения вреда. Разработчики ПО всегда ищут уязвимости, которые необходимо исправить, поэтому разрабатываются и выпускаются программные обновления.

Однако иногда злоумышленники обнаруживают уязвимость раньше разработчиков. Пока она не закрыта, злоумышленники могут написать и внедрить код, позволяющий ей воспользоваться. Он называется кодом эксплойта.

«Нулевой день» – это общий термин, описывающий недавно обнаруженные уязвимости в системе безопасности, которые могут быть использованы злоумышленниками для атаки на систему. Термин «нулевой день» показывает, что поставщик или разработчик только что узнали об уязвимости, и у них есть «ноль дней» на ее исправление. Атака нулевого дня происходит в результате использования злоумышленниками уязвимости до того, как разработчикам удалось ее исправить.

Уязвимость нулевого дня – программная уязвимость, обнаруженная злоумышленниками до того, как о ней узнали производители программы. Для уязвимостей нулевого дня еще не выпущены патчи, что повышает вероятность атаки.

Эксплойт нулевого дня – это метод, используемый злоумышленниками для атаки на системы с не выявленными ранее уязвимостями.

Атака нулевого дня – это использование эксплойта нулевого дня для нанесения ущерба или кражи данных из системы, в которой имеется уязвимость.

В результате внедрения кода эксплойта могут пострадать пользователи программного обеспечения. Как только злоумышленники находят уязвимость нулевого дня, им нужно получить доступ к уязвимой системе. Когда об уязвимости становится известно, разработчики пытаются исправить ее, чтобы остановить атаку. Однако уязвимости в системе безопасности часто не удается обнаружить сразу. Иногда до момента обнаружения уязвимости, ставшей причиной атаки, могут пройти дни, недели и даже месяцы. И даже после выпуска патча, закрывающего уязвимость нулевого дня, не все пользователи сразу же его устанавливают. В последние годы хакеры стали гораздо быстрее обнаруживать и использовать уязвимости.

Особая опасность атак нулевого дня заключается в том, что о них знают только сами злоумышленники. После проникновения в сеть преступники могут либо атаковать немедленно, либо затаиться и ждать наиболее подходящего времени.

При атаках нулевого дня могут использоваться различные уязвимые объекты: операционные системы, браузеры, приложения, интернет вещей и т.д.

Существуют различные виды уязвимостей нулевого дня: отсутствие шифрования данных, отсутствие авторизации, неработающие алгоритмы, ошибки, проблемы с безопасностью паролей и прочие. Обнаружить их может оказаться непросто. Из-за характера этих уязвимостей подробная информация об эксплойтах нулевого дня доступна только после их идентификации.

Организации, подвергшиеся атаке нулевого дня, могут наблюдать нетипичный трафик или подозрительные действия, такие как сканирование, исходящие от клиента или сервиса.

Перечислим некоторые методы обнаружения атак нулевого дня:

- Использование существующих баз вредоносных программ, содержащих описание их поведения, в качестве справочника. Такие базы данных постоянно обновляются и могут быть полезны в качестве ориентира, однако эксплойты нулевого дня по определению являются новыми и неизвестными, так что существующая база данных не сможет предоставить полную информацию.
- В качестве альтернативы выполняется поиск признаков вредоносных программ нулевого дня на основе их взаимодействия с целевой системой. При использовании этого метода не выполняется исследование кода входящих файлов, а рассматривается их взаимодействие с существующими программами и предпринимаются попытки выяснить, являются ли такое взаимодействие результатом злонамеренных действий.
- Для обнаружения данных о ранее зафиксированных эксплойтах все чаще используется машинное обучение. При этом устанавливается эталон безопасного поведения системы на основе данных о прошлых и текущих взаимодействиях с системой. Чем больше данных доступно, тем надежнее обнаружение.

Часто используется комбинация различных систем обнаружения.

К одним из последних примеров крупных атак нулевого дня можно отнести:

- **2021 год: Google Chrome.** В 2021 году Google Chrome подвергся серии атак нулевого дня, ставших причиной ряда обновлений Chrome. Уязвимость возникла из-за ошибки в JavaScript-движке V8, используемом в веб-браузере.
- **2020 год: Zoom.** У популярной платформы видео-конференц-связи была обнаружена уязвимость. В результате этой атаки нулевого дня злоумышленники получали удаленный доступ к компьютерам пользователей, на которых установлены старые версии Windows. Если атака была нацелена на администратора, злоумышленники могли полностью захватить его компьютер и получить доступ ко всем файлам.
- **2020 год: Apple iOS.** Apple iOS часто называют самой безопасной платформой для смартфонов. Однако в 2020 году она подверглась как минимум двум атакам нулевого дня. Одна из ошибок нулевого дня позволила злоумышленникам удаленно скомпрометировать iPhone.

Для защиты от атак нулевого дня и обеспечения безопасности компьютеров и данных частным лицам и организациям важно выполнять определенные правила кибербезопасности. Они включают:

- Своевременное обновление программ и ОС.
- Использование только необходимого ПО.
- Использование сетевого экрана.
- Обучение сотрудников организаций по основам информационной безопасности.
- Использование комплексного антивирусного программного решения.

Вопросы к параграфу:

1. Что такое уязвимость нулевого дня?
2. Почему киберпреступники используют эксплойт нулевого дня?
3. Существуют ли характерные особенности обнаружения атак нулевого дня?
4. Существует (существовала ли) уязвимость нулевого дня в операционных системах Windows и iOS?

kaspersky

§12. SQL-инъекция

Ключевые слова: SQL, SQL-инъекция, базы данных, веб-приложения

SQL – это язык построения запросов, который применяется в программировании для чтения, изменения и удаления информации, хранящейся в реляционных базах данных.

SQL-запрос – это запрос, направленный в базу данных для выполнения определенной операции или функции, такой как извлечение данных или исполнение SQL-кода. Например, запрос может осуществлять передачу учетных данных пользователя через веб-форму для доступа к сайту. Обычно подобные веб-формы сконфигурированы таким образом, чтобы принимать только определенные типы данных, такие как имя пользователя и (или) пароль. Введенная информация сверяется с базой данных. Если все совпадает, пользователь сможет войти на сайт, иначе в доступе будет отказано.

SQL-инъекция (или SQLi) – уязвимость, которая позволяет атакующему использовать фрагмент вредоносного кода на языке структурированных запросов (SQL) для манипулирования базой данных и получения доступа к потенциально ценной информации. Атаки на основе таких уязвимостей одни из самых распространенных и опасных: они могут быть нацелены на любое веб-приложение или веб-сайт, которые взаимодействуют с базой данных SQL (а подавляющее большинство баз данных реализованы именно на SQL).

Ситуация опасна тем, что большинство веб-форм не имеют механизмов, которые бы исключали ввод дополнительной информации в поле. Это дает злоумышленникам возможность передать в базу данных собственные запросы через поля ввода формы. Они могут использовать эту уязвимость в разных преступных целях, начиная с кражи конфиденциальных данных и заканчивая манипулированием сведениями в базе.

Так как подавляющее большинство веб-сайтов и серверов полагаются на базы данных, SQL-инъекции являются одними из самых давних и распространенных видов кибератак. В сообществе киберпреступников появилось несколько разработок, повышающих вероятность таких атак: прежде всего речь идет об инструментах, которые позволяют обнаружить уязвимое место для SQL-инъекции. Соответствующие утилиты представлены в свободном доступе как проекты с открытым исходным кодом. Достаточно нажать нужную кнопку, и за считаные минуты будет реализована атака, позволяющая заполучить доступ к любой таблице или столбцу базы данных.

Успешно проведенная атака с SQL-инъекцией может вообще никак себя не проявлять. Тем не менее иногда можно заметить следующие симптомы:

- Получение избыточного числа запросов за короткий промежуток времени. Например, массовый поток электронных писем от формы обратной связи веб-сайта.
- Рекламные блоки, перенаправляющие пользователя на подозрительные веб-сайты.
- Странные всплывающие окна и сообщения об ошибках.

Злоумышленники довольно часто прибегают к SQLi-атакам, ведь их относительно просто реализовать, а успешная атака может принести большую прибыль. Однозначной статистики на этот счет нет, но по усредненным оценкам, SQL-инъекции составляют основную часть атак на программные системы. По данным сообщества Open Web Application Security Project, атаки на основе внедрения кода, к которым также относится SQL-инъекция, являются третьим по значимости риском безопасности для веб-приложений.

Успешная SQLi-атака может нанести серьезный ущерб бизнесу и может привести к раскрытию конфиденциальных данных, нарушению приватности пользователей и получению злоумышленниками общих прав доступа ко всей системе.

Ущерб от SQLi-атак является не только финансовым. Успешная атака может привести к репутационным потерям и утрате доверия клиентов, если произойдет кража персональной информации (имен, адресов, телефонных номеров и данных кредитных карт). Вернуть доверие клиентов гораздо сложнее, чем его потерять.

За годы существования этого класса уязвимостей от SQLi-атак пострадало множество организаций. Приведем некоторые громкие случаи:

- **Fortnite, 2019 год**. Fortnite– это онлайн-игра с аудиторией, насчитывающей более 350 млн игроков. В 2019 году была обнаружена уязвимость для SQL-инъекции, которая позволила злоумышленникам получить доступ к пользовательским учетным записям. Уязвимость впоследствии закрыли.
- **Cisco, 2018 год.** Была найдена уязвимость для SQL-инъекции в Cisco Prime License Manager. Брешь позволила атакующим заполучить доступ к командной оболочке систем, на которых был развернут диспетчер лицензий Cisco. Компания Cisco впоследствии закрыла эту уязвимость.
- **Tesla, 2014 год.** Специалисты по кибербезопасности заявили об успешном взломе веб-сайта Tesla методом SQL-инъекции. Им удалось получить административные привилегии и украсть пользовательские данные.

Вопросы к параграфу:

1. Какой функционал у языка SQL?
2. Что такое SQL-инъекция?
3. Почему SQL-инъекция входит в топ атак на веб-приложения?
4. Что можно отнести к признакам успешно проведенной атаки средствами SQL-инъекции?

§13. Методы защиты в операционных системах. Сетевые технологии защиты

Ключевые слова: операционная система, аутентификация, авторизация, администрирование, KasperskyOS, OSI, VPN, IP-адрес, брандмауэр

Операционная система (ОС) – программное обеспечение, управляющее компьютерами и позволяющее запускать на них прикладные программы. Предоставляет программный интерфейс для взаимодействия с компьютером, управляет прикладными программами и занимается распределением предоставляемых ресурсов, в том числе между прикладными программами. Некоторые ОС позволяют прикладным программам работать с аппаратным обеспечением напрямую.

В широком смысле под операционной системой понимается совокупность ядра операционной системы и работающих поверх него программ и утилит, предоставляющих интерфейс для взаимодействия пользователя с компьютером.

Наиболее эффективными являются методы защиты компьютерной информации на уровне операционной системы. Особенностью защищенной операционной системы является то, что в ней каждое выполняемое действие должно быть авторизовано.

Авторизация – это проверка полномочий пользователя на выполнения каких-либо действий.

kaspersky

Защищенные системы, в том числе и операционные, базируются на трех основных процедурах: аутентификации, авторизации и администрировании и реализуют большинство типовых методов защиты информации: идентификация и аутентификация пользователей, контроль доступа, регистрация событий, резервное копирование и восстановление данных, шифрование и т.д.

Оценка безопасности ОС складывается из функциональной и эксплуатационной безопасности. Функциональная безопасность характеризуется набором средств и механизмов защиты информации в составе операционной системы и дает качественную, экспертную оценку эффективности механизмов защиты. Качественный уровень функциональной безопасности ОС может быть определен (подтвержден) при его сертификации по требованиям безопасности.

Среди известных на сегодняшний момент операционных систем архитектурой построения и методами защиты отличается KasperskyOS, которая реализует новый, кибериммунный подход к защите IT-систем и позволяет сделать неэффективными как известные, так и новые типы кибератак. Кибериммунные продукты на базе KasperskyOS применяются в отраслях, где существуют повышенные требования к кибербезопасности, надежности и предсказуемости работы IT-систем, например, в промышленности, энергетике, транспортной инфраструктуре, в системах умного города.

«Врожденная» безопасность KasperskyOS заложена в ее архитектуре и философии. Кибериммунитет обеспечивается разделением IT-системы на изолированные части и контролем взаимодействий между ними. На этапе проектирования продукта задаются политики безопасности, которые описывают каждое разрешенное действие. Запускаться и работать может только то, что разрешено администраторами системы и разработчиками приложений. Операционная система KasperskyOS в совокупности с методологией разработки IT-продуктов служит эффективной и надежной основой для создания доверенных информационных систем, обладающих иммунитетом в отношении киберугроз. Ядро операционной системы разработано в «Лаборатории Касперского» с нуля, без использования сторонних библиотек и кода

На сегодняшний момент практически каждый компьютер подключен к Интернету, либо к какой-то локальной сети, позволяющей производить обмен информацией между компьютерами. Угрозы информационной безопасности в сетях вызваны невозможностью обеспечить физическую защиту каналов передачи данных ввиду их протяженности и открытостью большинства сетевых протоколов.

На уровне сетевого ПО возможна реализация прослушивания сегмента локальной сети, перехвата сообщений на маршрутизаторе, создания ложного маршрутизатора, навязывания сообщений, отказа в обслуживании.

Прослушивание сегмента локальной сети происходит в пределах одного и того же сегмента. При этом любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента. Поэтому, если компьютер хакера подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента

Перехват сообщений на маршрутизаторе осуществляется в том случае, если хакер имеет привилегированный доступ к сетевому маршрутизатору, он получает возможность перехватывать все сообщения, проходящие через этот маршрутизатор, и, хотя тотальный перехват невозможен из-за слишком большого объема, чрезвычайно привлекательным является выборочный перехват сообщений, содержащих пароли пользователей и необходимые данные конкретных аккаунтов.

Создание ложного маршрутизатора осуществляется путем отправки в сеть сообщений специального вида. Хакер добивается, чтобы его компьютер стал маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям.

Навязывание сообщений реализуется средствами отправки в сеть сообщения с ложным обратным сетевым адресом, хакер переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей, чьи соединения обманным путем были переключены на компьютер хакера.

Отказ в обслуживании осуществляется отправлением в сеть сообщения специального вида, после чего одна или несколько компьютерных систем, подключенных к сети, полностью или частично выходят из строя.

kaspersky

Компьютерные сети являются открытыми распределенными системами. Для таких систем определена эталонная семиуровневая модель взаимодействия (OSI). Каждый из уровней модели, отвечает за выполнение специфических задач и использует соответствующие протоколы – набор правил и соглашений, регламентирующих формат и процедуру передачи данных.

Для реализации сетевых сервисов безопасности используются следующие механизмы и методы защиты информации: шифрование, подписывание сообщений, управление доступом.

Специальными технологиями сетевой защиты являются экранирование и туннелирование.

Экранирование выполняет функцию защиты внутреннего пространства сети (например, локальной сети организации) от внешних воздействий. Для организации экранирования используются межсетевые экраны. Туннелирование лежит в основе построения **виртуальных частных сетей (VPN).**

VPN (от англ. Virtual Private Network) необходим для защиты пользователей при использовании публичных сетей, так как шифрует интернет-трафик и скрывает личные данные: посторонним будет труднее украсть их или отследить действия в сети. Безопасное соединение шифрует данные в режиме реального времени.

Безопасное соединение маскирует **IP-адрес** – уникальный числовой идентификатор устройства в компьютерной сети, перенаправляя его через специально настроенный удаленный сервер, которым управляет отдельный провайдер. В результате сервер безопасного соединения, который используется, становится источником данных. Интернет-провайдер и другие лица не видят, какие сайты посещаются и какие данные отправляются или принимаются.

VPN действует как фильтр, превращая всю отправляемую и получаемую информацию в бессмыслицу. Даже если она попадёт в руки преступников, они не смогут ею воспользоваться.

Для защиты отдельных ПК и сетей от атак из Интернета используются **брандмауэры** (сетевой экран или файрвол) – это система защиты компьютерной сети, которая ограничивает прохождение входящего, исходящего и внутрисетевого трафика. Это ПО или программно-аппаратный модуль, который принимает решение – пропустить или заблокировать проходящий пакет данных. Его основная функция – блокировать вредоносную активность и предотвращать несанкционированные действия пользователей как в частной сети, так и за ее пределами. Брандмауэр входит в состав современных версий ОС.

Вопросы к параграфу:

1. Что такое операционная система?
2. Для чего необходим функционал авторизации в ОС?
3. Какие основные процедуры отличает защищенную систему от незащищенной?
4. Какие проблемы информационной безопасности могут возникнуть при подключении ПК к сети?
5. В каких случаях оправдано использование VPN?
6. Для чего необходим брандмауэр?

Задание:

Проанализируйте концепцию (стандарты, принципы, уровни) сетевой модели OSI.

kaspersky

Ситуация:

Вы находитесь в аэропорту и смартфон имеет плохой сигнал связи, но есть местная открытая сеть с подключением к Интернету. В данный момент Вам необходимо:

- узнать разницу во времени между городами;
- отправить фото друзьям;
- совершить онлайн покупку с введением данных банковской карты.

Какими будут Ваши действия?

§14. Антивирус

Ключевые слова: антивирус, базы данных антивируса, операционная система

Не всегда операционная система обладает функционалом, чтобы осуществить качественную защиту пользователя от вредоносного ПО или зловредов, в том числе и в сети. На помощь приходят различные программы, которые в той или иной степени позволяют осуществить такую защиту – антивирус – система, которая, используя антивирусные базы (базы данных, необходимые для обнаружения и удаления вредоносного ПО), выявляет различные типы зловредов.

Антивирус – базовый компонент большинства современных решений для борьбы с вредоносным ПО. Иногда термин ошибочно используется для описания любых решений, обеспечивающих безопасность.

Базы данных антивируса хранят данные, необходимые для обнаружения и удаления вредоносного кода – серии вирусных сигнатур или уникальных последовательностей байтов, специфичных для каждого отдельного зловреда. Сегодня сигнатурный анализ не самый распространенный метод защиты от вредоносного ПО.

Ядром любого антивирусного продукта является программный модуль, созданный для обнаружения и удаления вредоносного кода, так называемый «движок». Он разрабатывается независимо от конечного продукта и, таким образом, одинаково хорошо встраивается как в персональные защитные решения, так и в почтовые сканеры, файловые серверы, брандмауэры и т.п. Эти продукты могут быть созданы как разработчиком движка, так и сторонними лицами, встраивающими его в свои приложения или бизнес-процессы, используя комплект средств разработки.

Важность данных программ растёт в связи с такими трендами, как цифровизация, цифровая трансформация, ростом проникновения гаджетов и Интернета. На сегодняшний момент разработчики антивирусов сталкиваются с 400 тысячами зловредных программ ежедневно, во всём мире растёт количество киберугроз, и вместе с этим растёт объём рынка кибербезопасности во всём мире.

Антивирусные решения позволяют реализовать три основные задачи:

- Не допустить появления зловреда на компьютере.
- Обнаружить вредоносное ПО в системе.
- Уничтожить зловреда без ущерба для остальных данных.

Все антивирусные программы делят на виды в зависимости от того, как они ищут вредоносное ПО, как лечат заражённые файлы и с каким вредоносным ПО могут справиться. К примеру, их можно поделить на такие виды:

- **Несигнатурные.** Используют проактивную защиту – справляются с неизвестными зловредами, используя знания об уже существующем вредоносном ПО.
- **Сигнатурные**. Используют постоянно обновляемую базу данных, в которой есть информация о зловредах, и ищут совпадения с ней в файлах на ПК.

По механизму защиты можно выделить десятки видов антивирусов, такие как сканеры, мониторы, фильтры полифаги, ревизоры, блокировщики и т.д. В настоящее вермя антивирусное ПО объединяет в себе несколько видов защитных программ. Набор функций зависит от выбора пользователя.

В большинстве случаев невозможно одновременно использовать два антивируса на одном компьютере. Даже несмотря на заманчивую возможность для пользователей попытаться реализовать так называемую «двойную защиту». Если на одном компьютере работают два антивируса, они оба пытаются установить средства перехвата в одну и ту же часть ядра системы. Это приводит к конфликту между антивирусными средствами мониторинга и может повлечь последствия в работе ПК.

Как правило, киберпреступники стараются продумать свои атаки таким образом, чтобы их активность не бросалась в глаза пользователю. Ведь чем дольше атака остается незаметной, тем больше у нее шансов на успех. Зачастую по ряду признаков можно понять, что с компьютером что-то не так.

Очевидными признаками, что на компьютере работает вредоносное ПО или им заинтересовались хакеры, являются:

- Компьютер стал работать медленно.
- Проблемы с учетными записями.
- Внезапно появляющиеся окна.
- Подозрительное поведение браузера.
- Недоступные или исчезнувшие файлы, папки.
- Появились незнакомые файлы или приложения.
- Нотификации об удаленном подключении.
- Что-то мешает компьютеру выключиться или перезапуститься.
- Письма или сообщения, которые вы не отправляли.

Обычно компьютеры с операционной системой Mac менее уязвимы, чем компьютеры с операционной системой Windows. Основная причина в том, что злоумышленники большую часть усилий тратят на создание вредоносных программ для устройств, работающих под Windows, поскольку они занимают большую часть рынка и, следовательно, обещают большую выгоду. Однако с увеличением доли рынка компьютеров Mac киберпреступники все больше направляют свои усилия на продукты компании Apple. Компьютеры Mac имеют встроенные средства защиты, например файервол для блокировки сетевых атак, однако антивирусное ПО в общепринятом смысле на устройствах Mac не предустановлено.

Вопросы к параграфу:

1. Что такое антивирус?
2. Что является ядром антивирусного ПО?
3. Используется ли эвристика в работе антивирусных ПО?
4. Возможна ли установка антивирусного решения на компьютеры с ОС Windows, Linux, Mac?
5. В чем заключается проблема использования нескольких антивирусных приложений на одном ПК?

Задание:

Проанализируйте процентную составляющую пользователей операционных систем Windows, Linux, Mac. Как эти данные влияют на разработку вредоносного ПО?

kaspersky

Ситуация:

Вы скачиваете архив с файлами: установщик игры, русификатор. Автор размещенного архива рекомендует отключить антивирус для успешной и быстрой установки игры. Какими будут Ваши действия?

§15. Фишинг, вишинг, доксинг

Ключевые слова:

фишинг, ссылка, SMS, фарминг, вишинг, вредоносное ПО, QR-код, доксинг

Фишинг (phishing, искаженное написание англ. fishing – рыбалка) – разновидность интернет-мошенничества, нацеленная на кражу конфиденциальной информации, такой как учетные данные от аккаунтов в интернет-сервисах или данные банковских карт. Типичная фишинговая атака состоит из рассылки писем или сообщений от имени легитимных организаций с темой-«приманкой» и ссылкой на поддельную страницу ввода данных. В некоторых случаях понятие фишинга трактуется шире. К нему могут также относить рассылку писем или сообщений со ссылками на страницы загрузки вредоносного ПО или вредоносными вложениями.

Можно выделить некоторые виды фишинга в зависимости от того, какой канал связи злоумышленники используют для атаки: почтовый фишинг, фишинг в социальных сетях и мессенджерах, фишинговые ссылки в SMS, голосовой фишинг, фарминг (пользователя автоматически перенаправляют на фишинговый сайт, например, с помощью специального вредоносного ПО).

С точки зрения цели злоумышленников фишинг делится на массовый и целевой. Массовый фишинг рассылается по всем доступным злоумышленникам адресам, тогда как целевой фишинг рассчитан на конкретных получателей, а подготовка к нему часто включает предварительный сбор данных о целях.

Для того чтобы пользователь перешел по фишинговой ссылке, злоумышленники могут использовать разные «приманки». В их числе:

- Проблема с аккаунтом: например, аккаунт пользователя якобы заблокирован из-за подозрительной активности и необходимо подтвердить или обновить учетные данные.
- Специальные предложения, акции, розыгрыши.
- Недоставленные письма или голосовые сообщения, онлайн-документы и другие материалы, которые можно посмотреть, только перейдя по ссылке.

Злоумышленники часто используют различные приемы для повышения убедительности фишинговых писем и страниц, а также для обхода обнаружения, в частности:

- Злоумышленники регистрируют домены, похожие на домен организации, которой они притворяются. В случае фишинговых писем они также могут подменить отображаемый в почтовом клиенте адрес отправителя на легитимный.
- Копирование дизайна легитимного сайта.
- Размещение фишинговой страницы на взломанном легитимном сайте или в легитимном сервисе для проведения опросов.
- Рассылка фишинговой страницы в виде HTML-вложения вместо ссылки.
- Динамическая смена дизайна страницы в зависимости от почтового домена жертвы.

В последнее время участился особый вид фишинга – **вишинг** (от англ. voice – голос и phishing – фишинг) – вид мошенничества, при котором злоумышленники используют голосовую связь для манипуляции пользователем, например с целью получения его персональных данных, таких как учетные данные от аккаунтов в интернет-сервисах или финансовые сведения.

Термин «вишинг» могут использовать как для обозначения мошенничества, нацеленного на кражу данных, так и для обозначения любого телефонного мошенничества, в том числе сценариев, при которых злоумышленники убеждают жертву перевести им деньги или установить вредоносное ПО.

Для осуществления вишинговой атаки злоумышленники могут:

- Позвонить потенциальной жертве. При этом злоумышленники могут использовать IP-телефонию и подменять номер, отображающийся на устройстве жертвы.
- Отправить потенциальной жертве SMS, сообщение в мессенджере или электронное письмо с номером телефона.
- Использовать сайты с поддельными предупреждениями о вредоносном ПО на устройстве, которые пугают пользователя несуществующим заражением и предлагают решить проблему, позвонив на номер мошенников.
- Использовать реальное вредоносное ПО, которое, например, автоматически перенаправляет входящие звонки на мошеннический кол-центр.

Злоумышленники могут использовать голосовой фишинг в разных схемах. Ниже приведены несколько распространенных схем вишинга:

- Финансовое мошенничество. Злоумышленники представляются сотрудниками банка, кредитной организации, налоговой службы или другого финансового учреждения. Они звонят потенциальной жертве и сообщают, что возникла проблема, связанная с ее счетом: например, обнаружены несанкционированные транзакции или невыплаченные налоги. Чтобы «решить проблему», пользователю предлагают совершить платеж или сообщить учетные данные от онлайн-банка и одноразовый код.
- Ложная техподдержка. Злоумышленники представляются сотрудниками технической поддержки или IT-службы компании и сообщают пользователю о проблеме с его компьютером или аккаунтом. Чтобы решить ее, жертве якобы нужно предоставить собеседнику учетные данные, доступ к устройству или установить специальную программу (чаще всего это средство удаленного доступа) якобы для удаленного решения проблемы.
- «Легкие деньги». Мошенники сообщают жертве о крупном выигрыше или о полагающейся ей выплате и под этим предлогом убеждают предоставить им личные данные и данные счета или карты якобы для отправки банковского перевода.
- Звонки от торговых представителей. Злоумышленники выдают себя за сотрудников отдела продаж и предлагают несуществующие продукты или услуги по выгодным ценам, стремясь получить личные и банковские данные пользователя якобы для размещения заказа или его оплаты.
- Фальшивые запросы о помощи. Мошенники звонят от лица благотворительных организаций или правоохранительных органов, призывая жертву предоставить банковские данные для оказания финансовой помощи нуждающимся или личную информацию для расследования.

В последнее время участились случаи, когда пользователям на почту приходят письма от имени каких-нибудь крупных интернет-компаний (например, Microsoft или ее облачного сервиса Office 365) с QR-кодами. В тексте письма при этом содержится некий призыв к действию. К примеру: уведомление о том, что скоро закончится срок действия пароля учетной записи, после чего пользователь может потерять доступ к своему почтовому ящику. Пароль якобы нужно сменить, а для этого требуется отсканировать QR-код из письма и далее следовать инструкциям.

Создатели писем, вероятно, рассчитывают на то, что читатель где-нибудь сталкивался с приложениями-аутентификаторами, которые действительно используют QR-коды. Соответственно, это упоминание может пробудить в его голове какие-то ассоциации.

По содержащимся в QR-кодах ссылкам пользователи попадают на достаточно аккуратно сверстанные страницы входа в аккаунт, вполне убедительно копирующие фирменный стиль Microsoft. И все введенные на таких фишинговых страницах логины и пароли оказываются в руках злоумышленников. В результате аккаунт пользователя, поддавшегося на их уловки, оказывается под угрозой.

Следует отметить, что в некоторых случаях фишинговые ссылки в QR-кодах ведут на IPFS-ресурсы. IPFS (InterPlanetary File System, «межпланетная файловая система») – это протокол связи, похожий на «торренты». Он позволяет публиковать любые файлы в Интернете без регистрации домена, использования хостинга и прочих сложностей.

То есть в этом случае фишинговая страница находится прямо на компьютере злоумышленника, при этом она легко доступна по ссылке через специальный IPFS-шлюз. Протокол IPFS используется из-за простоты публикации, а также потому, что удалить такую ссылку значительно сложнее, чем заблокировать «обычный» вредоносный веб-сайт. Соответственно, ссылка будет «жить» дольше.

Отметим, что ни одна нормальная система аутентификации не предложит пользователю перейти по QR-коду в качестве единственного варианта. Поэтому, если пользователь получает письмо с просьбой что-то подтвердить, заново войти в аккаунт, сменить пароль или совершить еще какое-то подобное действие только по QR-коду, то перед вами практически 100% фишинг. Такое письмо необходимо проигнорировать и удалить.

Доксинг (от англ. сленг. dox – документы) – сбор и публикация в Интернете чьих-либо личных данных без разрешения владельца. Термин появился в 90-х годах прошлого века в субкультуре хакеров. Изначально он означал деанонимизацию конкретного пользователя сети, но впоследствии приобрел более широкое значение.

Информацию о жертве можно получить различными способами, к примеру:

- Поиск в открытых источниках.
- Фишинг.
- Психологические манипуляции с применением информационных технологий.
- Приобретение интересующей информации у брокеров данных – компаний, которые специализируются на сборе и продаже данных пользователей.

Как правило, публикация данных пользователя осуществляется с призывом к каким-либо действиям. Часто такие публикации провоцируют травлю, а в отдельных случаях влекут за собой угрозу физической безопасности жертвы. Угрозу публикации данных злоумышленники могут использовать в целях вымогательства.

В некоторых странах существуют законы, направленные на защиту граждан и организаций от доксинга. В остальном мире решение о противоправности доксинга принимается на основании наличия или отсутствия в конкретном инциденте признаков иных незаконных действий.

В интервью Wired Ева Гальперин, директор по кибербезопасности правозащитной организации Electronic Frontier Foundation, советует обратиться в поддержку всех соцсетей, где опубликовали данные жертвы доксинга. Как правило, разглашение сведений о ком-либо без разрешения владельца считается нарушением пользовательского соглашения. Полностью это проблему не решит, но потенциальный урон уменьшится. Помимо это, среди рекомендаций была блокировка учетных записей в соцсетях.

Говоря о рекомендациях по защите от доксинга, следует отметить, что лучше снизить вероятность утечки, чем разбираться с ее последствиями. Исключить доксинг полностью весьма непросто, так как вряд ли пользователь сможет повлиять на слив или утечку информации из баз данных госструктур или соцсетей.

По возможности не выкладывайте в сеть личные данные (адрес, номер телефона, фотографии, по которым можно узнать, где бываете). Следите за тем, чтобы публикуемые снимки не содержали геолокацию в метаданных. Настройки приватности в соцсетях и других сервисах стоит сделать максимально строгими. Следует закрыть свои профили, оставив доступ к странице только друзьям.

kaspersky

Вопросы к параграфу:

1. Что такое фишинг?
2. Какие виды фишинга вам известны?
3. С какими видами фишинга вы сталкивались лично?
4. Может ли QR-код содержать в себе фишинговую ссылку?
5. Что такое доксинг?
6. Каких рекомендаций следует придерживаться, чтобы защитить себя от доксинга?

Задание:

1. Проанализируйте фишинговую и правильную ссылки на сайт банка:

В чем заключается проблема первоначальной идентификации верного адреса сайта?
Продумайте аналогичные подмены адресов сайтов:

https://www.google.ru/
https://www.kaspersky.ru/

2. Вам поступает звонок с номеров:

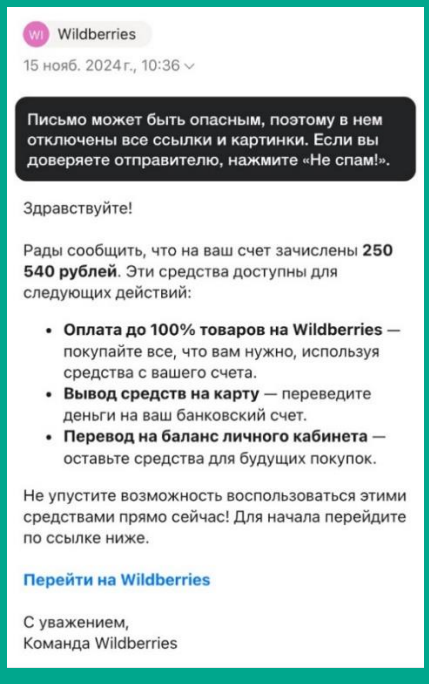
900
9-00
9OO
9-0-0
1-00-0

Какой из данных номеров может считаться оригинальным?
Проанализируйте возможности подмены маски номера и в каких случаях банк лично может выйти с вами на связь по возможному номеру.

3. Осуществите поиск по картинке средствами Яндекс (изображение фотоаппарата в правой части строки поиска).

Используйте личную фотографию или картинку, которая уже опубликована в ваших социальных сетях.
Находит ли поисковик оригинал объекта поиска и какие ссылки выдает в результате?

4. Вы получаете письмо на электронную почту от известного маркетплейса. Ваши действия?



Wildberries

15 нояб. 2024 г., 10:36

Письмо может быть опасным, поэтому в нем отключены все ссылки и картинки. Если вы доверяете отправителю, нажмите «Не спам!».

Здравствуйте!

Рады сообщить, что на ваш счет зачислены **250 540 рублей**. Эти средства доступны для следующих действий:

- **Оплата до 100% товаров на Wildberries** — покупайте все, что вам нужно, используя средства с вашего счета.
- **Вывод средств на карту** — переведите деньги на ваш банковский счет.
- **Перевод на баланс личного кабинета** — оставьте средства для будущих покупок.

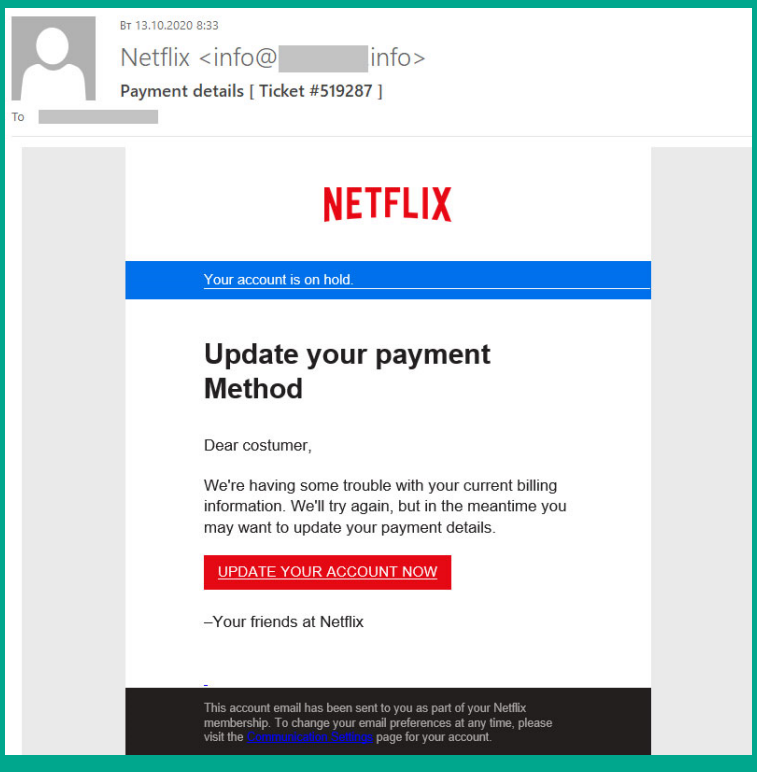
Не упустите возможность воспользоваться этими средствами прямо сейчас! Для начала перейдите по ссылке ниже.

Перейти на Wildberries

С уважением,
Команда Wildberries

Ситуация:

У вас есть аккаунт от стриминга Netflix, и в скором времени получаете письмо по электронной почте: обновите или подтвердите данные для оплаты, иначе потеряете учетную запись.



Вт 13.10.2020 8:33

Netflix <info@ info>

Payment details [Ticket #519287]

To

NETFLIX

Your account is on hold.

Update your payment Method

Dear costumer,

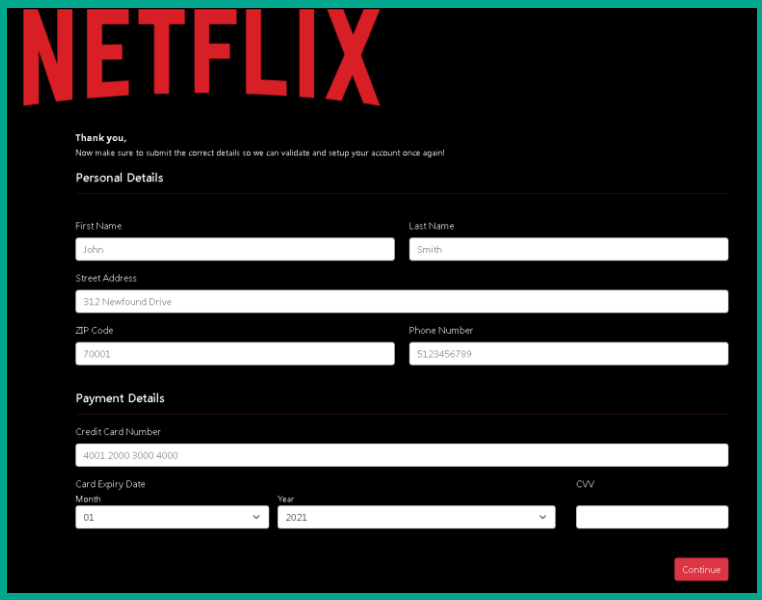
We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE YOUR ACCOUNT NOW

–Your friends at Netflix

This account email has been sent to you as part of your Netflix membership. To change your email preferences at any time, please visit the Communication Settings page for your account.

Пройдя по ссылке, вы попадаете на страницу с подтверждением платежной информации.



Какие правильные пути реагирования на получение такого письма? Данная ситуация соответствует фишингу?

§16. Социальная инженерия

Ключевые слова: психология, манипуляция, фишинг, претекстинг, Twitter

Социальная инженерия подразумевает манипуляции действиями человека без использования технических средств. В контексте кибербезопасности – незаметное принуждение пользователя сделать что-то, что подвергает риску его безопасность или безопасность организации, в которой он работает.

Успех в значительной степени зависит от удачной маскировки вредоносных и нежелательных сообщений под легитимные (в некоторых могут быть даже советы по борьбе с киберпреступностью).

Цель – вызвать ответную реакцию у жертвы: щелкнуть по зараженному вложению электронной почты, перейти по вредоносной ссылке или ответить на ложное уведомление.

Примерами достижения целей социальной инженерии в мошенническом плане могут быть: загрузка установочного файла из сообщения, полученного на электронную почту; получение в мессенджере сообщения от друга с ссылкой на сайт для голосования; ведение разговора с абонентом, чей телефонный номер поддельный и совпадает с телефонным номером известного банка.

К распространенным методам социальной инженерии относятся:

- **Услуга за услугу** – метод выполняется мошенниками, которые не имеют в своём арсенале продвинутых инструментов взлома, однако проводят предварительное исследование целей. Используя этот метод, злоумышленники под видом доброжелателей стимулируют жертву сделать определенные действия для них, что в скором времени приведет к колоссальной личной выгоде.
- **Фишинг** – метод нацелен на кражу конфиденциальной информации, такой как учетные данные от аккаунтов в интернет-сервисах или данные банковских карт. Типичная фишинговая атака состоит из рассылки писем или сообщений от имени легитимных организаций с темой-«приманкой» и ссылкой на поддельную страницу ввода данных, а также рассылка писем или сообщений со ссылками на страницы загрузки вредоносного ПО или с вредоносными вложениями.
- **Троянский конь** – метод получил название в честь мифа, так как жертва сталкивается с подменой необходимого объекта на какой-либо вредоносный, внешне никак это не проявляющий. Примером может служить скачивание установочного файла на компьютер не с официального источника и дальнейшую установку приложения. Но после завершения данного процесса жертва столкнется с тем, что компьютер работает неисправно, либо требует определенные манипуляции, которые вынуждают делать мошенники.
- **Дорожное яблоко** – метод состоит в адаптации предыдущего метода и требует обязательного применения какого-либо физического носителя информации (флешки или диски, которые стилизованы логотипами известных компаний, либо имеют надписи с «интересными» для жертвы словами). Такой носитель информации размещают на пути жертвы, например, рядом с машиной на парковке, на кратчайшем пути от остановки общественного транспорта до офиса, на рабочем столе т.д., чтобы при обнаружении возник интерес проверить, что находится на носителе.
- **Претекстинг** – метод включает в себя некое действие, отработанное по заранее составленному сценарию (претексту). В результате жертва должна выдать определённую информацию или совершить определённое действие. Метод чаще всего используется в телефонном разговоре. Включает в себя больше, чем просто ложь, и требует какого-либо предварительного поиска информации для ее персонализации, чтобы обеспечить доверие у жертвы.

Рассмотрим конкретные примеры использования социальной инженерии мошенниками в реальной жизни.

История произошла 15 июля 2020 года. Большое количество Twitter-аккаунтов стали распространять однотипные сообщения: «Все биткойны, отправленные на указанный внизу адрес, вернутся в удвоенном количестве! Если пошлете $1000, я верну вам $2000. Делаю это только следующие 30 минут».

Эти сообщения рассылались от имени известных людей и крупнейших компаний. Классический биткойн-развод, и в этом не было бы ничего интересного, если бы не один важный нюанс: все эти аккаунты были настоящими – они действительно принадлежали известным людям и крупнейшим компаниям.

Сначала мошеннические сообщения стали появляться в Twitter-аккаунтах, напрямую связанных с криптовалютами: раздачу анонсировали основатель криптобиржи Binance Чанпэн Чжао, страницы нескольких других криптобирж, включая Coinbase, и тематический новостной сайт Coindesk.

Но этим дело не ограничилось, один за другим к этой мошеннической схеме стали присоединяться новые и новые аккаунты, принадлежащие бизнесменам, знаменитостям, политикам и компаниям: Apple, Uber, Бараку Обаме, Илону Маску, Ким Кардашьян, Биллу Гейтсу, Джо Байдену (который на тот момент еще не был президентом США), Джеффу Безосу, Канье Весту и так далее.

За те несколько часов, пока в Twitter искали корень проблемы, взломщикам удалось собрать более $100 000 – сумма немалая, но, конечно же, не идущая ни в какое сравнение с ударом по репутации социальной сети.

Довольно быстро выяснилось – хакерам удалось получить доступ к внутренней системе Twitter для управления аккаунтами, причем первоначально предполагалось, что в этом им помог некий инсайдер.

Однако на деле все оказалось иначе. Хакеров довольно быстро удалось найти и арестовать, причем руководителем коллектива взломщиков оказался американский школьник – семнадцатилетний (на момент взлома) Грэм Айван Кларк.

В итоге он получил 3 года тюрьмы и еще 3 года испытательного периода. Но главное, в процессе расследования удалось выяснить, что хакеры обошлись без помощи инсайдера. Вместо этого они использовали социальную инженерию и фишинг, чтобы получить доступ к системе от сотрудников Twitter.

Для начала они провели исследование в LinkedIn (американская социальная сеть для поиска и установления деловых контактов), с помощью которого выявили сотрудников, вероятно, имеющих доступ к системе управления учетными записями. После этого с помощью функции LinkedIn для рекрутеров они добыли контактную информацию этих сотрудников, включая номера сотовых телефонов. Далее они звонили работникам Twitter, представлялись коллегами и при помощи ранее собранных данных убеждали тех посетить фишинговый сайт, имитирующий страницу входа во внутренние системы Twitter.

Таким образом они заполучили пароли и коды двухфакторной аутентификации, с которыми смогли в итоге войти в систему управления учетными записями Twitter и завладеть десятками аккаунтов с миллионами подписчиков.

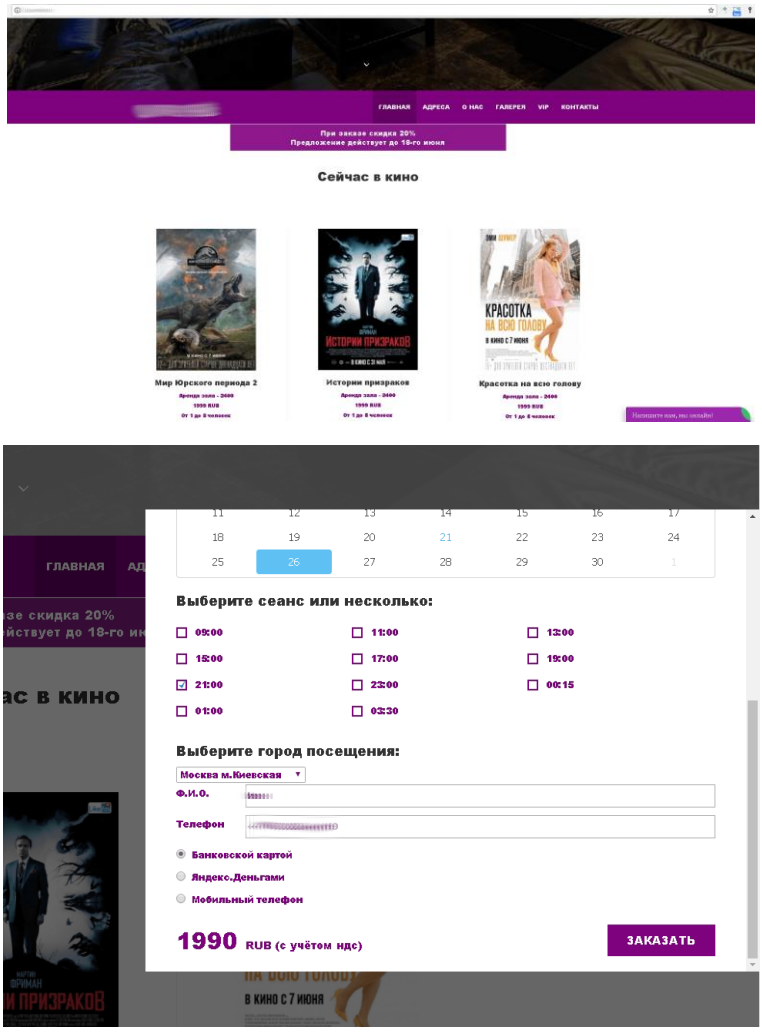
Другая история, связанная с фишингом, включала в себя психологические трюки в общении.

Схема, о которой пойдет речь, связана с частными кинозалами. Начинается все с того, что пользователю, разместившему анкету на сайте онлайн-знакомств, в один прекрасный день приходит сообщение от красивой девушки.

Фальшивый аккаунт формируется за счет фотографий реального человека, который размещает их в своих социальных сетях, не задумываясь и не зная, что их используют мошенники в своих целях.

После непродолжительного общения диалог подразумевает встречу в реальной жизни. Куда же сходить на первое свидание? Разумеется, в кино – такое предложение поступает с поддельного аккаунта.

Но предлагается сходить не в обычный кинотеатр, а в «как будто сделанный для вас двоих» – в частный кинозал, где кроме вас никого больше не будет. И присылается ссылка на сервис по бронированию билетов.



После выбора подходящего сеанса и ввода необходимой информации сайт перенаправляет на страницу оплаты. После этого у мошенников есть все данные банковской карты.

Следует отметить, что часто, при подделывании сайтов, мошенники формируют не весь его функционал, а только нужные страницы. В примере про кинотеатр сайт был полностью рабочим, с работающей службой поддержки, с указанием адресов в разных городах страны, при проверке которых через карты становилось ясно, что это какой-либо торговый центр с зоной развлечений.

Что могло выдать, что это фишинговый сайт?

- Графа «Счет получателя» при онлайн-оплате: в ней написано, что перевод отправится физическому лицу, но раздел с контактами на сайте утверждает, что владелец сети кинозалов – компания, то есть лицо юридическое.
- ИНН организации в разделе «Контакты»: при его проверке на сайте Федеральной налоговой службы получаем, что организация с таким ИНН имеет другое название и занимается другим направлением.
- Домен сайта: при проверке даты регистрации домена и его владельца через сервис WHOIS выяснилось, что его зарегистрировали на частное лицо, а не на организацию, и произошло это всего несколько недель назад, что является очень подозрительным.

В последнее время всё чаще мы сталкиваемся с претекстингом. Так как данный метод раскручивается по определенному сценарию, то рассмотрим распространенные мошеннические схемы:

- Получение какого-либо SMS с информацией неблагоприятного характер. Для разрешения поставленной проблемы требуется, в большинстве случаев, сделать денежный перевод на

указанный в сообщении телефонный номер и ни при каких обстоятельствах не выходить на контакт с данным человеком.

- Звонки от банков, управляющих компаний и т.д. Телефонные мошенники используют такой сценарий, чтобы ответы жертвы можно было использовать в своих целях (оформление кредитов, микро-займов и т.д.). Во многих случаях, параллельно телефонному разговору, требуется выполнение дополнительных действий, таких как ввод данных банковской карты на определенном сайте, установка какого-либо приложения и т.д.
- Использование нейросетей для подделки голоса, внешности пользователя. Чаще всего мошенники создают поддельный аккаунт в мессенджерах или социальных сетях и для правдоподобности присылают голосовые сообщения, в которых голос совпадает с голосом начальника, руководителя подразделения и т.д., суть сообщения – выполнения определенных действий, которые маскируются под благое дело, а фактически – потеря денежных средств или личных аккаунтов в социальных сетях, мессенджерах.

Рекомендации, которые позволят не поддаться воздействиям методов социальной инженерии:

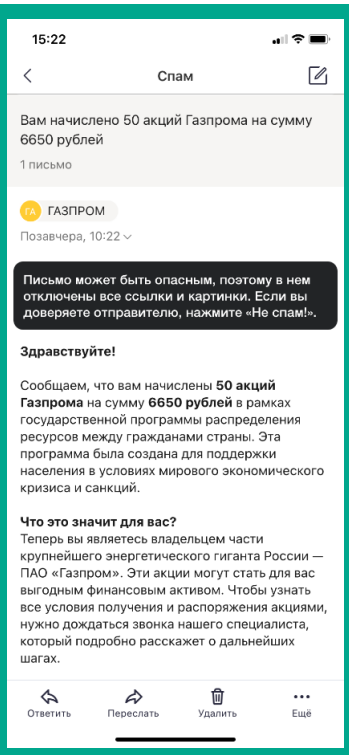
- Осведомленность об угрозах.
  Чем чаще мы осведомлены о различных событиях и ситуациях, тем больше мы к ним готовы, видя схожий сценарий проводимых манипуляций со стороны мошенников.
- Внимание на источник.
  Не переходим по сомнительным ссылкам, которые приходят в сообщениях или на электронную почту.
- Нет эмоциям.
  Если оппонент требует от нас мгновенных действий, то лучше взять паузу и обдумать, какие последствия могут быть. Не позволять незнакомым контактам манипулировать нашими эмоциями.
- Защита устройств.
  Устанавливаем приложения по защите личного информационного пространства, которые по своему функционалу могут проверять не только вредоносные приложения, но и спам, ссылки и сайты.
- Избегать общественных сетей.
  Подключаться к общественным сетям только в крайних случаях необходимости. А при онлайн покупке или авторизации на каких-либо сервисах использовать VPN, чтобы передаваемые данные были защищены методами шифрования.

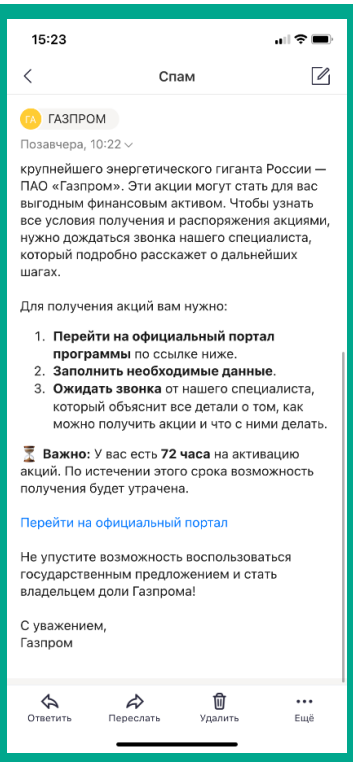
Вопросы к параграфу:

1. Почему понятие социальной инженерии рассматривается в контексте информационной безопасности?
2. Какие методы социальной инженерии Вам известны?
3. Как нейросети используются в мошеннических целях?
4. Каких рекомендаций следует придерживаться, чтобы не поддаваться воздействиям социальной инженерии?

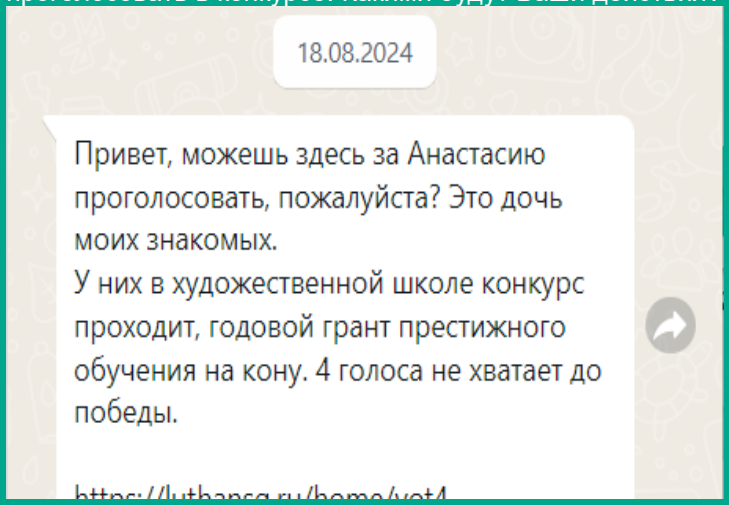
Ситуация:

1. Вы получаете на электронную почту письмо, которое информирует Вас о зачислении денежных средств, предварительно требующее заполнения личных данных и банковских карт. Какими будут Ваши действия?

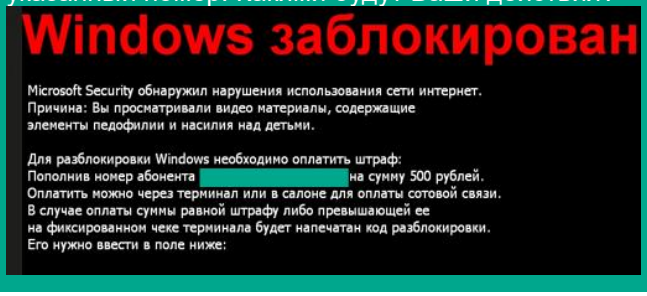




2. Вы получаете в мессенджере сообщение с просьбой проголосовать в конкурсе. Какими будут Ваши действия?



3. После установки приложения ПК перезагрузился и выдает сообщение на экране о недопустимом поведении в Интернете и требовании о переводе денежных средств на указанный номер. Какими будут Ваши действия?



kaspersky

§17. Инциденты информационной безопасности

Ключевые слова: Лаборатория Касперского, Windows, KUMA, Триангуляция, ILOVEYOU, Code Red, Tomiris, FinSpy, SteelFox, Trickbot, Necro, Harly, Sky Mavis, BlackCat, QBot, социальная инженерия, Telegram Wallet

Ежедневно Лаборатория Касперского сталкивается в среднем с 400 тыс. инцидентами информационной безопасности. Основная мишень злоумышленников – Windows. По статистике примерно 85% обнаруженных вредоносных файлов нацелено именно на эту ОС.

Ландшафт угроз становится всё более разнообразным, а злоумышленники активно используют мировую обстановку и новостную повестку для атак на пользователей. Есть все основания полагать, что и в следующем году число атак и объём вредоносного ПО продолжит расти.

Сегодня, чтобы совершить кибератаку, злоумышленнику необязательно самостоятельно совершать все её шаги и разрабатывать вредоносные инструменты. В даркнете доступны многочисленные предложения как вредоносного ПО, так и готового доступа в сети организаций. Рассмотрим конкретные инциденты информационной безопасности за последнее время.

Операция «Триангуляция»

Атака начиналась с невидимого сообщения iMessage, в котором было вредоносное вложение, обрабатывавшееся без ведома пользователя. Вся атака не требовала от пользователя никаких действий.

Эксперты Лаборатории Касперского смогли выявить атаку благодаря мониторингу корпоративной Wi-Fi-сети для мобильных устройств при помощи SIEM-системы KUMA.

В атаке использовались четыре уязвимости нулевого дня, которым были подвержены все устройства iOS до версии 16.2. Эксплойт «Триангуляции» мог работать и на современных вариантах iPhone, и на достаточно старых моделях.

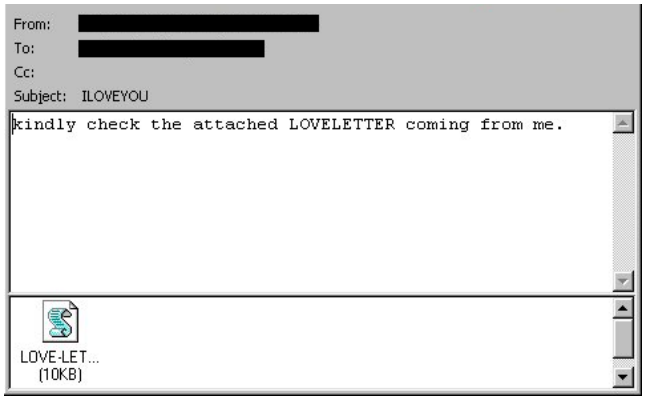
Применявшаяся уязвимость позволяла получить доступ ко всей физической памяти устройства на уровне пользователя, причем как на чтение, так и на запись.

Благодаря эксплуатации всех уязвимостей зловред мог получить полный контроль над устройством и запускать дальнейшую нагрузку, но вместо этого он запускал процесс IMAgent и через него удалял с устройства следы атаки, а также запускал процесс Safari в фоновом режиме и перенаправлял его на заранее подготовленную веб-страницу с эксплойтом уже под Safari. Эксплойт под этот браузер запускал дальнейшие этапы атаки.

Одна из уязвимостей iOS позволяла обходить механизм аппаратной защиты памяти, причем для этого использовались недокументированные и неиспользуемые прошивкой аппаратные регистры чипа. По версии экспертов, эта аппаратная функция была создана для отладки или тестирования и потом почему-то осталась включенной.

Сетевой червь «ILOVEYOU»

В 2000 году любой сервис с приставкой «e-» (электронный), любые сетевые технологии получали массу внимания и инвестиций. Некоторое разочарование инвесторов наступило чуть позже, в 2001 году, когда множество интернет-стартапов обанкротилось, а в индустрии стало чуть меньше хайпа и чуть больше смысла. В мае этого года пользователи электронной почты получали странное письмо с темой ILOVEYOU. В любви признавался знакомый человек. Это однозначно привлекает внимание, поэтому пользователи щелкали по вложенному файлу с именем «LOVE-LETTER-FOR-YOU.TXT.VBS».



Лишь через некоторое время обнаруживалось, что важные документы на жестком диске безнадежно испорчены, а еще одно любовное послание разослано уже от вашего имени по всем контактам в адресной книге почтового клиента.

ILOVEYOU был не первым зловредом, эксплуатирующим дыру в почтовых клиентах Microsoft Outlook. Но он точно инициировал одну из самых серьезных компьютерных эпидемий в начале нового тысячелетия.

Говоря строго, ILOVEYOU следует классифицировать как сетевого червя. Его ключевая особенность заключается в том, что изначальное заражение производится с помощью простейшей программы на языке программирования VBscript. VBscript, в свою очередь, развивает еще более древнюю идею макросов – по сути, простых программ, позволяющих автоматизировать определенные действия, например при работе с документами. Чаще всего макросы используются для проведения сложных расчетов в электронных таблицах, например в программе Microsoft Excel. С давних времен макросы поддерживались и в Microsoft Word, например для автоматической генерации отчетов на основе данных, введенных в форму.

Червь ILOVEYOU не использовал какую-то уязвимость в продуктах Microsoft, а задействовал штатную функциональность. Баг заключался только в том, что при запуске скрипта из почтового клиента Outlook не выводилось вообще никакого предупреждения.

Функциональность червя вовсе не ограничивалась рассылкой любовных сообщений всем адресатам. Помимо почтового спама от имени жертвы, он мог распространяться через мессенджер IRC (если тот был установлен на компьютере). Кроме того, червь загружал троянскую программу, которая отправляла создателю вируса пароли к почте и для доступа в Интернет.

ILOVEYOU объединил в себе разработки из предыдущих макровирусов, улучшил то, что сейчас называется социальной инженерией, добавил вредоносную функциональность и использовал возможности автоматического распространения по максимуму.

Создатель вируса даже не пытался скрыть вредоносный код под видом офисного документа. Имя файла LOVE-LETTER-FOR-YOU.TXT.VBS отчасти эксплуатировало особенность почтовых клиентов Microsoft, которые показывали только первую часть длинного названия, что видно на скриншоте. Внутри был, по сути, открытый для всех интересующихся исходный код, что моментально привело к появлению множества вариаций интернет-червя.

Итоговые оценки последствий работы вируса ILOVEYOU следующие: были заражены до 10% подключенных к Интернету компьютеров, а общий ущерб, учитывающий также деструктивные действия ILOVEYOU и его вариантов, оценивается примерно в 10 миллиардов долларов. Проблема широко обсуждалась в прессе, а в США даже проводились слушания в сенате.

Создателем интернет-червя ILOVEYOU является Онель де Гузман, на момент эпидемии ему было 24 года и он являлся студентом. В 2000 году сотрудники ФБР смогли определить, что первоначальные сообщения с вирусом были разосланы в популярные «листы рассылок» для пользователей из Филиппин, где до сих пор и живет де Гузман. В 2000 году он попал в список подозреваемых в авторстве ILOVEYOU. Но не получил наказания по двум причинам: недостаток улик и отсутствие на тот момент уголовной статьи за киберпреступления в местном законодательстве.

В 2020 году де Гузмана разыскали журналисты. Он рассказал им, что ILOVEYOU изначально не имел функции массовой рассылки по адресной книге Outlook, а создан был для кражи паролей для доступа в Интернет – его автору не хватало денег на оплату. Монетизировать свои вредоносные таланты де Гузману так и не удалось: на момент публикации статьи он работал в скромной мастерской по ремонту сотовых телефонов в Маниле.

Сетевой червь «Code Red»

Распространение интернет-червя Code Red, атакующего системы на базе Windows с установленным веб-сервером Microsoft IIS, удалось выявить в самом начале эпидемии. Первооткрывателями стали специалисты компании eEye Security: на момент обнаружения (13 июля 2001 года) они как раз занимались разработкой системы по поиску уязвимостей в Microsoft IIS. Их тестовый сервер неожиданно перестал отвечать на запросы. Вслед за этим последовала бессонная ночь, которую исследователи провели, изучая логи системы в поисках следов заражения. Зловред назвали по первому попавшемуся на глаза предмету: это была газировка Mountain Dew Code Red. Однако относительно раннее обнаружение не особо помогло остановить эпидемию. Зловред использовал уже зараженные системы для дальнейших атак и буквально за считанные дни распространился по всему миру.

Интернет-червь использовал уязвимость в одном из модулей веб-сервера – расширение для индексации данных. В библиотеке idq.dll была обнаружена ошибка переполнения буфера. По современным меркам это простейшая ошибка, которую можно проэксплуатировать, отправив на сервер чрезмерно длинный запрос такого вида:

```
GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u68
58%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a
HTTP/1.0
```

В результате данные после многочисленных символов N интерпретируются как инструкции и выполняются. Вся вредоносная нагрузка содержится непосредственно в запросе, то есть при наличии уязвимой инсталляции Microsoft IIS система заражается моментально и со стопроцентной гарантией. Самым заметным следствием заражения становился дефейс веб-сайта, обслуживаемого веб-сервером. Вместо его содержимого выводилась заглушка.

По информации Лаборатории Касперского, через 10 часов после успешной атаки червь восстанавливал нормальное содержимое веб-сайта. Дальнейшие действия зависели от даты. С 1 по 19 число каждого месяца червь занимался собственным распространением, отправляя вредоносные запросы по случайным

IP-адресам. С 20 по 27 число производилась DDoS-атака на ряд фиксированных IP-адресов, среди которых был адрес сайта администрации президента США. С 28 числа до конца месяца у Code Red были выходные.

Происшествия, подобные Code Red, происходят и по сей день, но чаще всего они связаны с уязвимостями нулевого дня.

Бэкдор «Tomiris»

Основная задача бэкдора Tomiris – доставка дополнительного вредоносного ПО на компьютер жертвы. Он постоянно опрашивает командный сервер злоумышленников, скачивает с него исполняемые файлы и запускает с указанными аргументами. Эксперты Лаборатории Касперского обнаружили вариант Tomiris, который умел похищать файлы. Зловред выбирал недавно созданные файлы с определенными расширениями (.doc, .docx, .pdf, .rar и т.д.), а затем закачивал их на командный сервер.

Авторы бэкдора снабдили его рядом функций, цель которых – обмануть защитные технологии и запутать расследование инцидента. Так, попадая на компьютер, зловред ничего не делает девять минут, вероятно, для обмана механизмов детектирования на базе песочницы. Внутри Tomiris не закодировано точного адреса командного сервера, он получает URL и порт от промежуточного звена.

Для доставки бэкдора на компьютер жертвы злоумышленники используют тактику перенаправления DNS-запросов. Каким-то образом (вероятно, получив учетные данные от контрольной панели на сайте регистратора доменных имен) они перенаправляют на собственные ресурсы трафик с почтовых серверов атакуемых организаций. В результате клиенты попадают на сайт, имитирующий оригинальную страницу логина для веб-интерфейса почтового сервиса. Введенные учетные данные незамедлительно попадали в руки злоумышленников. Однако иногда сайт выдавал нотификацию о необходимости установки обновления безопасности, без которого продолжить работу с сервисом невозможно. В качестве обновления скачивался загрузчик бэкдора Tomiris.

Шпионское ПО «FinSpy»

FinSpy – коммерческая шпионская программа, которой пользуются силовые структуры и государственные органы разных стран. Впервые она попала на радары исследователей в 2011 году, когда на Wikileaks появились связанные с ней документы. В 2014 году исходный код зловреда выложили в Интернет, однако на этом его история не закончилась: разработчики переписали FinSpy, и он до сих пор продолжает заражать устройства по всему миру.

В отличие от шпионских программ, нацеленных на какую-то определенную ОС, FinSpy универсален: у него есть версии и для компьютеров под управлением Windows, macOS и Linux, и для мобильных устройств с Android и iOS. В зависимости от платформы его возможности могут различаться, однако в любом варианте это опасный зловред, способный добираться до жертвы различными способами и тайком передавать своим хозяевам множество данных о ней.

FinSpy не ограничивается одним методом заражения. Например, зловред может скрываться в зараженных дистрибутивах приложений для ОС. Эксперты Лаборатории Касперского обнаружили множество таких программ, в их числе установщики TeamViewer, VLC Media Player, WinRAR и другие. Если жертва загрузит и выполнит модифицированное приложение, оно запустит многоступенчатую цепочку заражения.

Кроме того, был обнаружен загрузчик зловреда в компонентах, которые загружаются до операционной системы. Это UEFI – интерфейс, с помощью которого операционная система взаимодействует с «железом», и MBR – загрузочная запись, которая нужна, чтобы запустить Windows. В обоих случаях FinSpy устанавливается на компьютер при включении.

FinSpy располагает широкими возможностями для слежки за пользователями. Так, версии зловреда для ПК может:

- Включать микрофон и записывать или транслировать злоумышленникам все, что он слышит;
- Записывать или передавать злоумышленникам в реальном времени все, что пользователь вводит на клавиатуре;

- Включать камеру и записывать или транслировать изображение с нее;
- Копировать файлы, которые пользователь изменяет, отправляет на печать, получает, удаляет и так далее;
- Снимать скриншоты или захватывать участок экрана там, где пользователь кликает мышью;
- Воровать письма из клиентов Thunderbird, Outlook, Apple Mail и Icedove;
- Перехватывать контакты, чаты, звонки и файлы в Skype.

В дополнение к этому версия FinSpy для Windows может подслушивать VoIP-звонки, перехватывать сертификаты и ключи шифрования для определенных протоколов, а также загружать и запускать утилиты для сбора криминалистических данных. Помимо вышеперечисленного, Windows-версия шпиона умеет еще и заражать смартфоны Blackberry.

Мобильные версии FinSpy умеют прослушивать и записывать звонки, читать SMS и следить за активностью пользователя в мессенджерах, таких как WhatsApp, WeChat, Viber, Skype, Line, Telegram, Signal и Threema. Кроме того, мобильный шпион отправляет злоумышленникам список контактов и звонков жертвы, мероприятия из календаря, информацию о местоположении устройства и многое другое.

Троянец «SteelFox»

В августе 2024 года команда Лаборатории Касперского обнаружила новый образец вредоносного ПО, который назвали SteelFox. В этих атаках задействуется сложная цепочка, включающая использование шелл-кода, а также злоупотребление службами и драйверами Windows. Троянец написан на C++ с использованием сторонних библиотек и способен похищать различные пользовательские данные, которые могут заинтересовать организаторов этой кампании. Распространяется угроза через форумы, торрент-трекеры и блоги, маскируясь под такие популярные программы, как Foxit PDF Editor и AutoCAD, и с помощью стилера собирает данные о банковских картах жертв, а также информацию о зараженном устройстве.

Атака не направлена на отдельных лиц или конкретные организации. Троянец действует с большим размахом, массово заражая всех, кто сталкивается со скомпрометированным ПО. На момент проведения исследования защитные решения Лаборатории Касперского обнаружили угрозу более 11 тыс. раз. Жертвами этой кампании стали пользователи со всего мира, большинство из них находятся в Бразилии, Китае, России, Мексике, ОАЭ, Египте, Алжире, Вьетнаме, Индии и Шри-Ланке.

Троян «Trickbot»

В октябре 2016 года, решения Лаборатории Касперского начали сталкиваться с трояном под названием Trickbot. Тогда он встречался в основном у домашних пользователей и применялся для кражи учетных данных от сервисов онлайн-банкинга. Однако за последние годы создатели этого зловреда развили достаточно бурную деятельность и превратили банковский троян в многофункциональный модульный инструмент.

На сегодняшний момент Trickbot пользуется популярностью у нескольких преступных группировок в качестве системы доставки сторонних зловредов в инфраструктуру компаний. Основная цель современного варианта – проникновение и распространение в локальных сетях. Далее операторы могут использовать его для решения множества разных задач – от предоставления захваченной площадки сторонним злоумышленникам до кражи конфиденциальных и данных. Возможности трояна Trickbot:

- Перехватывать веб-трафик на зараженном компьютере.
- Обеспечивать удаленное управление устройством.
- Воровать файлы cookie из браузеров.
- Красть учетные данные, сохраненные в реестре, базах данных различных приложений, конфигурационных файлах и файлы данных криптовалютных кошельков.
- Перехватывать информацию из механизмов автозаполнения форм в веб-браузерах.
- Перехватывать информацию из форм для ввода данных на банковских веб-сайтах.
- Внедрять вредоносные скрипты в веб-страницы.
- Собирать учетные данные из профиля Outlook, перехватывать электронные письма в Outlook и рассылать через него спам.

- Получать низкоуровневый доступ к аппаратному обеспечению.
- Находить адреса SQL-серверов и выполнять поисковые запросы по ним.
- Создавать VPN-подключения.

Троян «Necro»

В 2019 году эксперты Лаборатории Касперского обнаружили троян в приложении для распознавания текста CamScanner, которое пользователи Android загрузили из Google Play более 100 миллионов раз.

Necro сегодня – это загрузчик, который имеет запутанный код, чтобы избежать детектирования. Вредоносную нагрузку он скачивает не менее хитрым образом: прячет ее код в безобидной с виду картинке, используя стеганографию.

Скачанные вредоносные модули умеют загружать и запускать любые DEX-файлы (скомпилированный код Android-приложения), устанавливать скачанные приложения, запускать туннель через устройство жертвы и (потенциально) оформлять платные подписки. Кроме того, в невидимых окнах они могут показывать рекламу и взаимодействовать с ней, а также открывать произвольные ссылки и выполнять любой JavaScript-код.

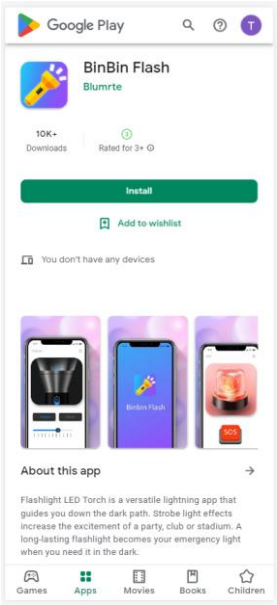
Следы вредоносного ПО были обнаружены в пользовательской версии Spotify, в приложении для редактирования фото Wuta Camera, в браузере Max Browser, в модах для WhatsApp, Minecraft и других популярных игр. Мод для Spotify распространялся по неофициальным каналам, а приложение Wuta Camera с Necro находилось в Google Play, откуда это приложение с трояном внутри скачали более 10 миллионов раз.

Троян «Harly»

С 2020 года в Google Play было обнаружено более 190 приложений, зараженных Harly. Судя по нижней границе данных по количеству скачиваний приложения в магазине, суммарно его установили более 4,8 миллиона раз. При этом реальное число скачиваний может быть намного больше.

Трояны семейства Harly имитируют легитимные приложения. Злоумышленники скачивают обычные приложения из Google Play и внедряют в них вредоносный код, после чего загружают их в магазин под другим именем. При этом приложения могут сохранять заявленные в описании функции, так что пользователь не подозревает о наличии угрозы. Трояны этого семейства сразу содержат всю полезную нагрузку внутри приложения и различными способами расшифровывают ее для запуска.

В качестве примера рассмотрим приложение-фонарик с количеством загрузок более 10 тыс.



При его запуске загружается подозрительная библиотека, в которой происходит расшифровка файла из ресурсов приложения. Авторы зловредов научились писать на языках программирования Go и Rust, правда, пока только расшифровку и загрузку вредоносного SDK.

Как и другие трояны подобного рода, Harly собирает информацию об устройстве пользователя, в особенности о мобильной сети. Телефон пользователя переключается на мобильную сеть, после чего троян запрашивает у командного сервера конфигурацию и список подписок, которые необходимо оформить.

Рассматриваемый троян работает только с тайскими операторами, поэтому он проверяет коды мобильной сети – уникальные идентификаторы операторов связи.

В невидимом окне троян открывает адрес подписки, с помощью инъекции JS-скриптов вводит номер телефона пользователя, нажимает нужные кнопки и подставляет проверочный код, извлеченный из пришедшего на телефон SMS. В результате без ведома пользователя на него оформляется подписка.

Еще одна интересная особенность этого трояна – он умеет оформлять подписки, защищенные не только SMS-кодом, но и телефонным звонком: троян совершает звонок по определенному номеру, подтверждая оформление подписки.

Ограбление Sky Mavis

История произошла в 2022 году. Главную роль в ней сыграла компания Sky Mavis, создавшая NFT-игру Axie Infinity. Эта игра позволяет пользователям зарабатывать криптовалюту. Причем одно время некоторые жители Юго-Восточной Азии ходили в нее как на работу. На пике популярности дневная аудитория игры доходила до 2,7 миллиона человек, а выручка до 215 миллионов долларов в неделю.

Однако в марте 2022 года, еще до того у Sky Mavis случилась серьезная неприятность. В ходе атаки на блокчейн-платформу Ronin, которая является основной всей криптовалютной деятельности в Axie Infinity, взломщикам удалось увести со счетов компании около 540 миллионов долларов.

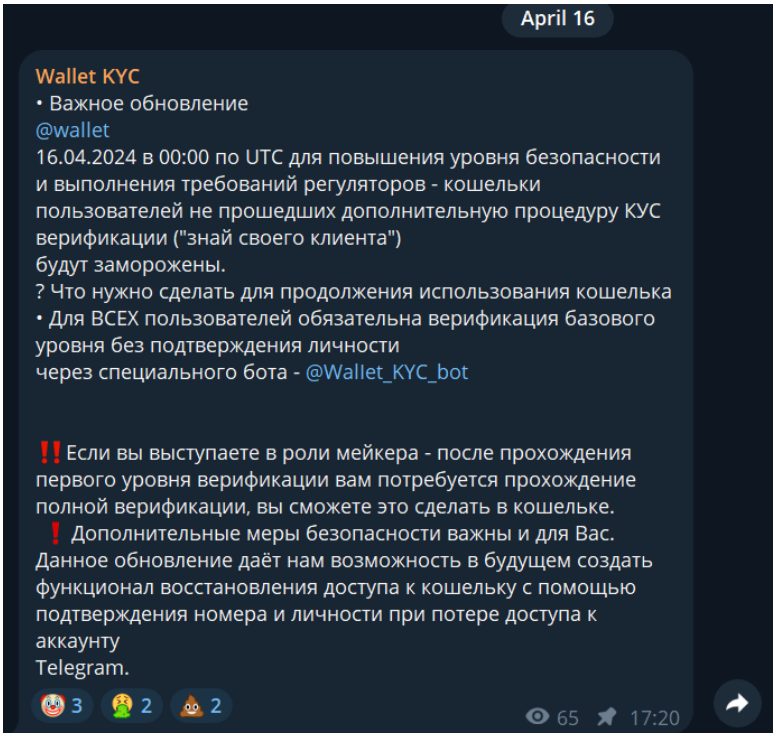
В июле того же года стали известны подробности ограбления. Оказалось, что хакеры от имени некой фейковой компании связывались на LinkedIn с сотрудниками Sky Mavis и приглашали их проходить собеседования для трудоустройства. Таким образом им удалось выйти на одного из старших инженеров Sky Mavis, которому после нескольких раундов собеседований они сделали крайне заманчивое предложение работы. Фейковый оффер был прислан в зараженном PDF-файле. С его помощью взломщики в итоге получили доступ во внутреннюю сеть компании. Используя доступ в корпоративную сеть, хакеры смогли раздобыть необходимое для подтверждения транзакций количество секретных ключей и успешно вывести криптовалюту. Отмывали украденные средства они через сложную схему, задействовавшую два криптомиксера, порядка 12 тыс. промежуточных криптокошельков и конвертацию в BTC с последующим обналичиванием уже через биткойн.

По заявлениям аналитиков, помогавших правоохранительным органам США расследовать атаку, к взлому имела отношение северокорейская группировка Lazarus. Вернуть удалось лишь небольшую часть похищенной криптовалюты (около 10% в номинальных монетах или около 5%, если считать в долларах).

Угон аккаунтов и криптокошельков в Telegram

Говоря о мессенджере Telegram и его функционале, киберпреступники сфокусировались на владельцах криптокошельков Telegram Wallet, которые совершают сделки по P2P-торговле (это когда пользователи могут покупать и продавать криптовалюту без посредников).

Как только потенциальная жертва найдена, мошенники связываются с ней под видом легитимного покупателя или продавца, в зависимости от контекста. Одним из первых же предложений в переписке становится просьба пройти KYC-верификацию (Know Your Customer – «Знай своего клиента»). Это реальное требование Telegram Wallet, направленное на повышение уровня безопасности платформы. Пользователям на самом деле требуется предоставить свои реальное имя, номер телефона и адрес, чтобы совершать сделки. Но есть нюанс: мошенники отправляют ссылку на фейковый канал для прохождения KYC-верификации и угрожают заморозкой криптоактивов в случае, если жертва проигнорирует просьбу. Для большей убедительности криптомошенники упоминают выдуманные «требования регуляторов».



Как определить, что канал принадлежит мошенникам: малое число просмотров поста, синтаксические ошибки и активный призыв перейти по ссылке

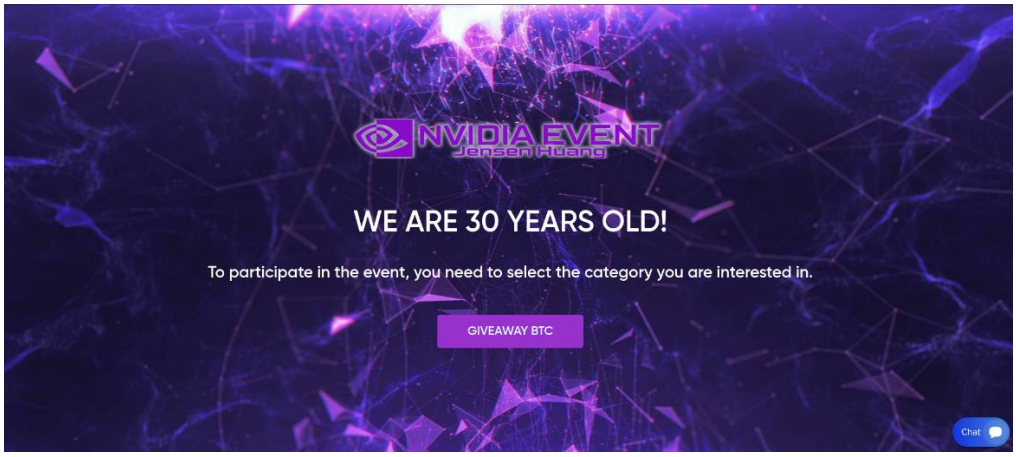
Самое интересное в этом канале – ссылка на якобы официального бота, который нужен для прохождения KYC-верификации. Жертве предлагается следовать несложной инструкции.

Первый шаг жертвы – поделиться с ботом своим номером телефона. Мошенник узнает номер, необходимый для авторизации в аккаунте жертвы. После бот попросит отключить двухфакторную аутентификацию и подскажет, как выключить облачный пароль. Мошенник будет уверен, что ничего не помешает ему как можно скорее захватить аккаунт. Заключительный шаг – введение кода для входа в Telegram. Мошенник ликует, так как жертва сама выдала ему свой номер телефона, отключила защиту, а в придачу выдала одноразовый пароль для входа.

После прохождения всех этих шагов жертва теряет доступ не только к личному аккаунту, но и к криптовалютному кошельку Telegram Wallet.

Фальшивый розыгрыш биткойнов от Nvidia

Злоумышленники создали фальшивый сайт, якобы посвященный юбилею Nvidia, и вывесили на нем объявление о розыгрыше крупной суммы биткойнов. При входе на сайт пользователь видит фиолетовый логотип компании, а не зеленый, и имя генерального директора, Дженсена Хуанга (Jensen Huang). Здесь же посетителей просят «выбрать категорию», чтобы принять участие в «событии». Однако по факту выбирать не из чего, под приглашением есть только одна большая кнопка с надписью «розыгрыш биткойнов».



После нажатия на кнопку пользователь попадает на страницу с подробной информацией о мифическом розыгрыше. На первый взгляд она выглядит убедительно: тут есть и фото генерального директора, и приятный дизайн, и дополнительные разделы меню. Правда, на месте логотипа Nvidia находится значок биткойна, а в текстах на сайте много грамматических ошибок.

Здесь же от лица господина Хуанга и всего Nvidia злоумышленники объявляют розыгрыш 50 тысяч биткойнов. Одно из главных условий участия – пользователь сам сперва делает определенный взнос, как будто покупает лотерейный билет. Мошенники обещают, что участник сразу же получит свои деньги обратно в двойном размере, а в перспективе еще и те самые 50 тыс. биткойнов.

Под инструкцией для участников был указан адрес криптокошелька, на который нужно было перевести деньги. А в самом низу проходила онлайн-трансляция «выигрышей», которые пользователи получают от организаторов. Чтобы укрепить образ легитимного сайта, мошенники организовали онлайн-чат техподдержки с фальшивой Nvidia.

При проверке адреса криптокошелька мошенников на сайте blockchain.com, окажется, что на него действительно приходили деньги. В общей сложности на счет преступников перевели 0,42 биткойна. Неизвестно, кто их отправлял. Это могли быть как жертвы, так и сами злоумышленники: например, чтобы проверить доступ к кошельку или изобразить действия участников «лотереи».

Шифровальщик «BlackCat»

После ухода группировок BlackMatter и REvil неизбежно должны были появиться новые игроки. Одним из них является группировка ALPHV, известная как BlackCat.

Создатели шифровальщиков из BlackCat предлагают свои услуги по схеме Ransomware-as-a-Service (RaaS), то есть предоставляют другим злоумышленникам доступ к своей инфраструктуре и вредоносному коду за процент от выкупов. Кроме того, они, вероятно, берут на себя переговоры с жертвой. Таким образом, все, что остается оператору – получить доступ к корпоративной среде, так что разработки BlackCat применяются для атак на компании разного размера по всему миру.

В арсенале BlackCat имеется одноименный шифровальщик. Он написан на языке Rust, благодаря чему злоумышленникам удалось добиться определенной кроссплатформенности (варианты зловреда существуют и под Windows, и под Linux). Кроме того, они используют утилиту Fendr, которая служит для эксфильтрации данных из зараженной инфраструктуры.

Среди инцидентов с применением шифровальщика BlackCat эксперты Лаборатории Касперского видели как минимум одну атаку на южноамериканскую промышленную компанию, занимающуюся полезными ископаемыми и строительством, а также заражение нескольких клиентов ближневосточного ERP-провайдера (организации, предоставляющей инструменты для планирования ресурсов предприятия).

Беспокойство вызывает модернизация, которую претерпел инструмент Fendr. Теперь он умеет автоматически выкачивать гораздо более широкий спектр файлов. Ему добавили способность находить

файлы с расширениями *.sqlite, *.catproduct, *.rdp, *.accdb, *.catpart, *.catdrawing, *.3ds, *.dwt и *.dxf. Файлы этих типов используются приложениями для промышленного дизайна и инструментами для удаленного доступа. Это может означать, что создатели зловреда нацелены на промышленные среды.

Троянец «QBot»

QBot – это банковский троянец, существующий уже более тринадцати лет. Он был обнаружен в 2007 году и с тех пор постоянно совершенствуется. Его основная цель – кража учетных данных (логинов, паролей и т.д.) для входа в финансовые сервисы. Помимо этого, он может шпионить за банковской деятельностью организации, распространяться по сети и устанавливать программы-шифровальщики для получения максимальной прибыли от атаки на организации.

QBot постоянно совершенствуется, получая новые возможности и применяя новые техники: он записывает нажатия клавиш, выполняет функции бэкдора и использует различные приемы для защиты от обнаружения. Из последних функций стоит отметить обнаружение виртуальных сред, регулярное самообновление и изменение схем шифрования и упаковки бинарного кода. Кроме того, QBot старается защитить себя от анализа и отладки вручную или с помощью автоматизированных инструментов.

Еще одна интересная функция – перехват электронных писем. Злоумышленники впоследствии используют их для целевых рассылок: содержащаяся в них информация может помочь убедить жертву открыть вредоносное письмо.

QBot известен тем, что заражает системы жертв в основном через спам. В некоторых случаях письма содержат вложенные документы Microsoft Office (Word, Excel) или защищенные паролем архивы с такими файлами. В документах присутствуют вредоносные макросы. Пользователям предлагается открыть вложение, потому что оно якобы содержит важную информацию. В других письмах злоумышленники рассылают ссылки на страницы загрузки вредоносных документов.

Помимо спам-рассылок злоумышленники используют еще один вектор заражения, который предусматривает загрузку полезной нагрузки QBot на компьютер жертвы с помощью другого вредоносного ПО, уже присутствующего на нем.

Как правило, злоумышленники выбирают тот вектор заражения, который считают наиболее действенным для конкретной организации. Известно, что многие преступники заранее собирают и анализируют информацию о целевых организациях из открытых источников, чтобы решить, какой вектор заражения будет наиболее эффективен.

Цепочка заражения для последних вариантов QBot (2020-2021 гг.) выглядит следующим образом:

- Пользователь получает фишинговое письмо с вложенным ZIP-архивом, содержащим документ Office со встроенным макросом или незаархивированным документом; также в письме может быть ссылка для загрузки исполняемого файла QBot.
- Пользователь открывает вредоносное вложение или ссылку и соглашается включить содержимое документа.
- Выполняется вредоносный макрос. Некоторые варианты зловреда отправляют GET-запрос на загрузку файла PNG. Однако на самом деле это бинарный исполняемый файл.
- Загруженная полезная нагрузка (промежуточный компонент) включает в себя другой бинарный файл, содержащий зашифрованные модули ресурсов. Один из зашифрованных ресурсов содержит двоичный файл DLL (загрузчик), который расшифровывается позже при выполнении вредоносного файла.
- Промежуточный компонент загружает в память загрузчик, который дешифрует и выполняет полезную нагрузку. Параметры конфигурации извлекаются из другого ресурса.
- Полезная нагрузка взаимодействует с командным сервером.
- На зараженный компьютер могут загружаться дополнительные вредоносные программы, например программа-шифровальщик ProLock.

К стандартным функциям QBot относятся сбор учетных данных, подбор паролей, манипуляции с реестром (закрепление в системе), копирование себя, внедрение кода в процессы, чтобы скрыть вредоносную активность.

Вопросы к параграфу:

1. Из рассмотренных инцидентов информационной безопасности, что можно отнести к:
   - Фишингу;
   - Социальной инженерии;
   - Вредоносному ПО?
2. Каких рекомендаций следует придерживаться, чтобы рассмотренные инциденты не повторились?

§18. Элементы области искусственного интеллекта и информационная безопасность

Ключевые слова: искусственный интеллект, нейросеть, машинное обучение, персональные данные, ChatGPT

Инструменты искусственного интеллекта (ИИ) встречаются везде – от операционных систем и офисных пакетов до графических редакторов и чатов. Взрывной рост приложений, сервисов и плагинов для работы с искусственным интеллектом будет лишь ускоряться. Элементы искусственного интеллекта внедряют в давно привычные инструменты – от офисных программ и графических редакторов до сред разработки вроде Visual Studio. Программисты создают тысячи новых приложений, обращающихся к крупнейшим ИИ-моделям. Но в этой гонке пока никто не сумел решить проблемы безопасности – не организовать полноценную защиту от футуристического «злого искусственного интеллекта», а хотя бы минимизировать проблемы с утечкой конфиденциальных данных или выполнением хакерских действий на личных аккаунтах и устройствах через разнообразные ИИ-инструменты. Пока не придумано готовых коробочных решений для защиты пользователей ИИ-ассистентов.

Хотя автоматизация и машинное обучения используются в ИБ почти 20 лет, эксперименты в этой области не останавливаются ни на минуту. Защитникам нужно бороться с более сложными киберугрозами и большим числом атак без существенного роста бюджета и численности ИБ-отделов. ИИ помогает значительно разгрузить команду аналитиков и ускорить многие фазы работы с инцидентом – от обнаружения до реагирования. Но ряд очевидных, казалось бы, сценариев применения машинного обучения оказываются недостаточно эффективными.

Рассмотрим два основных и давно протестированных способа применения машинного обучения:

- **Поиск атак.** Обучив ИИ на примерах фишинговых писем, вредоносных файлов и опасного поведения приложений, можно добиться приемлемого уровня обнаружения схожих угроз. Основной подводный камень – эта сфера слишком динамична, злоумышленники постоянно придумывают новые способы маскировки, поэтому модель нужно очень часто обучать заново, чтобы поддерживать ее эффективность. При этом нужен размеченный набор данных, то есть большой набор свежих примеров доказанного вредоносного поведения. Обученный таким образом алгоритм не эффективен против принципиально новых атак, которые он не анализировал раньше. Кроме того, есть определенные сложности при обнаружении атак, целиком опирающихся на легитимные ИТ-инструменты. Несмотря на ограничения, этот способ применяется большинством производителей

ИБ-решений, например, он весьма эффективен для анализа e-mail, поиска фишинга, обнаружения определенных классов вредоносного ПО. Однако ни полной автоматизации, ни 100%-ной надежности он не обещает.

- **Поиск аномалий.** Обучив ИИ на «нормальной» деятельности серверов и рабочих станций, можно выявлять отклонения от этой нормы, когда, например, бухгалтер внезапно начинает выполнять административные действия с почтовым сервером. Подводные камни – этот способ требует собирать и хранить очень много телеметрии, переобучать ИИ на регулярной основе, чтобы он поспевал за изменениями в ИТ-инфраструктуре. Но все равно ложных срабатываний будет немало, да и обнаружение атак не гарантировано. Поиск аномалий должен быть адаптирован к конкретной организации, поэтому применение такого инструмента требует от сотрудников высокой квалификации как в сфере кибербезопасности, так и в анализе данных и машинном обучении.

Элементы искусственного интеллекта прекрасно подходят для решения рутинных задач, в которых предметная область и характеристики объектов редко и медленно меняются: написание связных текстов, распознавание пород собак и тому подобное. Когда за изучаемыми данными стоит активно сопротивляющийся этому изучению человеческий ум, статично настроенный ИИ постепенно становится менее эффективен. Аналитики дообучают и настраивают его вместо того, чтобы писать правила детектирования киберугроз. Фронт работ меняется, но экономии человеческих сил не происходит. При этом стремление повысить уровень ИИ-детектирования угроз неизбежно приводит к увеличению и числа ложноположительных срабатываний, а это напрямую увеличивает нагрузку на людей. В результате ИИ занимает свое место в ансамбле инструментов детектирования, но не способен стать «серебряной пулей», то есть окончательно решить проблемы детектирования в информационной безопасности или работать полностью автономно.

Стремительное развитие ИИ-систем и попытки их повсеместного внедрения вызывают и оптимизм, и опасения. Искусственный интеллект способен помочь человеку в самых разных областях деятельности, и индустрия кибербезопасности знает об этом не понаслышке. Например, в «Лаборатории Касперского» применяется машинное обучение уже почти 20 лет, без ИИ-систем в принципе невозможно защититься от гигантского количества существующих киберугроз. За это время компания идентифицировала и широкий спектр проблем, которые могут порождаться использованием элементов искусственного интеллекта – от обучения на некорректных данных и злонамеренных атак на ИИ-системы до применения в неэтичных целях.

Различные площадки и международные организации уже разработали общие принципы этичного искусственного интеллекта (например, рекомендации ЮНЕСКО), однако более конкретные руководства для индустрии кибербезопасности пока не стали общепринятыми.

Чтобы применять искусственный интеллект в кибербезопасности без негативных последствий, «Лаборатория Касперского» предлагает индустрии принять Этические принципы ИИ. Разумеется, принципы требуют обсуждения в индустриальном сообществе и уточнения, однако мы их придерживаемся уже сейчас.

Что же это за принципы? Рассмотрим краткую версию:

- **Прозрачность и объяснимость.** Пользователь имеет право знать, что обеспечивающая его безопасность компания использует ИИ-системы. Знать, в каких целях и каким образом эти системы принимают решения. Поэтому мы обязуемся разрабатывать системы ИИ, работа которых интерпретируема и объяснима в максимально возможном объеме, а также внедрять необходимые предосторожности и защитные меры, чтобы ИИ-системы генерировали корректные результаты. При необходимости с кодом, техническими и бизнес-процессами «Лаборатории Касперского» можно ознакомиться, посетив один из центров прозрачности компании.
- **Безопасность использования.** Среди угроз, связанных с использованием ИИ-систем, важное место занимают атаки, в которых кто-то манипулирует входными данными, чтобы спровоцировать ИИ-систему на неверное решение. Поэтому мы считаем, что разработчики должны иметь своим приоритетом устойчивость и безопасность ИИ. Для этого мы принимаем целый ряд практических мер, обеспечивающих высокое качество ИИ-систем: аудиты безопасности с фокусом на специфику ИИ и red-teaming, минимизацию использования сторонних наборов данных в обучении и целый ансамбль

различных технологий для создания многослойной защиты. По возможности рекомендуем предпочитать ИИ, основанный на облачных технологиях вместо локально установленных моделей.

- **Человеческий контроль.** Хотя наши системы машинного обучения могут работать автономно, результаты и качество их работы постоянно отслеживаются специалистами. При необходимости вердикты автоматических систем корректируются, а сами системы адаптируются и модифицируются экспертами, чтобы противостоять принципиально новым или очень сложным киберугрозам.
- **Конфиденциальность.** Обучение ИИ невозможно без огромных массивов информации, при этом их часть может оказаться персональными данными. Этичный подход к обучению требует, чтобы права человека на защиту личных данных строго соблюдались. На практике в информационной безопасности это может выражаться в целом ряде мер: ограничении типов и количества обрабатываемых данных, использовании псевдонимизации и анонимизации, обеспечении целостности данных, применении технических и организационных мер для защиты данных.
- **Применение в защитных целях.** Технологии ИИ в сфере кибербезопасности должны применяться сугубо в защитных целях.
- **Открытость к диалогу.** Мы считаем, что преодолеть препятствия, связанные с внедрением и использованием искусственного интеллекта в целях безопасности можно только сообща. Поэтому мы стремимся к диалогу со всеми заинтересованными сторонами, чтобы делиться передовым опытом этического использования ИИ.

В последнее время всё чаще слышны новости о развитии и использовании ChatGPT. Возникает вопрос: как использовать данную нейросеть без угрозы для своей цифровой безопасности?

Политика конфиденциальности OpenAI, компании-разработчика ChatGPT, вполне недвусмысленно уведомляет, что все диалоги с чат-ботом сохраняются и могут быть использованы для нескольких целей: для решения технических проблем или работы с нарушениями; данные могут быть использованы для обучения новых версий GPT и других «усовершенствований продукта».

Поэтому следует помнить: все, что пользователь напишет чат-боту, может быть использовано против него. При общении с ИИ рекомендуется соблюдать меры предосторожности. Не отправляйте чат-боту никакие персональные данные и не загружайте документы.

Внимательно изучите политику конфиденциальности и доступные настройки своего поставщика языковой модели – с их помощью обычно можно минимизировать отслеживание. Например, в разработках OpenAI можно отключить сохранение истории чатов – тогда через 30 дней данные будут удалены и никогда не будут использоваться для обучения. У тех, кто пользуется решениями OpenAI по API, через сторонние клиентские приложения или сервисы, эта настройка подключается автоматически.

Программистам, использующим ИИ-ассистенты для проверки и доработки кода, следует исключать API-ключи, адреса серверов и другую информацию, выдающую структуру приложения и серверной инфраструктуры.

Вопросы к параграфу:

1. Почему возможности искусственного интеллекта рассматриваются в контексте информационной безопасности?
2. В чем плюсы и минусы использования машинного обучения в различных сферах?
3. Как рекомендательная система маркетплейсов и онлайн-кинотеатров связана с машинным обучением?
4. Всегда ли ответ на запрос, сгенерированный нейросетями, будет истинным?

kaspersky

Задание:

1. Проведите сравнительный анализ функционала нейросетей по генерации изображений: Шедеврум от компании Яндекс, Kandinsky от компании Сбер.
2. Отправьте запрос «ПРОГРАММНЫЙ КОД НА ПАЙТОНЕ ПО НАХОЖДЕНИЮ ПЛОЩАДИ ТРАПЕЦИИ» в нейросети ChatGPT и Алису от компании Яндекс. Проанализируйте полученные ответы.
3. Отправьте запрос «РЕЦЕПТ СВИНЫХ КРЫЛЫШЕК» в нейросети ChatGPT и Алису от компании Яндекс. Есть ли аномалия в запросе и полученных ответах?

§19. Пути защиты личного информационного пространства

Ключевые слова: киберугрозы, пароль, менеджер паролей, двухфакторная аутентификация, автообновление, социальная инженерия

С киберпреступниками рано или поздно сталкиваются практически все. Интернет-мошенники стали настоящей эпидемией последних лет. Если раньше на их уловки попадались в основном люди преклонного возраста, то сейчас жертвой аферистов может стать и банковский работник, и служащий силовых структур, и сотрудник сферы информационной безопасности. Если все время откладывать на потом свою кибербезопасность, потому что эта тема кажется слишком сложной, то в этом параграфе собрана информация о возможных методах защиты себя и своего личного информационного пространства от угроз, с которыми можно столкнуться.

Автоматизируйте пароли

Пароли к каждому сайту и приложению должны быть длинными (минимум 12 символов) и никогда не должны повторяться. Придумывать и запоминать столько паролей не может никто, поэтому храните, создавайте и вводите их при помощи менеджера паролей. Придется придумать и запомнить только один (длинный!) мастер-пароль к нему, а все остальное – от создания до заполнения паролей – будет происходить автоматически.

Менеджер паролей нужно установить на все личные устройства, чтобы вводить пароли с удобством повсюду. Данные будут синхронизироваться между всеми устройствами, и, сохранив пароль в смартфоне, вы сможете автоматически подставить его в поле ввода на компьютере, и наоборот.

Во многих менеджерах паролей можно хранить в зашифрованном виде не только пароли, но и пин-коды, данные кредитных карт, адреса, заметки и сканы документов.

Включите двойную проверку

Двухфакторная аутентификация защищает пользователя от хакеров, не позволяя зайти в личные аккаунты с украденным паролем. Кроме пароля потребуется ввести одноразовый код, присланный по SMS или в приложение.

Хотя банки сейчас включают двухфакторную аутентификацию автоматически, во многих других онлайн-сервисах она все еще необязательна. Рекомендуется во всех сервисах (в соцсетях, мессенджерах, «Госуслугах», электронной почте и т.д.) зайти в настройки и при наличии такой возможности включить двухфакторную аутентификацию.

Обычно пользователь может выбрать, как получать одноразовые коды проверки: через электронную почту, SMS или генерировать их в специальном приложении-аутентификаторе на смартфоне. Из этих способов наиболее безопасным является последний вариант.

Дважды проверяйте ссылки и вложения

Не переходите по ссылкам и не открывайте файлы, присланные в мессенджере и по электронной почте, если не знаете, от кого они, и не ждете никаких посланий. Если же пишут друзья, коллеги или знакомые, но их просьба выглядит хоть немного странно, то перезвоните или напишите этому человеку по другому каналу связи, чтобы убедиться, что он действительно вам что-то отправлял: его могли взломать.

Будьте бдительными и используйте комплексное защитное приложение. Оно предотвратит переход на фишинговые сайты, выманивающие пароли и деньги, а также остановит запуск вредоносных программ.

Переходите в электронную почту, банки, прочие сервисы и приложения только из закладок в браузере или вводя адрес вручную, а не открывая ссылки из сообщений, почты или уведомлений – они могут быть поддельными (фишинговыми).

Включите автообновления

Это нужно, чтобы преступники не могли заразить вас, пользуясь ошибками в операционной системе, браузерах, офисных приложениях и других программах. Все они умеют обновляться самостоятельно. Необходимо не откладывать это действие, когда появляется приглашение перезагрузить программу или компьютер.

Иногда фальшивое обновление предлагают на сайтах. На сайте появляется уведомление, что нужно обновить браузер или видеоплеер. Это обман, чтобы пользователь скачал вредоносное ПО. Настоящее приглашение обновиться показывается прямо в меню программ или служебных оповещениях ОС.

Дважды подумайте, чем делиться онлайн

Отправленные неизвестному пользователю фото или опубликованный в соцсети скан документов могут принести немало проблем в будущем. Вы или ваши близкие могут стать жертвой шантажа, а доступные онлайн данные позволяют мошенникам создать убедительную легенду, чтобы выманить деньги у жертвы. Следует помнить, что всё, что опубликовано в сети, бывает весьма нелегко убрать.

В социальных сетях и мессенджерах есть настройки конфиденциальности, ограничивающие видимость различного вида информации пользователей. Просмотрите настройки социальных сетей и уберите побольше пунктов «Видны всем», заменив их на «Только друзьям».

Не поддавайтесь воздействиям социальной инженерии

Не переходите по ссылкам из сообщений и не звоните по предложенным в них номерам (даже если сообщение пришло якобы с официального номера рассылки сервиса). Лучше заходите в официальное приложение и уже через него связывайтесь со службой поддержки.

Следует помнить, что сотрудники службы поддержки обычно нарасхват и не будут общаться с пользователем дольше 10-15 минут. Долгие переговоры – повод включить подозрительность. Помимо этого, сотрудники служб и сервисов редко контактируют друг с другом. Сотрудник «Госуслуг» вряд ли подключит к разговору коллегу из банка, а коллега из банка кого-либо из Федеральной службы безопасности и т.д.

Помните о презумпции невиновности и о том, что уголовные дела не заводятся по телефону. Если вам угрожают, смело кладите трубку и прекращайте общение.

Если подозрительное письмо или сообщение пришло от имени вашего знакомого, перезвоните ему лично и уточните, действительно ли ему нужна помощь. Обращайте внимание на историю активностей в личных аккаунтах. Если видите частые запросы или уведомления, срочно займитесь сменой пароля.

kaspersky

Вопросы к параграфу:

1. Как надежность пароля отвечает требованиям защиты личного информационного пространства?
2. Достаточно ли защищены личные аккаунты, если вход может быть осуществлен только по паролю?
3. Какие способы двухфакторной аутентификации можно использовать?
4. В каком случае не следует обновлять какое-либо установленное приложение на смартфоне?
5. Какие приложения по защите от спам-звонков вам известны?
6. В чем преимущество пользоваться менеджером паролей?

Ситуация:

Вы зашли на свою личную страницу в социальных сетях и видите, что с нее была рассылка личными сообщениями о просьбе проголосовать в каком-либо конкурсе. Какими будут ваши действия?

§20. Интеллектуальная собственность

Ключевые слова: авторское право, патентное право, лицензионное соглашение

Интеллектуальная собственность – закреплённое законом временное исключительное право, а также личные неимущественные права авторов на результат интеллектуальной деятельности.

Законодательство, которое определяет права на интеллектуальную собственность, устанавливает монополию авторов на определённые формы использования результатов своей интеллектуальной, творческой деятельности, которые, таким образом, могут использоваться другими лицами лишь с разрешения авторов.

Одним из видов интеллектуальной собственности является **авторское право**. Авторским правом регулируются отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства. Авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты. По законам большинства стран компьютерные программы и данные охраняются авторским правом. Это означает, что автор может ограничить распространение и использование программы.

Также к видам интеллектуальной собственности относится **патентное право** – система правовых норм, которыми определяется порядок охраны изобретений, полезных моделей, промышленных образцов.

Интеллектуальная собственность в Росси охраняется законом. Эти права детально определены в Гражданском кодексе РФ. Нарушение авторского права попадает под действие Уголовного кодекса РФ.

Авторские права распространяются на ПО и базы данных, но не касаются алгоритмов и языков программирования, идей и принципов, лежащих в основе программ, баз данных, интерфейса и официальных документов.

kaspersky

Право на использование ПО дает **лицензионное соглашение** – это соглашение между правообладателем и пользователем, где чётко прописаны права и обязанности сторон. По типу лицензии ПО делится на коммерческое, условно-бесплатное, бесплатное и свободное.

Вопросы к параграфу:

1. Что такое интеллектуальная собственность?
2. Какие виды интеллектуальной собственности Вам известны?
3. Какие нормативные документы регламентируют работу с интеллектуальной собственностью?
4. Какие существуют типы лицензий у ПО? По каждому пункту приведите примеры программ.

Ситуация:

Вы разработали несколько библиотек на языке программирования Python и загрузили их на сайт GitHub. Будет ли является нарушением авторского права, если кто-то из пользователей сайта скачает одну из библиотек для личного пользования с дальнейшей модификацией кода?

kaspersky

Глава 2. Основы криптологии

§21. Криптология

Ключевые слова: криптология, криптография, криптоанализ, текст, алфавит, шифрование

Долгое время наука криптография была засекречена, т.к. применялась, в основном, для защиты государственных и военных секретов. **Криптология** – наука, занимающаяся методами шифрования и дешифровки. И состоит из двух частей – криптографии и криптоанализа.

Криптография занимается разработкой методов шифрования данных, в то время как криптоанализ занимается оценкой сильных и слабых сторон методов шифрования, а также разработкой методов, позволяющих взламывать криптосистемы.

В настоящее время, методы и средства криптографии используются для обеспечения информационной безопасности не только государства, но и частных лиц и организаций. На сегодняшний момент очень большой обмен информацией происходит в цифровом виде через открытые каналы связи. К этой информации возможно применение угроз недружественного ознакомления, накопления, подмены, фальсификации и т.д. Наиболее надежные методы защиты от таких угроз дает именно криптография, которая базируется на математических методах. В силу присущей методам криптографии специфики, большой интерес представляет множество целых чисел и различные алгебраические структуры на его базе.

Математическая криптография возникла как наука о шифровании информации, т.е. как наука о криптосистемах. Большое влияние на развитие криптографии оказали появившиеся в середине двадцатого века работы американского математика Клода Шеннона.

При обмене информацией между участниками часто возникает ситуация, когда информация не является конфиденциальной, но важен факт поступления сообщений в неискаженном виде, т.е. наличие гарантии, что никто не сумеет подделать сообщение. Такая гарантия называется обеспечением целостности информации.

Для предотвращения угрозы контроля за источниками информации (откуда пересылаются сообщения) необходима система контроля за доступом к ресурсам, которая должна удовлетворять двум, казалось бы, взаимно исключающим требованиям. Во-первых, всякий желающий должен иметь возможность обратиться к этой системе анонимно, а во-вторых, при этом все же доказать свое право на доступ к ресурсам. Обеспечение неотслеживаемости – одна из задач криптографии.

Если задача обеспечения конфиденциальности решается с помощью криптосистем, то для обеспечения целостности и неотслеживаемости разрабатываются криптографические протоколы.

Современная криптография включает в себя четыре основных направления:

- Симметричные криптосистемы.
- Криптосистемы с открытым ключом.
- Системы электронной подписи.
- Управление ключами.

Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

kaspersky

В качестве информации, подлежащей шифрованию и дешифрованию, рассматриваются тексты (упорядоченный набор), построенные на некотором **алфавите** – конечном множестве используемых для кодирования информации знаков.

Вопросы к параграфу:

1. Что такое криптология?
2. Чем криптология отличается от криптографии?
3. Какие задачи стоят перед криптографией?
4. Какие направления современной криптографии Вам известны?

§22. Математические основы криптологии

Ключевые слова: множество, отображение множества, функция, простое число, основная теорема арифметики, псевдопростые числа, вероятность, частотность, комбинаторика, арифметика остатков, сравнения по модулю, функция Эйлера, высказывания, логические операции

На сегодняшний момент криптология как наука выстраивает свою структуру на основе математического аппарата. Существующие шифры уже имеют некие математические модели, которые позволяют реализовать рассматриваемые алгоритмы компьютерным кодом. Рассмотрим некоторые темы из математики, на которых базируются многие шифры, в том числе и криптоанализ.

Теория множеств

Математическое понятие множество является одним из центральных во всей математике. Оно определяется в зависимости от задач.

Множество – любая совокупность объектов, называемых элементами множества. Множества с конечным числом различных элементов могут быть описаны путем явного перечисления всех элементов. Обычно эти элементы заключаются в фигурные скобки. Например, {16,32,64} – множество степеней двойки, заключенных между 10 и 100.

Для некоторых особо важных множеств приняты стандартные обозначения, которых следует придерживаться. Так, буквами N, Z, Q, R обозначают соответственно множество натуральных чисел, множество целых чисел, множество рациональных чисел и множество действительных чисел.

Два множества равны тогда и только тогда, когда они содержат в точности одинаковые элементы.

Пустое множество – это множество, не содержащее ни одного элемента. Обозначается пустое множество: ∅.

Отображение множества – это правило, по которому каждому элементу одного множества ставится в соответствие элемент (или элементы) другого множества.

Примером отображения множества в школьном курсе математики является понятие **функция**, так как ее можно определить как отображение одного множества (области определения) в другое множество (область значений), которое каждому элементу из первого множества сопоставляет и при том единственный элемент из второго множества.

Взаимно однозначное соответствие – это отображение множества, при котором каждому элементу одного множества соответствует ровно один элемент другого множества, при этом определено обратное отображение, которое обладает тем же свойством.

kaspersky

Арифметика

Натуральное число p > 1 называется **простым**, если оно имеет ровно два положительных делителя (1 и p). В противном случае число p > 1 называется **составным**. Единица является ни простым, ни составным числом.

Наименьший отличный от единицы делитель составного числа n не превосходит $\sqrt{n}$. Таким образом, если натуральное число n > 1 не делится ни на одно простое число, не превосходящее $\sqrt{n}$, то оно простое.

Теорема Евклида: Простых чисел бесконечно много.

Основная теорема арифметики: Каждое натуральное число a > 1 представимо в виде произведения простых чисел, причем данное разложение единственно (с точностью до порядка следования сомножителей).

Вопрос определения того, является ли натуральное число простым, известен как **проблема простоты**. Тестом простоты (или проверкой простоты) называется алгоритм, который, приняв на входе натуральное число, позволяет либо не подтвердить предположение о том, является ли это число составным, либо точно утверждать его простоту. То есть, тест простоты представляет собой только гипотезу о том, что если алгоритм не подтвердил предположение о том, что число составное, то это число может являться простым с определённой вероятностью.

Существующие алгоритмы проверки числа на простоту могут быть разделены на две категории: истинные тесты простоты и вероятностные тесты простоты. Истинные тесты результатом вычислений всегда выдают факт простоты числа, вероятностный тест даёт ответ о простоте числа с некоторой вероятностью. Если сказать проще, то вероятностный алгоритм говорит, что число скорее всего не является составным, однако в итоге оно может оказаться как простым, так и составным. Числа, удовлетворяющие вероятностному тесту простоты, но являющиеся составными, называются **псевдопростыми**.

Наибольшее известное простое число (2018г.) содержит 24 862 048 цифр – это число $2^{82589933}- 1$.

Теория вероятности

Вероятность – это степень возможности наступления некоторого события, которая определяется как отношение числа благоприятных событий к числу всевозможных событий. Вероятность события может варьироваться от 0 до 1, где 0 – событие точно не произойдет, 1 – событие точно произойдет.

Необходимость понятия вероятности и исследований в этом направлении была исторически связана с азартными играми. До появления понятия вероятности формулировались в основном как комбинаторные задачи подсчёта числа возможных исходов при бросании нескольких костей, а также задача раздела ставки между игроками, когда игра закончена досрочно.

К примеру, все возможные комбинации перестановок n-элементов между собой без повторений можно рассчитать при помощи n! (факториал числа n):

$$n! = 1 \cdot 2 \cdot \ldots \cdot (n - 1) \cdot n.$$

Данная формула интуитивно выводится при рассмотрении конкретных задач. На первую позицию будут претендовать n элементов, на вторую – n-1 элементов и т.д., на предпоследнюю позицию останется 2 элемента и на последнюю – 1. Согласно комбинаторному принципу умножения, данные варианты умножаются и получается, что n! – это произведение всех натуральных чисел, которые не превосходят n, и будет являться числом возможных перестановок без повторения.

Первые работы о вероятности относятся к XVII веку. Это работы Б. Паскаля, П. Ферма, Х. Гюйгенса.

Частотность – отношение числа случаев, в которых встретился данный результат, к общему числу случаев.

Эмпирическое «определение» вероятности связано с частотой наступления события исходя из того, что при достаточно большом числе испытаний частота должна стремиться к объективной степени возможности этого события.

kaspersky

Теоремы:

- Вероятность суммы двух несовместных событий равна сумме вероятностей этих событий.
- Вероятность произведения двух независимых событий равна произведению их вероятностей.

Модульная арифметика (арифметика остатков)

Для любых целых a и b, $b \neq 0$, существуют, и притом единственные, целые q и r, такие что $a = b \cdot q + r$, $0 \leq r \leq |b|$. В этом случае r – остаток от деления a на b.

Пусть m – некоторое натуральное число. Целые числа a и b называются **сравнимыми по модулю m**, если разность a - b делится на m и обозначают $a \equiv b \pmod{m}$. Данное соотношение читается «a сравнимо с b по модулю m». Таким образом, можно дать и такое определение: целые числа a и b называются **сравнимыми по модулю m**, если остатки от деления этих чисел на m равны.

Следующие условия эквивалентны:

- a сравнимо с b по модулю m.
- a и b имеют одинаковые остатки при делении на m.
- имеет место представление $a = m \cdot t + b$, где t – некоторое целое число.

К примеру:

- $5 \equiv 1 \pmod{2}$, так как 5 - 1 делится на 2.
- $14 \equiv 2 \pmod{12}$, так как 14 - 2 делится на 12.
- $10 \equiv -1 \pmod{11}$, так как 10 - (-1) делится на 11.

Пусть $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$. Рассмотрим некоторые **свойства сравнений по модулю**:

- $a \pm c \equiv b \pm d \pmod{m}$.
- $a \cdot c \equiv b \cdot d \pmod{m}$.
- $a^n \equiv b^n \pmod{m}$.

Рассмотрим пример применения данных свойств: докажите, что $6^{22} - 1$ делится на 7. Доказательство представим в таблице.

1 шаг	Переформулируем задачу под условия модульной арифметики	Докажите, что $6^{22} \equiv 1 \pmod{7}$
2 шаг	Так как в задании фигурирует степень, то удобнее всего подобрать такое сравнение по модулю 7, чтобы проще считался результат возведения в степень	$6 \equiv -1 \pmod{7}$
3 шаг	Возведем обе части сравнения по модулю 7 в степень 22 (согласно третьему свойству)	$6^{22} \equiv (-1)^{22} \pmod{7}$ $6^{22} \equiv 1 \pmod{7}$
4 шаг	Распишем определение сравнения двух чисел по заданному модулю	$6^{22} - 1$ делится на 7

kaspersky

Рассмотрим еще один пример: найдите остаток от деления 2^{29} на 11. Решение представим в таблице.

1 шаг	Так как в задании фигурирует степень, то удобнее всего подобрать такое сравнение по модулю 11, чтобы проще считался результат возведения в степень	$2^5 \equiv -1 \pmod{11}$
2 шаг	Возведем обе части сравнения по модулю 11 в степень 5 (согласно третьему свойству)	$(2^5)^5 \equiv (-1)^5 \pmod{11}$ $2^{25} \equiv -1 \pmod{11}$
3 шаг	Так как 29 представляется как сумма 25 и 4, то подберем сравнение со степенью 4	$2^4 \equiv 5 \pmod{11}$
4 шаг	Перемножим сравнения по модулю 11 из шагов 2 и 3	$2^{29} \equiv -5 \pmod{11}$
5 шаг	Получили -5, но остаток не может быть отрицательным, то составим сравнение по модулю 11	$-5 \equiv 6 \pmod{11}$

Ответ: Остаток от деления 2^{29} на 11 равен 6.

Функция Эйлера φ(a) – функция, определенная на множестве всех натуральных чисел, значение которой от аргумента a представляет собою количество натуральных чисел меньших a и взаимно простых с ним.

К примеру:

- φ(1) = 1.
- φ(3) = 2, так как меньше числа 3, и взаимно просты с ним только числа 1 и 2.
- φ(11) = 10, так как все числа от 1 до 10 взаимно просты с числом 11.
- φ(12) = 4, так как меньше числа 12, и взаимно просты с ним только числа 1, 5, 7, 11.

Как следует из определения, чтобы вычислить φ(n), необходимо перебрать все числа от 1 до n−1, и для каждого проверить, имеет ли оно общие делители с числом n, а затем подсчитать, сколько чисел оказались взаимно простыми с n. Эта процедура для больших чисел n весьма трудоёмка, поэтому для вычисления φ(n) используют другие методы, которые основываются на специфических свойствах функции Эйлера:

- Одним из основных свойств функции Эйлера является её мультипликативность. Это свойство было установлено ещё Эйлером: если числа m и n взаимно простые, то $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.
- Для простого числа p значение $\varphi(p) = p - 1$.
- Для вычисления функции Эйлера от степени простого числа справедливо: $\varphi(p^n) = p^n - p^{n-1}$.

Теорема Эйлера: Для любого натурального m и любого целого a, взаимно простого с m, справедливо $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Теорема Ферма: Для любого простого p и любого целого a, не делящегося на p, справедливо $a^{p-1} \equiv 1 \pmod{p}$.

Алгебра логики

Базовыми элементами, которыми оперирует алгебра логики, являются **высказывания** – это повествовательные предложения, в отношении которых можно однозначно сказать, истинно оно или ложно.

Над высказываниями производятся логические операции, такие как отрицание, конъюнкция, дизъюнкция и т.д. Как правило, в математических выражениях Ложь отождествляется с логическим нулём, а Истина – с логической единицей, а операции отрицания (НЕ), конъюнкции (И) и дизъюнкции (ИЛИ) определяются в привычном понимании. К дополнительным операциям относятся импликация и эквиваленция.

kaspersky

Вопросы к параграфу:

1. Что такое множество?
2. Что такое отображение множества?
3. Может ли функция быть взаимно однозначным соответствием?
4. Какое число называется простым?
5. Существуют ли натуральные числа, которые являются ни простыми, ни составными?
6. Какие числа называются псевдопростыми?
7. Что такое вероятность события?
8. Как можно вычислить количество n-элементов перестановок без повторений?
9. Что такое частотность?
10. Какие числа можно назвать сравнимыми по определенному модулю?
11. Что такое функция Эйлера?
12. Чему равна функция Эйлера от простого числа?
13. Какие логические операции выполняются над высказываниями?

Ситуация:

В общественном транспорте в былые времена висела табличка с информацией: «За бесплатный проезд и провоз багажа штраф 1000 рублей». Пассажир оплатил только свой проезд, а на крупногабаритный багаж не стал производить оплату. Нарушил ли пассажир требование общественного транспорта? В чем логическая ошибка данного предписания?

Задание:

1. Составьте возможную формулу функции y = f(x), если f(1) = 3, f(2) = 9, f(3) = 27.
2. Является ли функцией линия, заданная уравнением:
   $x^2 + y^2 = 81$?
3. На клавиатуре телефона 10 цифр, от 0 до 9. Какова вероятность того, что случайно нажатая цифра окажется четной?
4. Рассматриваются символьные последовательности длины 5 в шестибуквенном алфавите {У, Ч, Е, Н, И, К}. Сколько существует таких последовательностей, которые начинаются с буквы У и заканчиваются буквой К?
5. Для создания пароля из пяти символов пользователь использовал цифры 0, 3, 4, 8 и 9. Какова вероятность подобрать установленный пароль?
6. Вероятность того, что загруженный файл на компьютер с неофициального источника заражен вирусом, равна 0,8. Пользователь загружает два таких файла. Найдите вероятность того, что оба файла окажутся незараженными.
7. Найдите возможное значение неизвестной:
   $x \equiv 1 \pmod 6$
   $x \equiv 3 \pmod 7$
   $x \equiv -4 \pmod 9$
   $29 \equiv x \pmod{13}$
   $(x + 2) \equiv 5 \pmod{13}$
   $x^2 \equiv 3 \pmod{11}$
8. Найдите остаток от деления числа 3^{25} на 10.
9. Разложите на простые множители числа 270, 385, 1210.
10. Вычислите квадратный корень из числа 27225, предварительно разложив его на простые множители.

11. Вычислите функцию Эйлера от чисел 25, 31, 81.
12. Выберите из предложений те, которые являются высказываниями:
    - Москва – столица России
    - В феврале 30 дней
    - Сегодня хороший день
    - Это предложение ложно
13. Упростите логическое выражение:
    $\neg(A \vee B) \& A \& \neg B$.
14. Найдите наибольшее целое число X, для которого истинно высказывание:
    ¬(X – чётное) & ¬(X ≥ 11).

§23. Шифрование данных

Ключевые слова: шифрование, шифр, шифр-текст, симметричное шифрование, асимметричное шифрование, скиталы, диск Энея, квадрат Полибия

Вопрос о целостности и сохранности передаваемой информации был актуален во все времена. Поэтому в истории человечества неоднократно встречались способы сокрытия информации от недоброжелателей или сокрытие самого факта передачи той или иной информации.

Шифрование – обратимое преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней.

Если говорить простыми словами, то термин «шифрование» описывает процесс «перемешивания» данных таким образом, что неавторизованным лицам, не обладающим ключом для дешифровки, невозможно их понять.

Если опираться на математический аппарат, то шифрование можно определить как некое отображение множества открытых текстов во множество шифр-текстов.

Главным образом, шифрование служит для соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма. Что влечет обеспечение трёх состояний безопасности информации: конфиденциальность, целостность, идентифицируемость.

К методам шифрования относятся:

- **Симметричное шифрование.** В симметричных криптосистемах для шифрования и расшифровывания используется один и тот же ключ. Алгоритм и ключ выбираются заранее и известны обеим сторонам. Сохранение ключа в секретности является важной задачей для установления и поддержки защищённого канала связи. В связи с этим, возникает проблема начальной передачи ключа. Кроме того, существуют методы, позволяющие дешифровать информацию, не имея ключа или же с помощью его перехвата на этапе согласования. Недостатками симметричного шифрования является проблема передачи ключа собеседнику и невозможность установить подлинность или авторство текста.

- **Асимметричное шифрование.** В системах с открытым ключом используются два ключа – открытый и закрытый, связанные определённым математическим образом друг с другом. Открытый ключ передаётся по открытому каналу и используется для шифрования информации. Для расшифровки сообщения используется секретный ключ. В асимметричных системах другой стороне передается открытый ключ, который позволяет шифровать, но не расшифровывать информацию. Таким образом решается проблема симметричных систем, связанная с синхронизацией ключей.

Первыми исследователями, которые изобрели и раскрыли понятие шифрования с открытым кодом, были Уитфилд Диффи, Мартин Хеллман и Ральф Меркле.

Потребность шифровать и передавать шифрованные сообщения возникла очень давно. Так, еще в V-IV вв. до н.э. греки применяли специальное шифрующее устройство. По описанию Плутарха, оно состояло из двух палок одинаковой длины и толщины. Одну оставляли себе, а другую отдавали отъезжающему. Эти палки называли скиталами. Когда правителям нужно было сообщить какую-нибудь важную тайну, они вырезали длинную и узкую, вроде ремня, полосу папируса, наматывали ее на свою скиталу, не оставляя на ней никакого промежутка, так чтобы вся поверхность палки была охвачена этой полосой. Затем, оставляя папирус на скитале в том виде, как он есть, писали на нем все, что нужно, а написав, снимали полосу и без палки отправляли адресату. Так как буквы на ней разбросаны в беспорядке, то прочитать написанное можно только при помощи соответствующей скиталы, намотав на нее без пропусков полосу папируса.

Древнегреческий полководец Эней Тактика в IV веке до н.э. предложил устройство, названное впоследствии «диском Энея». Принцип его таков. На диске диаметром 10-15 см и толщиной 1-2 см высверливались отверстия по числу букв алфавита. В центре диска помещалась «катушка» с намотанной на ней ниткой достаточной длины. При зашифровании нитка «вытягивалась» с катушки и последовательно протягивалась через отверстия, в соответствии с буквами шифруемого текста. Диск и являлся посланием. Получатель послания последовательно вытягивал нитку из отверстий, что позволяло ему получать передаваемое сообщение, но в обратном порядке следования букв. При перехвате диска недоброжелатель имел возможность прочитать сообщение тем же образом, что и получатель. Но Эней предусмотрел возможность легкого уничтожения передаваемого сообщения при угрозе захвата диска. Для этого было достаточно выдернуть «катушку» с закрепленным на ней концом нити до полного выхода всей нити из всех отверстий диска.

Заметным вкладом Энея в криптографию является предложенный им так называемый книжный шифр, описанный в сочинении «Об обороне укрепленных мест». Эней предложил прокалывать малозаметные дырки в книге или в другом документе над буквами (или под ними) секретного сообщения.

В Древней Греции (II в. до н.э.) был также известен шифр, называемый квадрат Полибия. Это устройство представляло собой квадрат 5x5, столбцы и строки которого нумеровали цифрами от 1 до 5. В каждую клетку этого квадрата записывалась одна буква. (В греческом варианте одна клетка оставалась пустой, в латинском – в одну клетку помещали две буквы i и j.) В результате каждой букве отвечала пара чисел и шифрованное сообщение превращалось в последовательность пар чисел.

На сегодняшний момент многие алгоритмы шифрования стали историческими, так как известны не только их алгоритмы, но и сформированы компьютерные модели, которые позволяют расшифровать шифр-тексты за доли секунд. Современные алгоритмы шифрования основываются на математической базе, в частности на теории чисел, так как многие задачи такой тематики являются трудоемкими (по времени) для современных компьютеров, и порой найденный вариант решения (к примеру, большие простые числа) не всегда является верным.

При шифровании очень важно правильно содержать и распространять ключи между пользователями, так как это является наиболее уязвимым местом любой криптосистемы. При использовании «идеальной» шифрующей системы всегда существует возможность найти дефект не в ней, а в тех, кто её использует. Можно выкрасть ключи у доверенного лица или подкупить его, и зачастую это оказывается гораздо дешевле, чем взламывание шифра. Поэтому процесс, содержанием которого является составление и распределение ключей между пользователями, играет важнейшую роль в криптографии как основа для обеспечения конфиденциальности обмена информацией.

kaspersky

Вопросы к параграфу:

1. Что такое шифрование?
2. Для чего необходим процесс шифрования информации?
3. В чем различие между симметричным и асимметричным методами шифрования?

Задание:

Перед Вами квадрат Полибия с латинским алфавитом.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

1. Расшифруйте: 32 51 13 13 43 25 43 24 13 41
2. Зашифруйте название сериала «Game of Thrones».

Пояснение: координаты каждой буквы представлены парой (столбец; строка).

§24. Шифры простой замены

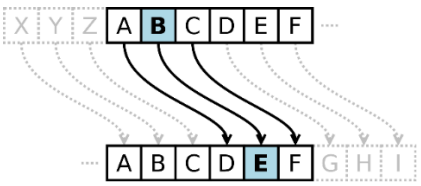
Ключевые слова: шифр, шифр-текст, шифр Цезаря, ROT13, частотный анализ

Шифры простой замены – это класс методов шифрования, которые образуют взаимно однозначное отображение символов открытого текста и символов шифр-текста (для каждого символа открытого текста по определенному правилу сопоставляется единственный символ шифр-текста и наоборот).

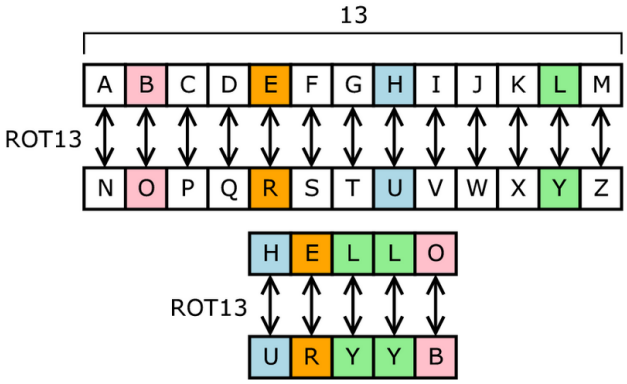
До появления компьютеров криптография состояла из алгоритмов на символьной основе. Различные криптографические алгоритмы либо заменяли одни символами другими, либо переставляли символы. Лучшие алгоритмы делали и то, и другое. На сегодняшний момент все шифры намного сложнее. При этом они работают с битами, а не с символами.

Примерами шифров простой замены могут являться:

- **Шифр Цезаря** – шифр, в котором каждый символ открытого текста заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него.



- **ROT13** – шифр для латинского алфавита, в котором каждая буква смещается на 13 позиций. Данный шифр не используется для безопасности, а часто применяется в почте, закрывая потенциально неприятный текст, решения головоломки на форумах и т.д.
  Рассмотрим пример, как слово «HELLO» после шифрования станет «URYYB».



Более сильные шифры простой замены могут преобразовывать букву открытого текста в различные символы. Следует заметить, что шифры такого вида легко взламываются, так как они не прячут частоты использования различных символом в открытом тексте. Частые слова и пары букв все равно составят едва заметные закономерности в шифр-тексте. Можно придумать больше символов для замены пар букв и общих слов, что еще больше затруднит частотный анализ, но противостоять ему не получится.

Вопросы к параграфу:

1. Что такое шифр простой замены?
2. В чем плюсы и минусы шифров простой замены?
3. Может ли символу начального текста соответствовать смайлик в шифрах простой замены?
4. Сколько существует возможных перестановок букв латинского алфавита?

Задание:

1. Зашифруйте текст «The World Is Not Enough» шифрованием ROT13.
2. Расшифруйте название мультипликационного фильма «Svaqvat Arzb», который был зашифрован методом ROT13.

§25. Шифр Цезаря

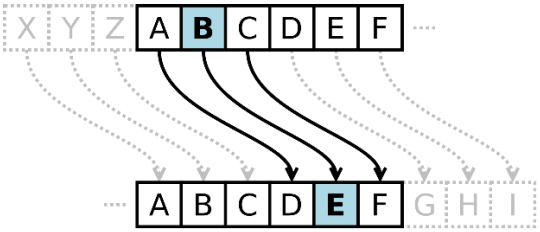
Ключевые слова: Цезарь, шифр Цезаря, шифр простой замены

Шифр Цезаря – один из самых известных и самых древних шифров. В этом шифре каждая буква заменяется на другую, расположенную в алфавите на заданное число позиций k вправо от нее. Алфавит замыкается в кольцо, так что последние символы заменяются на первые.

kaspersky

Шифр Цезаря относится к шифрам простой замены, так как каждый символ исходного сообщения заменяется на другой символ из того же алфавита.

На рисунке показан пример шифра Цезаря со сдвигом 3 (шаг равен 3).



Шифр Цезаря назван в честь Юлия Цезаря, который, согласно «Жизни двенадцати цезарей» Светония, использовал его со сдвигом 3, чтобы защищать военные сообщения. Хотя Цезарь был первым зафиксированным человеком, использовавшим эту схему, другие шифры простой замены использовались и ранее. Если у него было что-либо конфиденциальное для передачи, то он записывал это шифром, то есть так изменял порядок букв алфавита, что нельзя было разобрать ни одно слово.

Неизвестно, насколько эффективным шифр Цезаря был в то время, но, вероятно, он был разумно безопасен, не в последнюю очередь благодаря тому, что большинство врагов Цезаря было неграмотным, и многие предполагали, что сообщения были написаны на неизвестном иностранном языке.

Часто для удобства использования шифра Цезаря брали два диска разного диаметра, насаженных на общую ось, с нарисованными по краям дисков алфавитами. Например, если внутреннее колесо повернуть так, чтобы символу «A» внешнего диска соответствовал символ «D» внутреннего диска, то получим шифр со сдвигом 3 влево.

Если пронумеровать буквы алфавита начиная с нуля, то алгоритм шифрования может быть выражен математической формулой:

$$y = (x + k) \bmod n,$$

где x – код исходного символа, k – величина сдвига (ключ), y – код символа-замены, n – количество символов в алфавите.

Ключом для шифра Цезаря служит сдвиг k, если его знать, то сообщение легко расшифровать. Для этого используется формула:

$$x = (y - k) \bmod n.$$

Вопросы к параграфу:

1. В чем заключается концепция шифра Цезаря?
2. Почему шифр Цезаря имеет такое название?
3. Насколько надежно использовать шифр Цезаря на сегодняшний момент?

Задание:

1. Зашифруйте текст «Это предложение ложно» шифром Цезаря со сдвигом 5.
2. Расшифруйте название мультипликационного фильма «Фшъщшъйати цшчыьъшл», если использовался шифр Цезаря. Чему равен ключ шифрования?
3. После использования шифра Цезаря фраза «Невозможное возможно» стала «Сиётлртксти ётлрткст». Чему равен ключ шифрования?

kaspersky

§26. Частотный анализ

Ключевые слова: частота, частотный анализ, шифр простой замены

Частотный анализ – один из методов криптоанализа, основывающийся на предположении о существовании статистического распределения отдельных символов и их последовательностей, как в открытом тексте, так и в шифр-тексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.

То есть, частотный анализ предполагает, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом, в случае шифров простой замены, если в шифр-тексте будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой.

Частотный анализ основывается на факте, что вероятность появления отдельных букв, а также их порядок в словах и фразах естественного языка подчиняются статистическим закономерностям. Анализируя достаточно длинный текст, зашифрованный методом простой замены, можно по частоте появления символов произвести обратную замену и восстановить исходный текст.

Например, в типичных английских текстах буква «E» встречается наиболее часто. Если наиболее частой буквой в шифр-тексте является «R», то есть большая вероятность, что в подстановке «E» была заменена на «R».

В общем случае частотность букв в процентном выражении можно определить следующим образом: подсчитывается, сколько раз она встречается в шифр-тексте, затем полученное число делится на общее число символов шифр-текста (для выражения в процентах полученный результат умножается на 100).

Следует сказать, что частотность существенно зависит не только от длины текста, но и от его характера. Например, в техническом тексте обычно редкая буква «Ф» может появляться гораздо чаще. Поэтому для надёжного определения средней частоты появления букв желательно иметь набор различных текстов.

Метод частотного анализа известен с IX века. Начиная с середины XX века большинство используемых алгоритмов шифрования разрабатывались устойчивыми к частотному криптоанализу, поэтому на сегодняшний момент он применяется в основном в процессе обучения будущих криптографов.

kaspersky

Вопросы к параграфу:

1. Что такое частотный анализ?
2. Для каких шифров подходит использование частотного анализа?
3. Где на сегодняшний момент используют частотный анализ?
4. Любой ли длины шифр-текст подходит для применения частотного анализа?
5. Всегда ли частота появления конкретной буквы алфавита одинакова в различных текстах?

§27. Шифр Вернама (XOR)

Ключевые слова: шифр Вернама, исключающее «или», XOR, гамма, гаммирование, одноразовый блокнот, распределение ключей

Шифр Вернама – система симметричного шифрования, изобретённая в 1917 году Гилбертом Вернамом.

В алгебре логики изучаются различные операции с выражениями – отрицание, конъюнкция, дизъюнкция и т.д. Вернам запатентовал свою систему шифрования, не пользуясь аппаратом данного раздела математики, но подразумевая операцию **исключающее «или» (XOR)** – логическая операция над двумя переменными, которая истинна тогда и только тогда, когда выражения, входящие в нее, имеют разные логические значения.

Рассмотрим таблицу истинности для операции XOR:

A	B	A XOR B
0	0	0
1	0	1
0	1	1
1	1	0

Легко убедиться, что (A XOR B) XOR B = A. То есть, если A – это изначальный текст, B – ключ для шифрования, то использование исключающего «или» сначала для шифрования, а потом для расшифровки, дает изначальный текст. Простыми словами, выполняется концепция симметричного шифрования.

Для каждого сообщения Вернам брал такую же по длине последовательность нулей и единиц – гамму, каждый ее бит подвергался исключающему «или» с соответствующим битом сообщения и отправлялся адресату.

kaspersky

Рассмотрим пример шифрования способом Вернама:

текст	1	0	1	1	0	1	1	0	0
гамма	0	1	1	1	0	0	1	0	1
шифр-текст	1	1	0	0	0	1	0	0	1

Теперь произведем расшифровку, используя ту же гамму (ключ):

шифр-текст	1	1	0	0	0	1	0	0	1
гамма	0	1	1	1	0	0	1	0	1
текст	1	0	1	1	0	1	1	0	0

Гамма – это ключ в шифре Вернама. Но правильно говорить – ключевая последовательность, потому что гамма длинная (равна длине сообщения). К примеру, гамма может быть такой:

0010101110101010101110010111111001110100001010100001l0...

Поэтому шифр Вернама еще называют **шифром гаммирования**. Или **шифром одноразового блокнота**, так как одна гамма, которую Вернам записал себе в блокнот, может применяться к какому-либо сообщению только один раз. После этого Вернам ее вычеркивал из блокнота.

Следует заметить, что гамма должна быть случайной последовательностью нулей и единиц. Поэтому плюс использования XOR в таком методе шифрования – равновероятное появление нуля и единицы в конкретной позиции. Для работы шифра Вернама необходима истинно случайная последовательность гаммы (ключа). Последовательность, полученная с использованием любого алгоритма, по определению является не истинно случайной, а псевдослучайной. Следовательно, случайную последовательность нужно получить не алгоритмически.

Криптосистема, требующая ключа той же длины, что и сообщение, вместе с условием однократного использования каждого ключа, крайне неудобна при интенсивной эксплуатации. Происходит это потому, что передача секретного ключа в рамках одной криптосистемы от одного пользователя к другому становится неразрешимой задачей. Действительно, скрытая передача необходимого ключа требует очередного ключа, тот – следующего, и т.д. Возникающую проблему называют проблемой распределения ключей.

В целях преодоления указанной трудности абсолютно стойкие криптографические алгоритмы заменяются системами. В этом состоят задачи современных криптографов, одна из которых – изобретение системы, удовлетворяющей следующим требованиям:

- Один ключ используется несколько раз.
- Небольшим ключом шифруются длинные сообщения.

В 1945 году Клод Шеннон написал работу «Математическая теория криптографии», в которой доказал абсолютную криптографическую стойкость шифра Вернама. То есть перехват шифр-текста без ключа не даёт никакой информации о сообщении. С точки зрения криптографии, невозможно придумать систему безопаснее шифра Вернама. Требования к реализации подобной схемы достаточно нетривиальны, поскольку необходимо обеспечить наложение уникальной гаммы, равной длине сообщения, с последующим её гарантированным уничтожением. В связи с этим коммерческое применение шифра Вернама не так распространено и используется, в основном, для передачи сообщений особой важности государственными структурами.

kaspersky

Вопросы к параграфу:

1. В чем заключается смысл шифра Вернама?
2. Что такое гамма в шифре Вернама?
3. Какой длины должен быть ключ при применении шифра Вернама?
4. Какой надежностью обладает шифр Вернама?
5. Почему шифр Вернама называют шифром одноразового блокнота?

Задание:

1. Постройте таблицу истинности для выражения: A XOR A.
2. Заполните пустые ячейки таблицы:

текст	0		0		0	0		0	1
гамма	1	1		1	0		1	0	0
шифр-текст		0	1	0		1	1	0	

3. Назовите длину необходимой гаммы, если шифруется текст:
   10101001010010100001010111101
4. Зашифруйте текст 101010001010110101l101, если гамма равна 01001010.

§28. Шифр Виженера

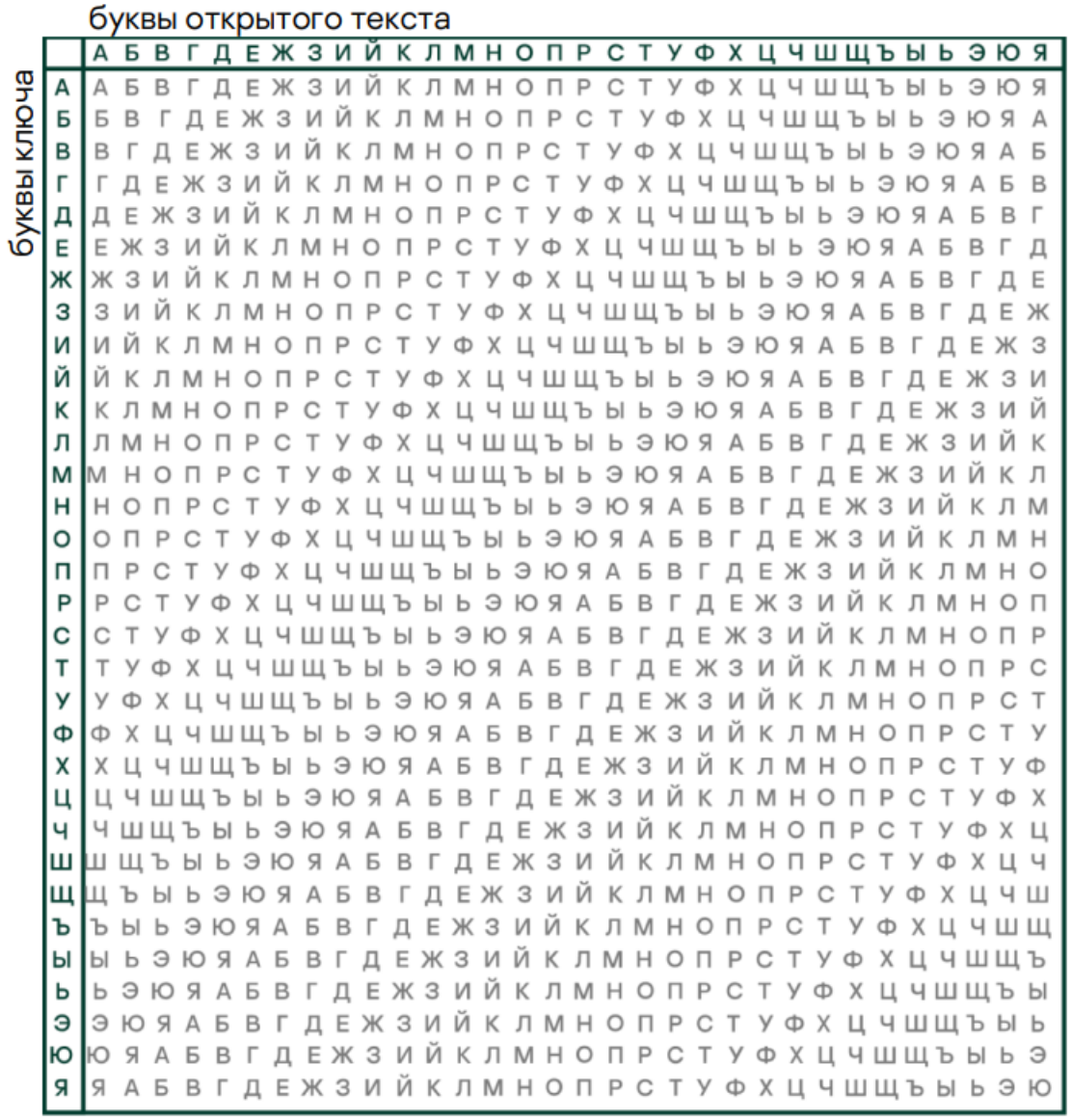
Ключевые слова: шифр Виженера, таблица Виженера, квадрат Виженера, частотный анализ, шифр Цезаря, шифр Гронсфельда

Шифр Виженера – метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая **квадрат (таблица) Виженера.** Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Человек, посылающий сообщение, записывает ключевое слово циклически до тех пор, пока его длина не будет соответствовать длине исходного текста.

Рассмотрим конкретный пример использования шифра Виженера. Для этого сформируем квадрат Виженера для русского алфавита. По горизонтали расположены буквы открытого текста, по вертикали – буквы ключа. Каждая новая строка внутри квадрата – это шифр Цезаря со сдвигом равным 1, 2, 3 и так далее до 32.

kaspersky



Пусть необходимо отправить сообщение «МЫ НА МЕСТЕ», используя секретное слово (ключ) «КОД». Необходимо, чтобы букв ключа хватило на весь текст сообщения, игнорируя пробелы. Поэтому, будем повторять ключ столько раз, сколько потребуется. Далее сопоставляем каждую букву сообщения с буквой ключа.

сообщение	М	Ы	Н	А	М	Е	С	Т	Е
ключ	К	О	Д	К	О	Д	К	О	Д
шифр-текст	Ц	Й	С	К	Ъ	Й	Ы	А	Й

Таким образом, передаваться буде сообщение «ЦЙСКЪЙЫАЙ». Обратите внимание, теперь одинаковым буква М в изначальном сообщении соответствуют разные буквы шифр-текста. Это означает, что статистика распределения частот букв нарушилась. Теперь для каждой буквы открытого текста используется свой ключ и, соответственно, свой алфавит.

kaspersky

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Если n – количество букв в алфавите, mj – номер буквы открытого текста, k_j – номер буквы ключа в алфавите, то шифрование Виженера можно записать следующим образом: $c_j = (m_j+k_j) \bmod n$.

А расшифровывание: $m_j = (c_j - k_j) \bmod n$.

Несмотря на стойкость шифра Виженера, он широко не использовался в Европе. Большее распространение получил **шифр Гронсфельда**, идентичный шифру Виженера, за исключением того, что он использовал только 10 различных алфавитов (соответствующих цифрам от 0 до 9). Преимущество шифра Гронсфельда состоит в том, что в качестве ключа используется не слово, а цифровая последовательность, которая повторяется до тех пор, пока не станет равной длине шифруемого сообщения. Для шифрования используется **таблица Гронсфельда**. Составим ее для латинского алфавита.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Алгоритм шифрования шифром Гронсфельда идентичен шифру Виженера. Пусть необходимо отправить сообщение «HELLO, WORLD», используя ключ «2025». Необходимо, чтобы цифр ключа хватило на весь текст сообщения, игнорируя пробелы и знаки препинания. Поэтому, будем повторять ключ столько раз, сколько потребуется. Далее сопоставляем каждую букву сообщения с цифрой ключа.

сообщение	H	E	L	L	O	W	O	R	L	D
ключ	2	0	2	5	2	0	2	5	2	0
шифр-текст	J	E	N	Q	Q	W	Q	W	N	D

Таким образом, передаваться буде сообщение «JENQQWQWN».

При использовании более длинных ключей каждая буква открытого текста будет иметь еще больше возможных замен. В результате шифр Виженера способен уменьшить угрозу частотного анализа. Этот шифр был изобретен в XVI веке и оставался нетронутым более 300 лет. Многие верили, что он несокрушим, пока первым шифр Виженера не взломал в 1845 году Чарльз Бэббидж. Но опубликовал схему анализа уже другой исследователь – Фридрих Касиски девятью годами позже.

Сегодня шифр Виженера может быть легко взломан любым компьютером. Наблюдая повторяющиеся последовательности букв в шифр-тексте, можно угадать длину ключа шифрования.

kaspersky

Вопросы к параграфу:

1. Что такое шифр Виженера?
2. На каком шифре базируется идея применения шифра Виженера?
3. В чем отличие шифров Виженера и Гронсфельда?
4. Существует ли математическая модель шифра Виженера?

Задание:

1. Зашифруйте текст «ПОГОДА ЧУДЕСНАЯ» шифром Виженера, используя в качестве ключа слово «ТОЧКА».
2. Расшифруйте текс «ПЬБШЖГ ЯВЬПЛДР ЮТФЯШЦ», который был зашифрован шифром Виженера, используя ключ «ГОРОД».
3. Зашифруйте текст «Mission: Impossible» шифром Гронсфельда, используя ключ «2671».

§29. Шифр RSA

Ключевые слова: RSA, асимметричное шифрование, простые числа, сравнения по модулю, функция Эйлера

Шифр RSA – алгоритм шифрования с открытым ключом, впервые описанный в 1977 году Роном Ривестом, Ади Шамиром и Леонардом Адлеманом в Массачусетском технологическом институте. Первые буквы их фамилий составляют название алгоритма.

Криптографические системы с открытым ключом используют так называемую одностороннюю функцию, под которой подразумевают практическую невозможность вычислить обратное значение, используя современные вычислительные средства, за обозримый интервал времени.

В основу криптографической системы RSA положена сложность задачи факторизации произведения двух больших простых чисел. Для шифрования используется операция возведения в степень по модулю большого числа. Для дешифрования (обратной операции) за разумное время необходимо уметь вычислять функцию Эйлера от данного большого числа, для чего необходимо знать разложение числа на простые множители.

В криптографической системе с открытым ключом каждый участник располагает как открытым ключом, так и закрытым ключом. В RSA каждый ключ состоит из пары целых чисел. Каждый участник создаёт свой открытый и закрытый ключи самостоятельно. Закрытый ключ каждый из них держит в секрете, а открытые ключи можно сообщать кому угодно или даже публиковать их.

kaspersky

Рассмотрим конкретный пример применения шифра RSA:

1. Формируем ключи.

1 шаг	Возьмем два простых числа	$p = 3, q = 7$
2 шаг	Находим произведение данных простых чисел	$n = p \cdot q = 3 \cdot 7 = 21$
3 шаг	Вычисляем от полученного результата функцию Эйлера	$\varphi(n) = \varphi(21) = \varphi(3 \cdot 7) = (3 - 1) \cdot (7 - 1) = 12$
4 шаг	Выбираем такое число, которое взаимно простое к φ(n)	$e = 5$
5 шаг	Находим такое d, чтобы было справедливо сравнение	$e \cdot d \equiv 1 \pmod{\varphi(n)}$ $5 \cdot d \equiv 1 \pmod{12}$ $d = 17$

Открытым ключом является пара (e,n), а закрытым ключом пара (d,n).

Таким образом, в нашем примере получили открытый ключ (5,21) и закрытый ключ (17,21). Открытый ключ пересылается пользователю, которой и будет шифровать необходимую информацию, после чего перенаправит ее обратно.

2. Пусть пользователь должен выслать последовательность чисел: 1, 2 и 3. Для шифрования он воспользуется открытым ключом (e,n), который был получен ранее, и формулой: $m^e \bmod n$.

1 шаг	Шифруем первое число	$1^5 \bmod 21 = 1$
2 шаг	Шифруем второе число	$2^5 \bmod 21 = 11$
3 шаг	Шифруем третье число	$3^5 \bmod 21 = 12$

Таким образом, высылаются числа: 1, 11 и 12.

3. Расшифруем полученные числа при помощи закрытого ключа (d,n) и формулы: $c^d \bmod n$.

1 шаг	Расшифруем первое число	$1^{17} \bmod 21 = 1$
2 шаг	Расшифруем второе число	$11^{17} \bmod 21 = 2$
3 шаг	Расшифруем третье число	$12^{17} \bmod 21 = 3$

Видим, что расшифрованные числа совпадают с изначальными, которые были подвергнуты шифрованию.

Чтобы взломать шифр, злоумышленнику необходимо узнать секретный показатель степени d. А для этого необходимо найти большие числа p и q. Если их произведение велико, то это сложная задача для современных компьютеров, ее решение перебором вариантов займет очень много времени.

В 2009 году группа ученых из разных стран в результате многочисленных расчетов на сотнях компьютеров смогла расшифровать сообщение, зашифрованное алгоритмом RSA с 768-битным ключом. Поэтому на сегодняшний момент надежными считаются ключи с длиной 1024 бита и более.

Следует отметить, физики, инженеры и математики работают над созданием квантовых компьютеров. Эти компьютеры будут делать все то же самое, что и современные компьютеры, но раскладывать числа на простые множители смогут быстрее, чем с помощью полного перебора. И если это случится, вся идея шифра RSA потеряет надежность.

При использовании симметричных шифров всегда возникает проблема: как передать ключ, если канал связи ненадежный? Так как получив ключ, противник сможет расшифровать все дальнейшие сообщения. Для алгоритма RSA этой проблемы нет, пользователям достаточно обменяться открытыми ключами, которые можно показывать кому угодно.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи, и используется в большом числе криптографических приложений. В настоящее время данный алгоритм активно реализуется как в виде самостоятельных криптографических продуктов, так и в качестве встроенных средств в популярных приложениях. Важнейшей проблемой практической реализации является генерация больших простых чисел.

Вопросы к параграфу:

1. Почему шифр RSA получил такое название?
2. Какое практическое применение имеет шифр RSA?
3. В чем плюсы и минусы шифра RSA?
4. Какие математические понятия используются в шифре RSA?

Задание:

Примените шифр RSA для шифрования числа 10, используя простые числа 7 и 11.

Пояснение: для вычислений можно воспользоваться средствами компьютерной алгебры https://www.wolframalpha.com/

§30. Электронная цифровая подпись

Ключевые слова: электронная цифровая подпись, токен, блокчейн, аутентификация

Электронная цифровая подпись (ЭЦП) – это блок данных, полученный в результате криптографического преобразования электронного документа или его хэша при помощи секретного ключа, принадлежащего определенному человеку или организации. ЭЦП используется для удостоверения (подписания) документа в электронном виде, гарантирует его целостность и неизменность, а также идентифицирует подписанта.

Концепцию электронной цифровой подписи для аутентификации информации предложили У. Диффи и М. Хеллман в 1976г. В основе большинства ЭЦП лежит асимметричный алгоритм шифрования, поэтому для подписи необходимы открытый и закрытый ключи. Они выдаются человеку (или организации) вместе с сертификатом, подтверждающим владение ими. В отличие от шифрования, в случае ЭЦП закрытый ключ используется для постановки подписи, а открытый – для ее расшифровки. Как правило, документы подписывают при помощи специального ПО.

Требования к ЭЦП:

- Однозначно идентифицировать подписанта.
- Давать возможность отследить, был ли документ модифицирован после подписания.
- Соответствовать требованиям законодательства страны, в которой она применяется.

Сертификат и ключи электронной подписи могут храниться на компьютере подписанта, на сервере его контрагента (например, электронная подпись, выданная налоговой службой для подписания деклараций, может храниться на стороне налоговой), а также на отдельном устройстве (например, USB-токене или смарт-карте).

Электронная подпись используется для заверения контрактов, налоговой документации, законов и постановлений, внутренних документов организаций, в блокчейне для авторизации транзакций и многого другого.

Вопросы к параграфу:

1. Что такое электронная цифровая подпись?
2. Какие требования выдвигаются к электронной цифровой подписи?
3. Кто является основоположником концепции электронной цифровой подписи?
4. Какой ранее изученный вами метод шифрования может являться основой электронной цифровой подписи?

§31. Хэш-функции

Ключевые слова: хэш, хэширование, хэш-функция, коллизии

Хэш (от англ. hash – превращать в фарш, мешанина) – последовательность символов фиксированной длины, полученная путем преобразования произвольных исходных данных (числа, текста, файла и др.) при помощи специального математического алгоритма, которая однозначно соответствует этим исходным данным, но не позволяет их восстановить. Процесс преобразования данных в хэш называют **хэшированием**, а алгоритм хэширования – **хэш-функцией**. Большинство распространенных хэш-функций на выходе дают большие числа в шестнадцатеричном представлении.

Преобразование данных в хэши используется в криптографии, а также для верификации и хранения информации. Рассмотрим популярные сферы применения хэширования:

- **Хранение паролей и аутентификации.** Как правило, сервисы хранят массив паролей в виде хэша, чтобы ни администраторы, ни возможные взломщики не имели к ним непосредственного доступа. Для аутентификации пользователя система хэширует введенный им пароль и сравнивает полученный хэш с тем, который хранит для соответствующего логина.
- **Проверка данных на целостность.** При пересылке сообщений и файлов возможны случайные или намеренные искажения данных. Чтобы убедиться, что этого не произошло, отправитель может переслать получателю хэш своего сообщения, а получатель – сравнить ее с хэшем сообщения, которое ему пришло.

- **Поиск вредоносного ПО.** Специалист или защитное решение могут сравнить хэш того или иного файла с базой хэшей вредоносных файлов. Если он совпадет хотя бы с одним хэшем из базы, файл помечается как вредоносный.

Рассмотрим примитивный пример использования хэш-функции. Пусть пользователь установил приложение, вход в которое осуществляется по паролю, длиной 6 символов, состоящему только из цифр. Для хэширования разработчики использовали функцию $h(k) = k \bmod 10$, а изначальный пароль всегда разбивается на двузначные числа. Пусть пользователь установил пароль 459987. Алгоритм действий рассмотрим в таблице:

1 шаг	Пользователь вбил пароль	459987
2 шаг	Программа разбивает пароль на двузначные числа	45 99 87
3 шаг	Применение хэш-функции $h(k) = k \bmod 10$	$h(45) = 45 \bmod 10 = 5$ $h(99) = 99 \bmod 10 = 9$ $h(87) = 87 \bmod 10 = 7$
4 шаг	Получение хэша	597

Таким образом, паролю 459987 соответствует хэш 597, который хранится внутри программы. Каждый раз, когда пользователь вбивает этот пароль, программа вычисляет от него хэш и сверяет со своей базой данных, соответствует ли данный хэш тем данным, которые хранятся в ней. Если хэши совпали, то пользователю предоставляется доступ в приложение. При этом сам пароль нигде не фигурирует.

Хэш обладает следующими свойствами:

- **Необратимость.** Из хэша нельзя восстановить исходные данные ни математическими методами, ни перебором.
- **Воспроизводимость.** Преобразование одних и тех же исходных данных при помощи одной и той же хэш-функции дает на выходе один и тот же результат.
- **Уникальность.** При хэшировании разных исходных данных должны получаться разные хэши, даже если данные различаются незначительно. Ситуация, когда в результате преобразования двух разных паролей получается один и тот же хэш, называется **коллизией**. Высокая вероятность коллизии делает хэш-функцию ненадежной.

Коллизии существуют для большинства хэш-функций, но для «хороших» частота их возникновения стремится к нулю. Так как криптографические хэш-функции используются для подтверждения неизменности исходной информации, то возможность быстрого отыскания коллизии для них обычно равносильна дискредитации. Например, если хэш-функция используется для создания цифровой подписи, то умение находить для неё коллизии фактически равносильно умению подделывать цифровую подпись. Поэтому мерой криптостойкости хэш-функции считается вычислительная сложность нахождения коллизии. В идеале не должно существовать способа отыскания коллизий более быстрого, чем полный перебор. Если для некоторой хэш-функции находится способ получения коллизий существенно более быстрый, чем полный перебор, то эта хэш-функция перестаёт считаться криптостойкой и использоваться для передачи и хранения секретной информации.

На сегодняшний момент для хэширования в большинстве случаев применяют алгоритмы MD5, алгоритмы семейства SHA и российский алгоритм, изложенный в ГОСТ Р34.11-94.

kaspersky

Вопросы к параграфу:

1. Что такое хэширование?
2. Какими свойствами обладает хэш?
3. Что такое коллизии и почему они возникают?
4. Какое применение у хэширования?

Задание:

Пусть пользователь установил приложение, вход в которое осуществляется по паролю, длиной 8 символов, состоящему только из цифр. Для хэширования разработчики использовали функцию h(k) = k mod 5, а изначальный пароль всегда разбивается на двузначные числа. Пусть пользователь установил пароль 17569137. Какой получится хэш от пароля?

§32. Протокол Диффи-Хеллмана

Ключевые слова: протокол, протокол Диффи-Хеллмана, арифметика остатков

Под протоколом понимается договоренность участников о том, что они будут делать. Например, следуя криптографическому протоколу, они могут выработать общий секретный ключ для шифрования своих сообщений.

Протокол Диффи-Хеллмана – криптографический протокол, позволяющий участникам информационного обмена создать общий секретный ключ шифрования, обмениваясь данными по незащищенному каналу связи. Полученный ключ можно использовать для шифрования и расшифровки сообщений с помощью симметричных алгоритмов.

Метод Диффи-Хеллмана решает одну из главных проблем симметричного шифрования – необходимость безопасной передачи ключей. Протокол назван в честь американских специалистов по криптографии Уитфилда Диффи и Мартина Хеллмана, которые первыми опубликовали рабочий алгоритм открытого обмена ключами по сети. Предложенная ими схема используется во многих программах и стандартах шифрованной коммуникации, например, в ПО Gnu Privacy Guard (GnuPG, GPG), VPN-протоколах, и т.д.

В основе протокола лежит концепция неполного обмена ключами шифрования, сформулированная американским криптографом Ральфом Мерклом, реализованная Диффи и Хеллманом в виде криптографического алгоритма с открытым ключом. В соответствии с этой схемой каждый участник обмена выполняет следующие действия:

1. Генерирует случайное натуральное число – закрытый ключ.
2. Совместно с удаленной стороной договаривается об открытых параметрах, которые будут использоваться для создания секретного ключа.
3. На основе закрытого ключа и открытых параметров вычисляет открытый ключ.
4. Обменивается открытыми ключами с удаленной стороной.
5. Вычисляет общий секретный ключ, используя открытый ключ удаленной стороны, свой закрытый ключ и открытые параметры.

kaspersky

Рассмотрим конкретный пример реализации, где Пользователь1 знает только свое секретное значение a, Пользователь2 знает только свое секретное значение c.

1 шаг	Пользователь1	Выбор простого числа p, произвольного g, секретного числа a	p = 7 g = 10 a = 4
2 шаг	Пользователь1	Вычисление значения $A = g^a \bmod p$	$A = 10^4 \bmod 7 = 4$
3 шаг	Пользователь1	Отправка Пользователю2 значений p, g, A	7 10 4
4 шаг	Пользователь2	Выбор секретного числа c	c = 5
5 шаг	Пользователь2	Вычисление значения $C = g^c \bmod p$	$C = 10^5 \bmod 7 = 5$
6 шаг	Пользователь2	Отправка Пользователю1 значения C	5
7 шаг	Пользователь1	Вычисление $C^a \bmod p$	$5^4 \bmod 7 = 2$
8 шаг	Пользователь2	Вычисление $A^c \bmod p$	$4^5 \bmod 7 = 2$

Таким образом получаем, что секретный ключ $C^a \bmod p = A^c \bmod p$ равен 2. Этот ключ может быть использован для дальнейшего шифрования и расшифрования сообщений между данными пользователями.

Чтобы такая схема была безопасной, числа должны быть большими: a, c, g и p должны быть выбраны таким образом, чтобы каждое число было длиной несколько сотен цифр. Кроме того, секретные числа a и c должны выбираться случайным образом. Если требования соблюдены, у злоумышленников не остается разумного метода обнаружения общего секретного ключа без знания a или c.

Метод Диффи-Хеллмана применим для любого количества участников коммуникации. Для получения общего секретного ключа необходимо, чтобы все участники обмена по очереди произвели вычисления над открытым ключом с использованием общих открытых параметров и своих закрытых ключей.

С точки зрения продолжительности жизни закрытых ключей различают два варианта реализации протокола Диффи-Хеллмана:

- **Статический.** Используются долгосрочные закрытые ключи, которые не сбрасываются после разрыва соединения.
- **Эфемерный (краткосрочный).** Закрытые ключи генерируются заново для каждого нового соединения.

Предложенная Диффи и Хеллманом система не предусматривает аутентификацию участников обмена и согласованного ключа. По этой причине протокол уязвим к атакам «человек посередине». Злоумышленник может внедриться в канал связи и организовать перехват и подмену сообщений протокола. В результате стороны установят защищенное соединение не друг с другом, а со злоумышленником, и тот сможет читать их переписку без их ведома.

kaspersky

Вопросы к параграфу:

1. В чем смысл протокола Диффи-Хеллмана?
2. Какие математические понятия фигурируют в реализации протокола Диффи-Хеллмана?
3. В чем различие статического и эфемерного закрытых ключей при реализации протокола Диффи-Хеллмана?
4. Какая существует уязвимость в использовании протокола Диффи-Хеллмана?

Задание:

Вычислите секретный ключ, который передается пользователями по протоколу Диффи-Хеллмана, если первый пользователь выбрал в качестве простого числа $p = 11$, произвольного $g = 2$, секретного числа $a = 10$ и отправил необходимые значения второму пользователю, который выбрал секретное число $c = 6$.

§33. Квантовые компьютеры и постквантовое шифрование

Ключевые слова: квантовый компьютер, бит, кубит, криптография, RSA

Квантовый компьютер – вычислительное устройство, построенное на принципах квантовой механики. Теоретическая производительность таких компьютеров во много раз превышает традиционные системы на базе полупроводниковых процессоров.

Квантовый компьютер оперирует кубитами (квантовыми битами) – минимальными квантовыми единицами хранения информации. С точки зрения физики кубит – это элементарная частица, а значение кубита – это значение одного из физических свойств этой частицы.

В отличие от классических битов, которые могут иметь только одно из двух значений («1» или «0»), кубиты в процессе вычислений (пока их итоговое состояние не измерят) находятся в суперпозиции этих двух значений, то есть с определенной вероятностью могут принять любое из них. Кроме того, каждый кубит постоянно взаимодействует с другими кубитами квантовой системы таким образом, что их состояния влияют друг на друга.

Благодаря особенностям кубитов квантовый компьютер в теории может решать некоторые задачи, для которых мощностей обычных компьютеров недостаточно. При этом для решения некоторых других задач квантовый компьютер не предназначен.

К числу задач, в которых квантовые компьютеры могут быть эффективнее классических, относятся:

- Создание новых криптографических алгоритмов.
- Быстрый поиск по базам данных.
- Моделирование молекулярных систем.
- Ресурсоемкие научные исследования.

Также квантовые компьютеры в теории могут облегчить взлом асимметричных алгоритмов шифрования, таких как RSA.

Пока опасность использования квантовых алгоритмов для взлома асимметричного шифрования в основном теоретическая. Чтобы воплотить такой взлом на практике, мощности существующих квантовых компьютеров недостаточно.

В последнее время считалось, что до появления достаточно больших квантовых систем есть еще лет десять. Однако опубликованная в 2023 году научная работа предложила определенные способы оптимизировать взлом, используя комбинацию классических и квантовых вычислений.

Несмотря на огромные теоретические вычислительные возможности квантовых компьютеров, на практике они развиваются довольно медленно. Для них характерен ряд проблем, которые исследователи пока решают с переменным успехом.

- **Чувствительность к окружению.** Внешние факторы влияют на состояние отдельных кубитов и системы в целом. Дестабилизировать ее могут малейшие изменения температуры, давления, или, например, пролетевший рядом фотон. Чтобы обеспечить стабильную работу квантовых компьютеров, их устанавливают в изолированных от внешней среды саркофагах, внутри которых поддерживается температура, близкая к абсолютному нулю. Системы экранирования и охлаждения стоят дорого и занимают много места.
- **Ошибки вычислений.** Результат квантовых вычислений – вероятностный, то есть не всегда правильный. При этом в работе квантовых систем, как и в работе традиционных компьютеров, могут возникать сбои и ошибки. Чем сложнее и мощнее система, тем больше она подвержена ошибкам.
- **Отсутствие стандартов.** Существующие квантовые компьютеры реализованы по-разному, поэтому универсального ПО для работы с ними нет. Эта проблема была характерна и для традиционных компьютеров на ранних этапах их развития.

Квантовая криптография – это наука о шифровании данных методами, основанными на законах квантовой механики. В отличие от традиционной криптографии, квантовое шифрование предполагает защиту и передачу данных при помощи физических свойств элементарных частиц.

В квантовой криптографии информация кодируется в виде состояний квантовых частиц. В первую очередь для этой цели используются фотоны, которые можно передавать по оптическому кабелю. Квантовую частицу невозможно полностью скопировать, а любое измерение ее состояния приведет к его изменению, что в теории позволяет однозначно определить факт перехвата передаваемой информации.

Чаще всего квантовые частицы используются для генерации и передачи криптографических ключей. Если посторонний попытается перехватить ключ, состояние частиц изменится, и легитимные стороны узнают, что ключ скомпрометирован.

Как и в случае с квантовыми компьютерами, существует ряд проблем, которые препятствуют повсеместному внедрению квантовых криптографических технологий. Во-первых, создание и поддержка сетей для квантовой коммуникации стоят дорого.

Другая проблема при реализации шифрования, использующего физические свойства квантовых частиц – дальность передачи информации. Чем больше дистанция, на которую нужно передать секретный ключ, тем выше риск, что не все фотоны дойдут до получателя в исходном состоянии.

Несмотря на это, методы квантовой криптографии применяются на практике в исследовательских центрах и коммерческих компаниях.

Анализируя сложившуюся в IT-индустрии практику, идеальный вариант внедрения постквантовой криптографии состоит в гибридном шифровании данных: то есть в шифровании «в два слоя» – сначала классическим алгоритмом, а потом постквантовым. Таким образом атакующему придется иметь дело с обеими криптосистемами, что сильно снижает шансы успешного взлома. Именно такой подход уже используют в Signal, Apple, Google и Zoom.

kaspersky

Вопросы к параграфу:

1. Что такое квантовый компьютер?
2. В чем заключается основная разница между битом и кубитом?
3. Какие проблемы встречаются в работе квантовых компьютеров?
4. Какие плюсы и минусы использования квантовых компьютеров в криптографии?
5. Почему метод шифрования RSA в будущем может потерять надежность при благополучном развитии квантовых компьютеров?
6. Какой подход постквантовой криптографии является актуальным для защиты данных?

§34. Стеганография

Ключевые слова: стеганография, контейнер, стегоанализ, Zero.T, гистограммный метод

Стеганография (от греч. Στεγανός – скрытый + γράφω – пишу; буквально «тайнопись») – наука, позволяющая спрятать передаваемые данные в некотором контейнере, таким образом скрыв сам факт передачи информации.

Контейнер (стегоконтейнер) – любой объект, используемый для тайного внедрения сообщения.

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых запрещена криптография.

Спрятать секретное послание можно практически в любой цифровой объект – текстовый документ, лицензионный ключ, расширение файла. Однако один из самых удобных «контейнеров» – медиафайлы (картинки, аудио, видео и так далее). Они обычно достаточно большие сами по себе, а значит, и скрываемая информация может быть не такой маленькой, как в случае, скажем, с документом Word.

Секретную информацию можно записать в метаданные файла или же прямиком в основное содержимое. Возьмем, например, картинку. С точки зрения компьютера она представляет собой набор из сотен тысяч точек-пикселей. У каждого пикселя есть «описание» – информация о его цвете.

Для формата RGB, который используется в большинстве цветных картинок, это описание занимает в памяти 24 бита. Если в описании некоторых или даже всех точек 1–3 бита будет занято секретной информацией, на картинке в целом изменения будут неразличимы. А за счет огромного числа пикселей всего в изображение можно вписать довольно много данных.

Изначальное изображение

Изображение с внедренной информацией

Если сравнить изначальное графическое изображение и внедренное, в которое вшили стихотворение Александра Сергеевича Пушкина «У лукоморья дуб зеленый», то заметим, что на глаз нет никакой разницы.

В большинстве случаев прячут информацию в пиксели и извлекают ее оттуда при помощи специальных утилит. Иногда для этой цели пишут собственные скрипты или добавляют нужную функциональность в программы другого назначения. А иногда пользуются готовыми кодами, которых в сети немало.

Исторически впервые понятие стеганографии было введено в 1499 году, но сам метод существовал очень давно. Легенды донесли до нас метод, который использовался в Римской империи: для доставки сообщения выбирали раба, голову которого брили, а затем с помощью татуировки наносили текст. После того как волосы отрастали, раба отправляли в путь. Получатель сообщения снова обривал голову раба и читал сообщение.

В течение всего XX века активно развивалась как стеганография, так и наука об определении факта внедрения информации в контейнер – **стегоанализ**.

На сегодняшний момент наблюдается новый и опасный тренд: все больше разработчиков вредоносного ПО и средств кибершпионажа прибегает к использованию стеганографии. Большинство антивирусных решений не защищают от стеганографии или защищают слабо, меж тем, нужно понимать, что каждый заполненный контейнер опасен. В нем могут быть скрыты данные, которые эксфильтруются шпионским ПО, или коммуникация вредоносного ПО с командным центром, или новые модули вредоносного ПО.

Качественную стеганографию распознать крайне сложно. Избавиться от нее тоже не так-то просто: есть методы, позволяющие вшить сообщение в картинку настолько глубоко, что оно сохранится даже после того, как ее напечатают и снова отсканируют, уменьшат, увеличат или еще как-то отредактируют.

Однако решения есть, они основаны на комбинировании различных способов анализа, высокоскоростных предетектах, исследовании метаданных потенциально заполненного контейнера и т.п. Такие решения есть у Лаборатории Касперского – платформа защиты от таргетированных атак – KATA. Ее использование позволяет сотруднику службы информационной безопасности своевременно узнать о возможной таргетированной атаке на защищаемый периметр и/или эксфильтрации данных из него.

За недавнее время наблюдается использование стеганографии в следующих вредоносных программах и средствах кибершпионажа: Microcin (AKA six little monkeys); NetTraveler; Zberp; Enfal (its new loader called Zero.T); Shamoon; KinS; ZeusVM; Triton (Fibbit).

На сегодня учеными разработаны и опробованы различные алгоритмы и методы стеганографии. Вот некоторые из них:

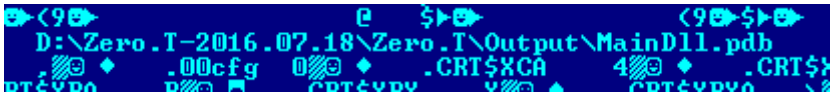
- LSB-стеганография – сообщение скрывается в младших битах (возможно использование одного или нескольких младших бит) контейнера. Чем меньше битов задействовано, тем меньше артефактов получает оригинальный контейнер после внедрения.
- Метод сокрытия информации при помощи младших бит палитры – этот метод по сути является вариантом общего метода LSB, но информация встраивается не в наименее значащие биты контейнера, а в наименее значащие биты палитры, очевидный недостаток такого метода – низкая емкость контейнера.
- Метод сокрытия информации в служебных полях формата – метод, основанный на использовании служебных полей заголовка контейнера для хранения сообщения. Очевидные минусы – низкая емкость контейнера и возможность обнаружения внедренных данных при помощи обычных программ для просмотра изображения (которые иногда позволяют видеть содержимое служебных полей).
- Метод встраивания сообщения – заключается в том, что сообщение встраивается в контейнер, затем при помощи схемы, известной обеим сторонам, извлекается. Можно встроить несколько сообщений в один контейнер, при условии, что способы их внедрения ортогональны.
- Широкополосные методы, которые подразделяются на:
    - метод псевдослучайной последовательности: используется секретный сигнал, который моделируется псевдослучайным сигналом.
    - метод прыгающих частот: частота несущего сигнала меняется по определенному псевдослучайному закону.
- Метод оверлея – по сути не является настоящей стеганографией, основан на том, что некоторые форматы содержат в заголовке размер данных, или же обработчик этих форматов будет читать файл до маркера конца данных. Примером такого метода является метод «rar-jpeg», который основан на конкатенации графического файла в формате JREG и RAR-архива. ПО для просмотра JPEG будет считывать информацию до границы, указанной в заголовке файла, а RAR-архиватор откинет все, что находится до сигнатуры «RAR!», которая обозначает начало архива. Таким образом, если такой файл открыть в программе для просмотра графических файлов, то увидим картинку, а если в RAR-архиваторе – содержимое RAR-архива. Минусы такого подхода заключаются в том, что оверлей, добавленный к контейнеру, легко выделяем при визуальном исследовании такого файла.

Авторы вредоносного ПО все активней используют стеганографию в своих разработках. Выделим три главные причины:

- Это позволяет им скрыть сам факт загрузки/выгрузки данных, а не только сами данные;
- Помогает обойти DPI-системы, что актуально в корпоративных сетях;
- Использование стеганографии может позволить обойти проверку в AntiAPT-продуктах, поскольку последние не могут обрабатывать все графические файлы (их слишком много в корпоративных сетях, а алгоритмы анализа довольно дорогие).

Подробно рассмотрим пример использования стеганографии – угроза **Zero.T**. Этот загрузчик был обнаружен Лабораторией Касперского в конце 2016 года, но первое описание было опубликовано компанией Proofpoint.

Угрозу назвали Zero.T, так как такая строка присутствует в его исполняемом коде (в пути к pdb-файлу проекта):



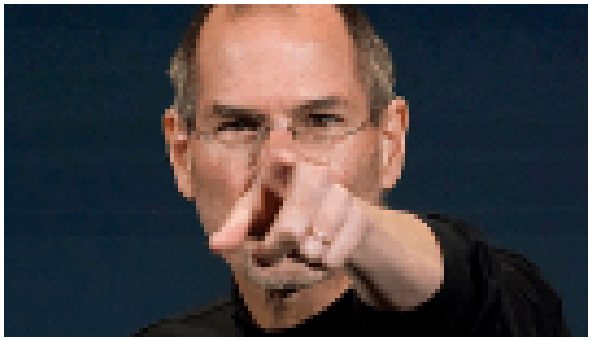
Не останавливаясь на попадании в систему и закреплении в ней, отметим, что Zero.T скачивает полезную нагрузку в виде Bitmap-файлов:

fsguidll.bmp
fslapi.bmp
fslapi.dll.bmp

Обрабатывает их особым образом, после чего получает вредоносные модули:

fsguidll.exe
fslapi.dll
fslapi.dll.bmp

На поверку эти три BMP-файла оказались картинками:



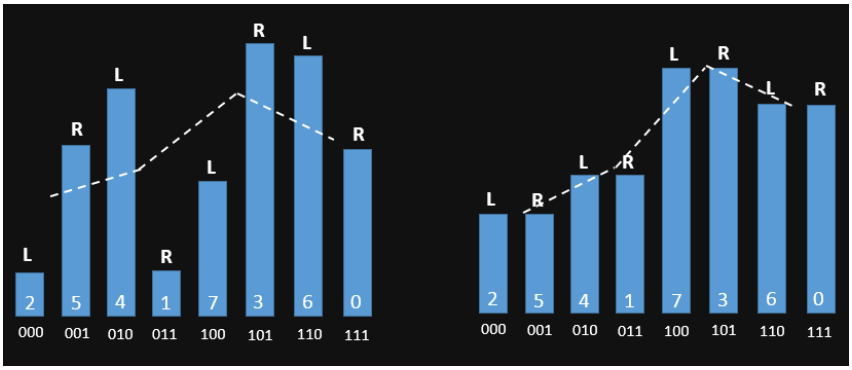
Но картинки эти не совсем обычные – заполненные контейнеры, в каждом из которых несколько (алгоритм допускает вариативность) младших значащих бит заменены на полезную нагрузку.

Как же определить, является ли картинка заполненным контейнером или нет?

Рассмотрим статистический метод анализа – гистограммный метод.

Описываемый метод, предложенный в 2000 году Андресом Вестфелдом и Андреасом Пфитцманом, также известен как «хи-квадрат»-метод. Попытаемся изложить его суть.

Весь растр анализируется, для каждого цвета считается количество точек такого цвета в растре (для простоты здесь говорим про изображение, имеющее одну цветовую плоскость).



а – пустой контейнер б – заполненный контейнер

Метод исходит из предположения, что количество точек двух соседних цветов («соседние» цвета – цвета, которые отличаются только наименее значимым битом) различается существенно для нормального, обычного изображения (пустого контейнера). И количество пикселей таких цветов является примерно одинаковым для заполненного контейнера.

Вопросы к параграфу:

1. Что такое стеганография?
2. В чем отличие стеганографии и шифрования?
3. Для чего используют стеганографию?
4. Какие способы и методы стеганографии вам известны?
5. Можно ли выявить стеганографию в графическом файле?

kaspersky

Литература

1. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. – Екатеринбург: Изд-во Урал. ун-та, 2019. – 204с.
2. Коробейников А.Г. Математические основы криптологии. Учебное пособие. – СПб: СПб ГУ ИТМО, 2004. – 106с.
3. Поляков К.Ю. Информатика. Базовый и углублённый уровни: учебник для 10 класса: в 2 ч. Ч. 2 / К.Ю. Поляков, Е.А. Еремин. – М.: БИНОМ. Лаборатория знаний, 2024. – 352с.: ил.
4. Рацеев С.М. Математические методы защиты информации: учеб. пособие для вузов / С.М. Рацеев. – СПб: Лань, 2023. – 544с.
5. Смарт Н. Криптография. – М.: Техносфера, 2006. – 528с.
6. Сухостат В.В. Основы информационной безопасности: учебное пособие / В.В. Сухостат, И.Н. Васильева. – СПб.: Изд-во СПбГЭУ, 2019. – 103с.
7. Федотов Н.Н. Форензика – компьютерная криминалистика. – М.: Юридический Мир, 2007. – 432с.
8. Феррейра Фило Владстон, Теоретический минимум по Computer Science. Сети, криптография и data science. – СПб.: Питер, 2022. – 288с.
9. Шнайер Б. Практическая криптография.: Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 432с.: ил.
10. Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходный код на языке С. – М.: Диалектика, 2022. – 1030с.

kaspersky

Полезные ссылки

Название портала	Описание	Ссылка на портал
Education	Бесплатный обучающий ресурс, на котором можно освоить комплекс знаний и практических умений по основам информационной безопасности в интерактивном формате. По окончании каждого курса генерируется сертификат о прохождении.	https://education.kaspersky.com/ru/
Блог Касперского	Самые свежие новости из мира информационной безопасности, написанные экспертами компании. Постоянно обновляющиеся новости, советы по различным проблемам в области корпоративной и личной информационной безопасности.	https://www.kaspersky.ru/blog/
Securelist	Сайт со всей отчетностью Лаборатории Касперского об угрозах информационной безопасности, анализе угроз, реверс-инжиниринге вирусов и статистике.	https://securelist.ru/
Kids safe media	Сайт о защите детского информационного пространства, на котором расположены различные видео, тексты, интерактивы и методические разработки для проведения занятий по информационной безопасности.	https://kids.kaspersky.ru/
Kaspersky.Academy	Сайт с различной курсовой подготовкой по востребованным разделам информационной безопасности (как для личного обучения, так и для корпоративного).	https://academy.kaspersky.ru/
Курс «Математика в кибербезопасности» на платформе Stepik	Бесплатный курс доступен как для школьников, так и для всех заинтересованных. Рассматриваются те математические темы, которые связаны непосредственно с информационной безопасностью, в частности, с шифрованием и защитой данных.	https://stepik.org/62247

kaspersky

www.kaspersky.com/
www.securelist.com