Балаковский инженерно-технологический институт - филиал

федерального государственного автономного образовательного учреждения

высшего образования

«Национальный исследовательский ядерный университет «МИФИ»

Факультет атомной энергетики и технологий

Кафедра

КОНТРОЛЬНАЯ РАБОТА

по дисциплине

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил: студент группы \_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_2024г.

|  |  |
| --- | --- |
|  | Проверил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  должность  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_2024г. |

Балаково 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3

1 Распространенные угрозы интернет-безопасности 4

2 Как защитить личные данные в сети 7

ЗАКЛЮЧЕНИЕ 10

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ 11

Практическое задание 1 12

Практическое задание 2 13

ВВЕДЕНИЕ

Интернет-безопасность – это безопасность действий и транзакций, совершаемых в интернете. Интернет-безопасность входит в более широкие понятия, такие как кибербезопасность и компьютерная безопасность, и включает безопасность браузера и сети, а также правильное поведение в сети.

Проводя значительное время в сети, можно столкнуться со следующими угрозами интернет-безопасности:

* Взлом – получение неавторизованными пользователями доступа к компьютерным системам, учетным записям электронной почты и веб-сайтам;
* Вирусы и вредоносные программы, которые могут повредить данные и сделать системы уязвимыми для других угроз;
* Кража личных данных, например, личной и финансовой информации злоумышленниками.

Частные лица и организации могут защититься от подобных угроз, используя приемы интернет-безопасности.

1 Распространенные угрозы интернет-безопасности

Чтобы сохранить конфиденциальность и безопасность в интернете, важно знать о различных типах интернет-атак. Ниже описаны распространенные угрозы интернет-безопасности.

Фишинг – это кибератака с использованием поддельных писем. Злоумышленники пытаются обмануть получателей электронной почты, убедив их в подлинности и актуальности сообщения. Например, они маскируют письма под запросы из банка или сообщения от коллег, чтобы пользователи переходили по ссылкам или открывали вложения. Цель атаки состоит в том, чтобы обманным путем заставить пользователей раскрыть личную информацию или загрузить вредоносные программы.

Фишинг – одна из старейших угроз интернет-безопасности, возникшая еще в 1990-х годах. Он остается популярным и сегодня, поскольку является одним из самых дешевых и простых способов кражи информации. В последние годы фишинговые сообщения и используемые методы становятся все более изощренными.

Взлом и удаленный доступ.

Злоумышленники всегда стремятся использовать уязвимости частной сети или системы для кражи конфиденциальной информации и данных. Технология удаленного доступа предоставляет им дополнительные возможности. Программное обеспечение для удаленного доступа позволяет пользователям получать доступ к компьютеру и управлять им удаленно. Его использование значительно выросло в период пандемии, когда все больше людей работают удаленно.

Протокол, позволяющий пользователям удаленно управлять компьютером, подключенным к интернету, называется RDP – протокол удаленного рабочего стола. Многие компании, независимо от размера, широко используют RDP, поэтому высоки шансы недостаточно надежной защиты сети. Злоумышленники используют различные методы выявления и эксплуатации уязвимостей RDP, чтобы получить полный доступ к сети и ее устройствам. Они могут как самостоятельно осуществлять кражу данных, так и продавать учетные данные в даркнете.

Вредоносные программы и вредоносная реклама.

Термин вредоносные программы охватывает все программы: вирусы, черви, трояны и прочие, которые злоумышленники используют для нанесения ущерба и кражи конфиденциальной информации. Любое программное обеспечение, предназначенное для повреждения компьютера, сервера или сети, может расцениваться как вредоносное.

Термин «вредоносная реклама» описывает онлайн-рекламу, распространяющую вредоносные программы. Интернет-реклама – это сложная экосистема, включающая веб-сайты рекламодателей, рекламные биржи, рекламные серверы, сети ретаргетинга и сети доставки контента. Злоумышленники используют эту сложность для размещения вредоносного кода там, где рекламодатели и рекламные сети не всегда могут его обнаружить. Пользователи, взаимодействующие с вредоносной рекламой, могут загрузить вредоносные программы на свое устройство или перейти на вредоносные веб-сайты.

Программы-вымогатели – это вредоносные программы, блокирующие использование компьютера или доступ к определенным файлам на компьютере, пока не будет уплачен выкуп. Они часто распространяются как троянские программы – вредоносные программы, замаскированные под легальные. После установки программа-вымогатель блокирует экран системы или определенные файлы до тех пор, пока злоумышленники не получат выкуп.

Для сохранения анонимности злоумышленники обычно требуют платежи в криптовалютах, например, биткойнах. Стоимость выкупа варьируется в зависимости от программы-вымогателя и курса обмена цифровых валют. Однако злоумышленники не всегда разблокируют зашифрованные файлы после получения выкупа.

Опасности в публичных и домашних сетях Wi-Fi

Использование публичных сетей Wi-Fi – в кафе, торговых центрах, аэропортах, отелях и ресторанах – сопряжено с определенными рисками, поскольку уровень безопасности в этих сетях часто низкий или защита полностью отсутствует. Это означает, что киберпреступники могут отслеживать действия пользователей в интернете и красть пароли и личную информацию. Другие опасности использования публичных сетей Wi-Fi включают:

Прослушивание сети – злоумышленники отслеживают и перехватывают незашифрованные данные при передаче по незащищенной сети.

Атаки типа «человек посередине» – злоумышленники взламывают точку доступа Wi-Fi и подключаются к процессу передачи данных между пользователем и точкой доступа с целью перехвата и изменения данных в процессе передачи.

Мошеннические сети Wi-Fi – злоумышленники создают приманку в виде бесплатной сети Wi-Fi для сбора личных данных. Точка доступа злоумышленника служит каналом для всех данных, передаваемых по сети.

Слежка за домашней сетью Wi-Fi не должна вызывать столько беспокойства, поскольку сетевое оборудование принадлежит вам. Но опасность, тем не менее, существует: в США провайдерам интернет-услуг разрешено продавать данные о пользователях. Хотя эти данные являются анонимными, сам факт сбора данных может вызывать беспокойство у тех, кто ценит конфиденциальность и безопасность в интернете. Использование VPN в домашней сети значительно усложняет отслеживание вашей онлайн-активности.

2 Как защитить личные данные в сети

Чтобы обеспечить безопасность в интернете и защитить свои данные, можно следовать перечисленным ниже рекомендациям.

Используйте многофакторную аутентификацию везде, где возможно

* Многофакторная аутентификация – это способ проверки подлинности, при котором для доступа к учетной записи используется два или более метода проверки. Например, вместо простого запроса имени пользователя или пароля при многофакторной аутентификации запрашивается дополнительная информация:
* Дополнительный одноразовый пароль, который серверы аутентификации веб-сайта отправляют на телефон или адрес электронной почты;
* Ответы на личные вопросы безопасности;
* Отпечаток пальца или другая биометрическая информация.

Многофакторная аутентификация снижает вероятность кибератаки. Чтобы защитить онлайн-аккаунты, рекомендуется по возможности использовать многофакторную аутентификацию. Для обеспечения безопасности в интернете можно также можете применять сторонние приложения проверки подлинности, такие как Google Authenticator и Authy.

Используйте сетевой экран

Сетевой экран исполняет роль барьера между вашим компьютером и сетью, например интернетом. Сетевые экраны блокируют нежелательный трафик, а также помогают предотвратить заражение компьютера вредоносными программами. Часто сетевой экран входит в состав операционной системы или системы безопасности. Для обеспечения максимальной безопасности в интернете рекомендуется убедиться, что сетевой экран включен и настроено автоматическое обновление.

Внимательно относитесь к выбору браузера

Браузер – это основной инструмент для выхода в интернет, он играет ключевую роль в обеспечении безопасности в интернете. Хороший веб-браузер должен быть безопасным и обеспечивать защиту от утечки данных. Фонд свободы прессы составил подробное руководство, описывающее плюсы и минусы безопасности основных веб-браузеров.

Создавайте надежные пароли и используйте менеджер паролей

Надежный пароль помогает обеспечить безопасность в интернете. Он обладает следующими свойствами:

Длинный: минимум 12 символов, в идеале, даже больше.

Содержит заглавные и строчные буквы, а также специальные символы и цифры.

Не очевидный: в пароле не используются комбинации последовательных цифр (1234) и личная информация, которую может угадать тот, кто вас знает, например, дата рождения или имя домашнего животного.

Не содержит запоминающихся сочетаний клавиш.

Замена букв и цифр похожими символами, например, “P@ssw0rd” вместо “password”, сейчас уже не является эффективной мерой – злоумышленники умеют обходить такую замену. Чем сложнее ваш пароль, тем сложнее его взломать. Использование менеджера паролей позволяет создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи.

Пароли необходимо хранить в секрете, никому не сообщать и нигде не записывать. Рекомендуется не использовать один пароль для всех учетных записей, а также регулярно менять пароли.

Используйте на устройствах последнюю версию программы безопасности

Антивирус, обеспечивающий защиту в интернете, очень важен для сохранения конфиденциальности и безопасности. Лучшие программы интернет-безопасности защищают от различных видов атак, а также обеспечивают безопасность данных в интернете. Очень важно обновлять антивирусное программное обеспечение. Большинство современных программ обновляются автоматически, что гарантирует защиту от последних угроз интернет-безопасности.

Используйте на устройствах последнюю версию программы безопасности

Антивирус, обеспечивающий защиту в интернете, очень важен для сохранения конфиденциальности и безопасности. Лучшие программы интернет-безопасности защищают от различных видов атак, а также обеспечивают безопасность данных в интернете. Очень важно обновлять антивирусное программное обеспечение. Большинство современных программ обновляются автоматически, что гарантирует защиту от последних угроз интернет-безопасности.

ЗАКЛЮЧЕНИЕ

Формирование информационной культуры и безопасности – процесс длительный и сложный, но важный и необходимый. Задача взрослых (педагогов, родителей) – формирование разносторонней интеллектуальной личности, высокий нравственный уровень которой будет гарантией ее информационной безопасности. А для этого необходимо повышать квалификацию педагогов по вопросам информационной безопасности, чтобы уметь оперативно ориентироваться и ориентировать детей в вопросах безопасного поведения в Интернете. Регулярно проводить родительский всеобуч по вопросам кибербезопасности и работать не вдогонку, а на опережение.

Ребенок не станет пропадать в Интернете, если он занят очень интересным для него делом, если его реальный мир намного ярче и увлекательней мира виртуального. Нужно развивать способности и тягу ребенка к реальным действиям и достижениям: кружки, факультативы, секции, дополнительное образование. К тому же настоящие социальные навыки, настоящая культура формируется только в совместном интересном труде. Если не направить позитивную энергию ребенка — она будет поглощена Интернетом, а ребенок останется опустошенным, бесцельно блуждающим по бесконечному Интернет пространству в ожидании от него чуда.

Мир меняется, наши дети отличаются от нас, какими мы были в том же возрасте, но ценность семьи для них остается по-прежнему очень высокой. Обратите внимание на своих детей! Интересуйтесь их жизнью, станьте им друзьями. И, возможно, реальное пространство станет для ваших детей более притягательным, чем виртуальное.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления / А. Ю. Пучков, А. М. Соколов, С. С. Широков, Н. Н. Прокимнов // Прикладная информатика. - 2023. - Т. 18, № 2. - С. 85-102.
2. Баринова А. Как HR-у самостоятельно провести обучение по информационной безопасности: готовый конспект лекций по главным угрозам / А. Баринова // Директор по персоналу. - 2022. - № 5. - С. 40-45.
3. Белов А. С. Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. - 2022. - № 4. - С. 76-80.
4. Васильев В. И. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров / В. И. Васильев, А. М. Вульфин, Н. В. Кучкарова // Вопросы кибербезопасности. - 2022. - № 2. - С. 27-38.
5. Гладких А. В. Методы защиты от DDoS –атак в интеллектуальных сетях / А. В. Гладких // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 3-5.
6. Гладков А. Н. Визуализация киберугроз как аспект формирования компетенций в области информационной безопасности = Visualization of Cyber Threats as an Aspect of the Formation of Competencies in the field of Information Security / А. Н. Гладков, С. Н. Горячев, Н. С. Кобяков // Защита информации. Инсайд. - 2023. - № 1. - С. 32-37.

Практическое задание 1

Ниже представлена реализация задания генерация пароля.

package org.example;

import java.util.Scanner;

import java.util.Random;

public class Main{

public static void main(String[] args) {

Scanner in = new Scanner(System.in);

System.out.println("Введите число в диапозоне от 3 до 15");

int count = in.nextInt();

passwordGenerator(count, "GShQVvZSLgigZR7PdRKw");

}

public static void passwordGenerator(int count, String charList){

StringBuilder password = new StringBuilder();

if(count < 3) { count = 3; }

if(count > 15) { count = 15; }

for (int i = 1; i <= count; i++ ) {

Random rand = new Random();

int indexChar = rand.nextInt(charList.length() - 1);

password.append(charList.charAt(indexChar));

}

System.out.print(password);

}

}

Результат выполнение программы представлен ниже на рисунке1

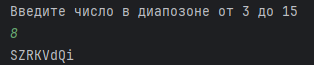


Рисунок 1 – результат выполнения программы

Практическое задание 2

Ниже представлено выполнения задания шифрование сообщения.

Слово: Прохладная вода хорошо освежила уставших ребят

Магическая матрица представлена в таблице 1.

Таблица 1 – магическая матрица

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 28 | 19 | 10 | 1 | 48 | 39 | 30 |
| 29 | 27 | 18 | 9 | 7 | 47 | 38 |
| 37 | 35 | 26 | 17 | 8 | 6 | 46 |
| 45 | 36 | 34 | 25 | 16 | 14 | 5 |
| 4 | 44 | 42 | 33 | 24 | 15 | 13 |
| 12 | 3 | 43 | 41 | 32 | 23 | 21 |
| 20 | 11 | 2 | 49 | 40 | 31 | 22 |

Шифртекст представлена в таблице 2.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Ж | Р | Я | П |  | И | Л |
| И | Е | О | А | Д |  | Ш |
| В | Т | В | Х | Н | А | Т |
| Я | А | С | С |  | Д | Л |
| Х | Б | Р | У | О | А | О |
| В | О | У |  |  |  | Ш |
| О |  | Р |  | Х | А | О |

Таблица 2 – шифртекст