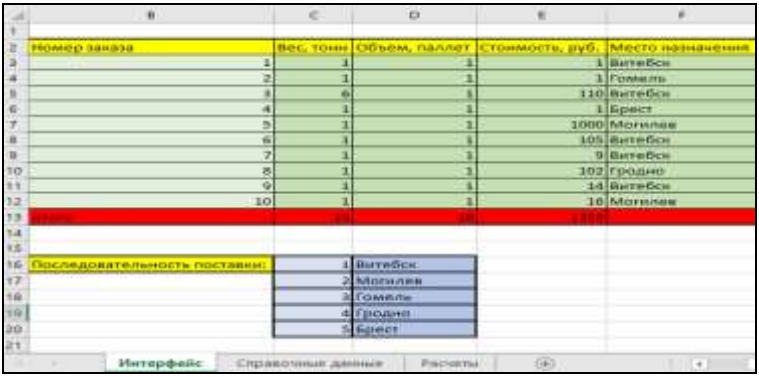

	B	C	D	E	F
1					
2	Номер заказа	Вес, тонн	Объем, паллет	Стоимость, руб.	Место назначения
3	1	1	1	1	Витебск
4	2	1	1	1	Гомель
5	3	6	1	110	Витебск
6	4	1	1	1	Брест
7	5	1	1	1000	Могилев
8	6	1	1	105	Витебск
9	7	1	1	9	Витебск
10	8	1	1	102	Гродно
11	9	1	1	14	Витебск
12	10	1	1	10	Могилев
13	Итого:	15	10	1352	
14					
15					
16	Последовательность поставки:	1	Витебск		
17		2	Могилев		
18		3	Гомель		
19		4	Гродно		
20		5	Брест		
21					

Интерфейс | Справочные данные | Расчеты

Рис. 1 – Результат работы моделируемой СППР.

Прототип этой системы может быть использован на любом предприятии города Минска.

Обучение студентов принципам построения СППР помогает ему приобрести навыки творческого подхода к решению задач в дальнейшей профессиональной деятельности.

Литература

1. Логистика и управление цепями поставок: практическое пособие / Д. В. Курочкин. – Минск: Альфа-книга, 2016. – 783 с.

2. Логистика и управление цепями поставок: учебник / [В. В. Щербаков и др.]. – Москва: Юрайт, 2015. – 581 с.

УДК 004.056.5

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Ковалькова И.А.
Белорусский национальный технический университет

Обеспечение кибербезопасности в современных условиях является одним из наиболее актуальных вопросов, связанных с использованием информационных технологий. С ростом числа интернет-пользователей, использующих различные онлайн-сервисы для работы, шопинга, общения и увеличением объёма информации, передаваемой через сеть, возрастает и количество угроз для безопасности данных. Увеличение угроз для

информационных систем и данных, в свою очередь, ставит под угрозу личную и коммерческую информацию, экономику и национальную безопасность.

Вместе с тем, киберпреступники постоянно ищут новые способы для хищения данных и денег, осуществления кибершпионажа и других злонамеренных действий в сети.

К наиболее распространённым угрозам кибербезопасности, с которыми сталкиваются компании, организации и частные лица в настоящее время относятся:

1) *Фишинг* – метод мошенничества, при котором киберпреступники отправляют электронные письма или сообщения, притворяясь представителями известных компаний или официальных органов, чтобы получить доступ к ценной информации (логинам, паролям, номерам кредитных карт и т.д).

2) *Вредоносное ПО* – программное обеспечение, способное закачиваться и запускаться на устройствах пользователей без их согласия, что может приводить к блокировке или уничтожению данных на устройстве, краже личной информации или обхода системы защиты. К вредоносному ПО относятся компьютерные вирусы, троянцы, шифраторы (программы-вымогатели), шпионское и рекламное ПО, ботнеты. [1]

3) *DDoS-атаки* – это хакерские атаки на серверы, направленные на «добивание» систем веб-сайтов приложений путём подачи большого количества запросов, превышающих пропускную способность сети, что приводит к блокировке работы, порче или замедлению работы сайтов. Потенциальными целями DDoS-атак являются финансовые и государственные учреждения, сайты СМИ и электронной коммерции, сайты компаний, коммерческих некоммерческих организаций, то есть представители практически всех отраслей. [2]

4) *Внутренние угрозы* – угрозы со стороны работников, которые могут нечаянно или намеренно украсть или передать конфиденциальную информацию, либо нежелательно взаимодействовать с информационными системами.

5) *Социальная инженерия* – это процесс манипуляции людьми, чтобы получить доступ к их личной информации (фотографиям, датам рождения, логинам, паролям и т.д.). Социальная инженерия часто используется вместе с другими методами атак, например, фишингом, чтобы похитить личные данные человека или взломом пароля, чтобы получить доступ к компьютерной системе. Цель социальной инженерии – не проникнуть в систему напрямую, а заставить человека дать доступ к ней или совершить непреднамеренную ошибку.

6) *Спам* (*«мусор»*) – это массовые неадресные рассылки со всевозможным сомнительным содержанием и рекламой, которые распространяются через электронную почту. Такие рассылки могут являться каналом для внедрения вирусных программ, способных разрушать операционную систему, блокировать и уничтожать файлы на компьютере пользователя.

7) *Рутkит* (*Rootkit*) – это программа или набор программ, которые используют технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр.) посредством обхода механизмов системы. [1]

И другие.

К тенденциям, которые могут способствовать возникновению угроз кибербезопасности в 2023 и в последующие годы, можно отнести:

1) *Использование искусственного интеллекта* (*AI*) *и машинного обучения* для улучшения атак киберпреступников. Многие вредоносные программы в настоящее время используют AI и машинное обучение для адаптации к контрмерам и повышения своей эффективности. Предполагается, что в 2023 году использование AI-технологий и машинного обучения в кибератаках станет ещё более распространённым.

2) *Атаки на Интернет вещей* (*IoT*). С увеличением числа устройств, связанных с Интернетом, предполагается, что киберпреступники будут всё чаще направлять свои атаки на IoT-устройства, такие как умные дома, умные термостаты и т.п., которые могут быть менее защищены.

3) *Распространение вредоносных программ через облачные технологии*. Облачные сервисы становятся всё более популярными, и эта тенденция, вероятно, будет продолжаться. И следовательно будут обнаружены новые уязвимости в облачных сервисах, которые будут использоваться для распространения вредоносных программ.

4) *Атаки на квантовые системы*. Квантовые системы вычислений, которые находятся в разработке, могут представлять новые возможности для киберпреступников. Они смогут использовать квантовые вычисления для расшифровки данных и для создания новых методов перехвата и кражи конфиденциальной информации.

Это лишь несколько возможных угроз, которые уже являются или могут быть актуальны, начиная с 2023 года. Поэтому нельзя забывать, что электронная безопасность является непрерывным процессом, и предотвращение любой угрозы зависит от усилий и бдительности как самих пользователей, так и компаний, занимающихся разработкой программного обеспечения и систем безопасности.

Кибербезопасность – это практика использования технологических средств и процессов для защиты электронных систем, сетей, данных и

программного обеспечения от несанкционированного доступа, использования, изменения, утечки, нарушений конфиденциальности, кражи и уничтожения. Особенно важна кибербезопасность в связи с увеличением онлайн-угроз, виды которых были рассмотрены выше. Цель кибербезопасности – обеспечить безопасное использование интернета и электронных информационных систем.

Современные методы защиты от кибератак включают использование различных программных и аппаратных средств. Это могут быть антивирусные программы, межсетевые экраны (или брандмауэры), системы обнаружения вторжений, шифрование данных, периодическое обновление программного обеспечения для исключения уязвимостей, создание сложных паролей и регулярная их смена, резервное копирование данных, использование двухфакторной аутентификации, защиты от DDoS-атак и других видов атак, а также другие технические решения. Однако, помимо технических способов защиты, важно соблюдать правила безопасного поведения в сети, в частности, обучать пользователей правилам безопасности при работе в Интернете (например, не следует открывать подозрительные письма и ссылки и т.п.).

Для эффективного обеспечения кибербезопасности необходимо учитывать особенности различных видов угроз и выбирать соответствующие меры защиты. Например, для защиты от фишинга и социальной инженерии важно обучать пользователей определять подобные атаки и не давать злоумышленникам доступ к личным данным. Также важно учитывать возможность утечки данных из-за ошибок в работе сетевых систем и человеческого фактора. Для этого необходимо регулярно проводить аудит безопасности и обучать персонал правильному использованию технических средств защиты.

В целом, обеспечение кибербезопасности является сложной и многогранной задачей, требующей постоянного мониторинга и анализа угроз, актуализации мер защиты и обучения пользователей правилам безопасного поведения в Интернете.

Литература

1. Ковалькова, И.А., Лабкович, О.Н. Киберугрозы, с которыми сталкиваются пользователи сети. / Информационные технологии в политических, социально-экономических и технических системах [Электронный ресурс] : материалы научно-практической конференции, 22 апреля 2022 года / Белорусский национальный технический университет, Факультет технологий управления и гуманитаризации; редкол.: Г. М.

Бровка (пред. редкол.) [и др.] ; сост. А. В. Садовская. – Минск : БНТУ, 2022. – С. 267-270.

2. DDoS-атаки: нападение и защита. // [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/ruvds/articles/321992/.

УДК 004.056.5

КРИПТОВАЛЮТЫ

Ковалькова И.А.
Белорусский национальный технический университет

Криптовалюта – это один из видов цифровой валюты, электронных денег. В отличие от традиционных систем, где все данные хранятся на централизованном сервере, криптовалюты децентрализованы. Все криптовалюты основаны на криптографии: надёжных механизмах шифрования. Взломать такую систему практически невозможно. Стоимость той или иной криптовалюты определяется спросом и предложением на рынке.

Криптовалюта храниться в *криптовалютных кошельках* – программах, позволяющих отправлять и получать криптовалюту. Кошельки используются для хранения *секретных ключей* – шестнадцатеричных кодов, известных только владельцу и кошельку. Криптовалютные кошельки бывают разными – либо устройством, подключаемым к Интернету только для выполнения транзакций (в остальное время его можно хранить хоть в банковском сейфе), либо листом бумаги с напечатанным на нём ключом (один из вариантов «холодного хранилища»).

Список видов криптовалют обширен. Наибольшее распространение получили следующие виды криптовалют: *Bitcoin* (первая, наиболее популярная и дорогая криптовалюта, имеет неофициальный статус «криптозолота», появилась в 2009 г); *Namecoin* (выпущен в апреле 2011 года по исходному коду Биткоина, максимальный лимит монет которого составляет 21 млн. штук); *Ethereum* (вторая по популярности цифровая валюта, выпущенная в 2015 году, количество монет которой составляет около 100 миллионов); *Litecoin* (также является форком Биткоина, по объёмам капитализации входит в четвёрку лидеров мировых криптографических валют).

Преимущества криптовалют: анонимность сведений о владельце, прозрачность всех операций; минимальные комиссии за совершение операций; строго установленный эмиссионный максимум; информация о