Литература

1. VBA в Excel: объясняем главные понятия и принципы работы https://skillbox.ru/media/management/vba-v-excel-obyasnyaem-glavnye-ponyatiya-i-printsipy-raboty [Дата доступа: 25.10.2024]
2. Начало работы с VBA в Office https://learn.microsoft.com/ru-ru/office/vba/library-reference/concepts/getting-started-with-vba-in-office [Дата доступа: 25.10.2024].
3. Работа между приложениями https://learn.microsoft.com/ru-ru/office/vba/language/concepts/getting-started/working-across-applications [Дата доступа: 25.10.2024].
4. Безопасность Microsoft Office: макросы VBA https://habr.com/ru/companies/dsec/articles/353800/ [Дата доступа: 27.10.2024].
5. Искусственный интеллект в программировании https://rep.bntu.by/handle/data/126785 [Дата доступа: 27.10.2024].

КИБЕРБЕЗОПАСНОСТЬ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

Ширяева А.Д.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

В настоящее время информация стала неотъемлемым ресурсом и вопрос о её безопасности становиться наиболее актуальным. Поэтому кибербезопасность и информационная безопасность компьютерных сетей стали приоритетными аспектами по защите данных, предотвращения угроз безопасности, обеспечения стабильной работы организаций и пользователей. С тех пор как информационные технологии стали более усовершенствованными и увеличилось количество подключённых устройств, угроза безопасности стала более высокой. Разные частные компании и государственные учреждения сталкиваются с большим количеством рисков, начиная от компьютерных вирусов и заканчивая кибершпионажем. Потери, вызванные киберпреступностью, могут быть критическими и включать утечку конфиденциальных данных, нанесение финансового ущерба, нарушение работы чрезвычайно важных систем.

Кибербезопасность и информационная безопасность играют важнейшую роль в защите цифровой информации и компьютерных сетей. Эти два понятия связаны между собой, но имеют отличия. *Кибербезопасность* занимается защитой цифровых систем и инфраструктуры от незаконного доступа, кибератак и взломов. В её задачу входит предотвращение угроз, таких как хакерские атаки, троянские программы и распространение вредоносного программного обеспечения (ПО). *Информационная безопасность* – это обеспечение защиты во всех

формах – от цифровых данных до данных на бумажном носителе – с целью предотвращения утечек и обеспечения конфиденциальности информации.

Основное различие между этими двумя понятиями в том, что кибербезопасность больше ориентирована на защиту инфраструктуры и сетей, а информационная безопасность – на сохранность данных. Но в наши дни эти два понятия пересекаются между собой, так как основная часть данных хранится и передаётся через компьютерные сети. В процессе растущей цифровизации границы между кибербезопасностью и информационной безопасностью становятся все более расплывчатыми.

Современные методы защиты от кибератак включают использование различных программных и аппаратных средств. Ими могут быть антивирусные программы, межсетевые экраны (или брандмауэры), системы обнаружения вторжений, шифрование данных, периодическое обновление ПО для исключения уязвимостей систем, создание сложных паролей и регулярная их смена, резервное копирование данных. [1, с. 1].

Современные компьютерные сети подвергаются множеству угроз, которые становятся всё более изощрёнными и разрушительными. Одной из наиболее распространённых из подобных угроз является вредоносное ПО (malware), включающее вирусы, черви, трояны и программы-вымогатели (ransomware). Эти программы проникают в информационные системы с целью их повреждения, шпионажа или блокировки данных, при этом требуя выкуп за их восстановление. Например, атаки программ-вымогателей могут парализовать работу целых организаций, вынуждая их либо платить немалые суммы хакерам, либо сталкиваться с существенной потерей данных.

Фишинг – это атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). [2, с. 1]. При этом злоумышленники отправляют ложные электронные письма, чтобы ввести в заблуждение пользователей, а потом обманным путём получают доступ к их личным данным. Каким бы не был подготовленным пользователь, но хакеру достаточно одного телефонного звонка и одного вопроса, чтобы все ваши деньги или важная информация оказались уже в его владении. Подобные фишинговые атаки часто направлены на сотрудников компаний и могут привести к появлению компрометирующей информации и утечке финансовых данных.

DDoS-атаки (распределённые атаки на отказ в обслуживании) направлены на перегрузку сетей и серверов путём одновременной отправки множества запросов. В этом случае, злоумышленники используют множество заражённых устройств для одновременной отправки большого количества запросов к целевому серверу. [3, с.1]. Это приводит к отказу в работе серверов и может значительно нарушить бизнес-процессы компаний или доступ к web-сайтам. Хакеры довольно часто используют такого вида атаки для шантажа или создания беспорядка.

Ещё одной немаловажной угрозой является утечка данных, когда секретная информация становится доступной для третьих лиц. Это может произойти по различным причинам, например в результате хакерской атаки или по вине самих сотрудников компаний. Подобные утечки данных являются серьёзной проблемой, так как наносят существенный вред репутации организации (или компании) и приводят к крупным финансовым проблемам. Например, утечка личных данных клиентов какой-либо компании может стать причиной штрафов и потерей доверия потребителей к ней.

Известны разные варианты обеспечения безопасности компьютерных сетей, где сочетаются как технические так и организационные меры. К сожалению, абсолютно защищённых систем не существует, но вероятность их защиты всё равно есть. Одним из важных способов защиты являются антивирусные программы и программные комплексы, которые помогают вовремя выявлять и устранять вредоносные программы, не допуская заражения системы и утечку данных.

Шифрование также играет важную роль в защите данных. Оно обеспечивает конфиденциальность, преобразуя данные в зашифрованный вид, который доступен только для авторизованных пользователей, имеющих соответствующий ключ.

Обучение пользователей и постоянное информирование их является важным аспектов в сфере безопасности. Даже самые сложные технические системы могут оказаться уязвимыми из-за человеческого фактора, например, из-за фишинговых атак или использования слабых паролей.

Ещё одним важным элементом в деле защиты информации является облачная безопасность. Облачная безопасность – это набор политик, средств контроля и технологий для защиты данных, приложений и инфраструктурных сервисов. Все эти компоненты работают вместе, помогая обеспечить безопасность данных, инфраструктуры и приложений. Эти меры безопасности защищают среду облачных вычислений от внешних и внутренних угроз и уязвимостей кибербезопасности. [4, с.1]

Обеспечение информационной безопасности невозможно без нормативно-правовой базы, которая устанавливает правила и стандарты для защиты данных и инфраструктуры. Государства и международные организации разрабатывают законодательные акты и стандарты, чтобы регулировать использование и защиту информации в различных сферах.

На уровне государств существуют важные законы и нормативные акты, которые регулируют информационную безопасность.

Важным элементом правового регулирования является разработка и реализация политик информационной безопасности внутри организаций. Компании создают внутренние регламенты, описывающие меры по защите данных, разграничение прав доступа и порядок реагирования на инциденты. Такие политики по-

могают стандартизировать процессы защиты информации и минимизировать риски.

Нормативно-правовое регулирование и международные стандарты способствуют созданию безопасной среды для работы с информацией, задавая рамки и стимулируя компании к внедрению надёжных систем защиты. Нужно отметить, что безопасность – это не статичный процесс, а постоянная работа, включающая мониторинг и адаптацию к новым вызовам.

Таким образом, кибербезопасность и информационная безопасность – это не просто задача специалистов по защите, а ответственность на всех уровнях, от частных пользователей до государственных органов. Только при слаженной работе всех участников можно противостоять современным киберугрозам и обеспечить надёжную защиту данных в цифровом пространстве.

Литература

1. Обеспечение кибербезопасности в современных [Электронный ре-сурс]. – Режим доступа: https://rep.bntu.by/bitstream/handle/data/130299/260-264.pdf?sequence=1&isAllowed=y. – Дата доступа: 24.10.2024

2. Что такое кибербезопасность? [Электронный ресурс]. – Режим до-ступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security – Дата доступа: 25.10.2024

3. Киберугрозы и атаки: виды и методы защиты [Электронный ре-сурс]. – Режим доступа: https://sky.pro/wiki/profession/kiberugrozy-i-ataki-vidy-i-metody-zashity/ – Дата доступа: 26.10.2024

4. Что такое облачная безопасность? [Электронный ресурс]. – Режим доступа:https://www.oracle.com/cis/security/cloud-security/what-is-cloud-security/– Дата доступа: 30.10.2024

КРИПТОГРАФИЯ КАК НАУКА. ТИПЫ КРИПТОСИСТЕМ

Синяк У.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Повседневная жизнь человека неразрывно связана с информацией, с процессами её обработки, хранения и дальнейшей передачи. А вопросы информационной безопасности и сокрытия информации остаются одними из наиболее горячей темой в быстроразвивающемся мире.

Криптография, что в переводе с греческого означает «тайное письмо», появилась ещё с момента возникновения первой письменности на земле. С необходимостью передавать информацию возникла и необходимость скрывать её от лишних глаз. Люди хотели, чтобы информация могла передаваться привычным и