Угрозы кибербезопасности и актуальные методы защиты информационных систем

Аннотация. В статье рассматриваются актуальные проблемы кибербезопасности. Анализируются наиболее распространённые кибератаки: фишинг, распространение вредоносного ПО, использование уязвимостей в программном обеспечении, социальная инженерия и внутренние утечки данных. Перечислены основные рекомендации для защиты информационной структуры учреждений на основе анализа писем ФСТЭК России.

В современном мире цифровые технологии всё больше проникают в различные сферы жизни, от личных данных до критически важных систем. Вместе с этим увеличивается и количество рисков в области кибербезопасности, таких как кибератаки, утечки информации и вредоносные программы.

С 2023 года Федеральная служба по техническому и экспортному контролю России осуществляет рассылку писем в государственные учреждения с информацией о выявленных компьютерных угрозах и способах их устранения. В основном в этих письмах рассматриваются угрозы, связанные с программными уязвимостями, деятельностью хакерских группировок, а также даны рекомендации по защите информационной инфраструктуры.

Кибератака - это серия вредоносных действий, которые злоумышленник совершает в цифровом пространстве с целью нарушить конфиденциальность или целостность данных, а также получить несанкционированный доступ к информационным и коммерческим системам или компьютерным сетям.

Среди наиболее распространённых и актуальных в настоящее время кибератак можно выделить фишинг, распространение вредоносного программного обеспечения, использование уязвимостей в программном обеспечении, социальную инженерию и внутренние утечки данных.

Фишинг — это вид интернет-мошенничества, направленный на получение конфиденциальной информации пользователей, такой как логины, пароли, номера кредитных карт и другие данные, а также на установку вредоносного программного обеспечения на компьютере пользователя.

Этот вид интернет-мошенничества основан на использовании психологических уловок, распространении поддельных сообщений от имени известных организаций и внедрении вредоносного программного обеспечения.

Социальная инженерия — это метод манипуляции людьми с целью получения конфиденциальной информации, доступа к ресурсам или другим ценным объектам.

Социальные инженеры разрабатывают схемы мошенничества, используя глубокое понимание психологии человеческого поведения.

Подготовка. На этом этапе злоумышленники собирают информацию о жертве или группе, к которой она принадлежит.

Установление контакта и завоевание доверия.

Использование уязвимостей. Злоумышленники находят и используют слабые места жертвы для достижения своих целей.

Завершение. После достижения желаемого результата злоумышленники прекращают общение с жертвой, чтобы избежать обнаружения.

Весь процесс может длиться от нескольких месяцев до нескольких дней и включать в себя множество этапов коммуникации.

Вредоносное программное обеспечение скачивается на компьютер при переходе по неизвестным ссылкам или через рассылку писем. Эти программы могут маскироваться под что угодно: от PDF-файлов до игр и пиратского программного обеспечения. Автоматически устанавливаются на компьютер и предоставляют

злоумышленникам возможность несанкционированно и дистанционно управлять зараженным устройством (троянские программы) и «маскировать» другие вредоносные программы для антивирусов (руткиты), также могут повреждать и удалять важные файлы (вирусы) или записывать все нажатия клавиш на клавиатуре зараженного компьютера (кейлоггеры).

Уязвимости в используемом программном обеспечении.

Это ошибки, допущенные программистами на этапе разработки программного обеспечения. Они позволяют злоумышленникам получить незаконный доступ к функциям программы, хранящимся в ней данным или передать вредоносное программное обеспечение.

Этой проблемой занимаются этичные хакеры («белые» хакеры). Они моделируют взломы систем безопасности, проводят тесты на уязвимости и придумывают новые способы проверки.

На основе таких проверок ФСТЭК России ведёт Банк данных угроз (БДУ), в котором перечислены все выявленные угрозы. На данный момент выявлено более 60 тысяч программных уязвимостей.

Утечки данных из-за ошибок или небрежности сотрудников – это непреднамеренное распространение важной информации сотрудниками организации: пересылка с корпоративной почты на личный электронный адрес списка сотрудников или студентов, скачивание вирусов и вредоносных программ из фишинг-писем, хранение или пересылка паролей в мессенджерах и т.д.

Это является одной из наиболее важных проблем кибербезопасности. Несмотря на все средства защиты информации, человеческий фактор остаётся самым слабым звеном.

Анализ писем от ФСТЭК России позволил выделить основные рекомендации для защиты информационной структуры учреждений:

- мониторинг информационной системы на наличие вирусов и вредоносного программного обеспечения;
- фильтрация доступных ресурсов по «чёрным» и «белым» спискам;
- проведение обучения сотрудников и студентов основам информационной безопасности;
- минимизация прав пользователей информационной системы учреждения;
- удаление неиспользуемых учётных записей пользователей из системы;
- регулярное обновление программного обеспечения;
- использование антивирусов;
- проверка всех входящих и загружаемых файлов;
- удаление сохранённых данных (логины, пароли, данные банковских карт) из браузеров;
- установка двухфакторной защиты аккаунтов (подтверждение входа через СМС или генерация кодов доступа);
- минимальное использование приложений для удалённого доступа (AnyDesk, Chrome Remote, VNC и др.);
- подготовка плана реагирования на компьютерные инциденты.

Очевидно, что успех кибератак зависит от уязвимости информационно-технологической инфраструктуры учреждения.

В условиях стремительного развития цифровых технологий кибербезопасность становится критически важной областью. Для обеспечения надежной защиты информации необходимо применять комплексный подход, включающий мониторинг сетевой активности, обновление используемого программного обеспечения, фильтрацию трафика и обучение сотрудников основам информационной безопасности.

Важность постоянного обновления защитных мер невозможно переоценить, так как цифровые угрозы постоянно эволюционируют. Только непрерывное

совершенствование методов защиты и адаптация к новым угрозам могут обеспечить надежную защиту информации и устойчивость к кибератакам в эпоху цифровизации.