УДК 681.3.06

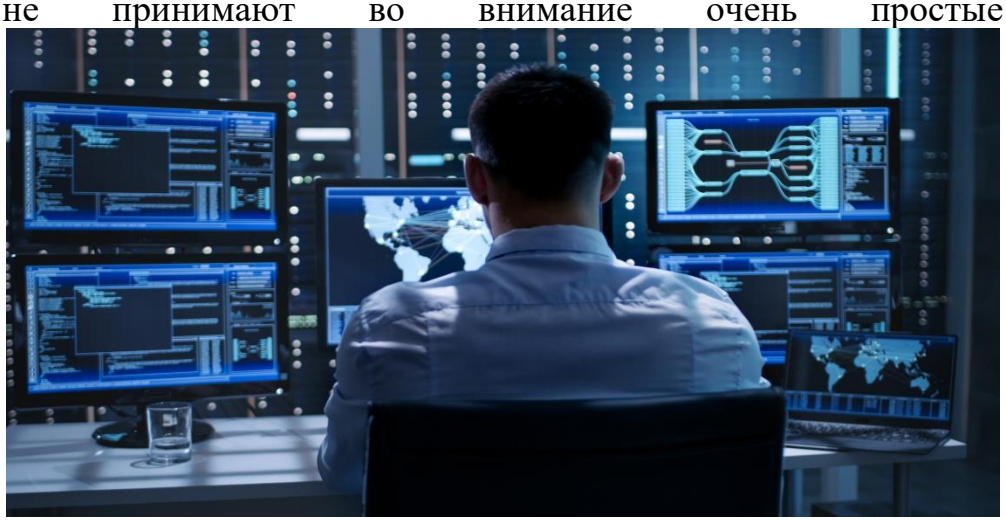
Гавриленков Е. А. студентХОб-201,
Янина Т.И. к.т.н., доцент,
Гумённый А.С. к.т.н., доцент
Кузбасский государственный технический университет имени Т.Ф. Горбачева

Gavrilenkov E.A. student HOB-201,
Yanina T.I. Ph.D., associate professor,
Gumienny A.S. Ph.D., associate professor
T.F. Gorbachev Kuzbass State Technical University

О ПРОБЛЕММАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ABOUT THE PROBLEMS OF INFORMATION SECURITY

На ряду, с проблемами безопасности технологических процессов на предприятиях остро стоит вопрос кибербезопасности. Ежегодно в мире происходит миллиарды киберпреступлений, будь то кибератака ради получения выгоды или целый кибертерроризм с целью захвата целой компьютерной сети. С каждым годом этих преступлений становится только больше. Накоплен огромный практический опыт работы в интернете, в локальных с компьютерных сетях, но число преступлений такого рода только растет. Это связано с тем, что многие люди, даже те, кто хорошо разбирается в сфере компьютеров и интернета, не знают, игнорируют или не принимают во внимание очень простые правила.



Компьютерная безопасность или кибербезопасность – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

Говоря о статистике, она шокирует: за первые 9 месяцев 2019 года было зафиксировано около 8 миллиардов случаев утечки данных, эти цифры превышают показатели за тот же период 2018 года более чем в 2 раза (на 112%) [1].

В основном целью злоумышленников являются медицинские и государственные учреждения, а также организации из сферы розничной торговли. Причина – действия преступников. Некоторые организации привлекают злоумышленников финансовыми или медицинскими данными, на некоторые организации «налетают» с целью охоты на данные клиента, чтобы шпионить или готовить атаку на одного из клиентов.

Кибербезопасность борется с тремя видами угроз:

- Киберпреступление – действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду;
- Кибератака – действия, нацеленные на сбор информации, в основном политического характера;
- Кибертерроризм – действия, направленные на дестабилизацию электронных систем или панику [2].

Чем же пользуются злоумышленники? – Это вредоносное программное обеспечение (ПО), то есть, то программное обеспечение, которое наносит вред. Все логично. Оно может быть самым разнообразным, но вот самые распространенные из них:

- Вирусы – программы, заражающие файлы вредоносным кодом;
- Троянцы (Trojan) – вредоносы, которые прячутся под маской легального ПО;
- Шпионское ПО – программы, следящие в тайне за действиями пользователя и собирающие информацию (к примеру, данные кредитных карт);
- Программы-вымогатели (популярный – winlocker) – программы, блокирующие или шифрующие доступ к файлам и данным. Затем преступники требуют выкуп за восстановление, утверждая, что пользователь рискует потерять свои данные;
- Рекламное ПО – программы рекламного характера, которые могут распространять вредоносное ПО;

Помимо вредоносного ПО преступники также пользуются и другими методами взлома и обмана, один из таких – Фишинг.

Фишинг – атаки, цель которых обманом заполучить конфиденциальную информацию пользователя. Часто преступники в ходе таких атак представляются официальной организаций и отправляют соответствующие письма на почту.

Разобрав способы взлома и обмана, стоит также разобраться в том, как же защититься от злоумышленников? Способов защиты огромное количество, на разных устройствах используются разные методы защиты. Профессионалы в области кибербезопасности ищут и анализируют новые угрозы, а затем разрабатывают способы борьбы с ними. Важно научить сотрудников пользоваться защитным ПО. Чтобы защитные средства эффективно выполняли свои функции, они должны быть во включенном состоянии и постоянно обновляться.

Самые популярные и эффективные способах защиты:

- **Постоянное обновление ПО и ОС.** Используя новое ПО, вы получаете также и свежие исправления безопасности;
- **Антивирусные программы.** Защитные решения, коих огромное количество, могут выявить и устранить угрозы, одни из самых надежных и популярных антивирусов: Dr.Web, Avast, KasperskyInternetSecurity, EsetNod 3. Для максимальной защиты стоит регулярно обновлять программное обеспечение, то есть антивирусные программы;
- **Использование надежных паролей.** Не стоит использовать в качестве паролей комбинации, которые популярные или легко подобрать, или угадать. Стоит также регулярно менять свой пароль;
- **Не стоит открывать почтовые вложения, полученные от неизвестных отправителей –** Они могут быть заражены вредоносным ПО;
- **Не стоит переходить по ссылкам, полученным по почте от неизвестных отправителей –** Также один из стандартных и популярных путей распространения вредоносного ПО;
- **Избегание незащищенных сетей Wi-Fi.**

Многие компании и предприятия ежедневно подвергаются атакам злоумышленников с целью заполучить данные компании, дабы всячески навредить ей. Что же предпринимают предприятия для защиты своих данных?

Чтобы обезопасить свои данные, многие компании связывают свои ПК единой локальной сетью без выхода в интернет для обычных рабочих и с неполным доступом для руководителей подразделений. Чтобы безопасность данных была еще на более высоком уровне, для каждого работника создают отдельный аккаунт с определенным сложным паролем, который должен регулярно меняться либо самим пользователем, либо системой, чтобы доступ к сети был максимально ограничен. Также на многих предприятиях и компаниях вводят свои правила пользованием ПК:

- Запрет на какие-либо сторонние цифровые носители (флешки, диски и другие носители памяти);

- Запрет на скачивание и установку нового софта (для этого на все компьютеры ставят админ-пароль, который знают только управляющие компанией люди);
- Запрет на скачивание и открытие неизвестных и/или вредоносных файлов.

Для еще большей безопасности на предприятии рекомендуется использовать только лицензионные софты, дабы обезопасить ПК от вирусов и других вредоносных ПО.

Урон, причиненный предприятию, может быть абсолютно разным. Например, может произойти утечка файлов по вине одного из сотрудников, но системные администраторы очень быстро решили проблему и утечка не произошла. Но кибератаки могут быть и настолько серьезными и мощными, что системные администраторы не смогут решить проблему и все данные и финансы предприятия уйдут к злоумышленникам, таким образом, сделав это предприятие банкротом. То есть от того, какой урон был причинен компании, напрямую зависит будущее этой компании.

На предприятиях постоянно происходят какие-то сбои, неполадки, которые также могут повлечь за собой непоправимый урон для компании. Даже, например, от какой-то простой попытки взлома локальной сети в компании может произойти сбой и вывести из строя все производство не на один час, а может и не на один день, что уже повлечет за собой последствия, которые могут оказаться непоправимыми.

Подводя итог, стоит сказать, что в компьютерных системах и интернете стоит быть максимально внимательным и допуск посторонних лиц к служебным компьютерным системам строго запрещен.

Список литературы

1.https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security.

2. https://ru.wikipedia.org/wiki/Компьютерная_безопасность.

3.https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html#~types-of-threats.

References

1.https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security.

2.https: //ru.wikipedia.org/wiki/Computer_Security.

3.https://www.cisco.com/c/en_ru/products/security/what-is-cybersecurity.html#~types-of-threats.