УДК 378.147:614.841.41

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

Попов Роман Сергеевич
студент
Криволапов Иван Павлович
кандидат технических наук, доцент
ivan0068@bk.ru
Чечевицын Иван Дмитриевич
студент
Щербаков Сергей Юрьевич
кандидат технических наук, доцент
scherbakov78@yandex.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. В статье пречислены причины утчеки информации и её последствия.

Ключевые слова: безопасность информации, информационная безопасность, ИБ, утечка информации.

Информационная безопасность — это не только защита данных сотрудников и клиентов в организации, это так же защита данных самой организации от распространения или иных способ нанесения материального или финансового ущерба.

Информационная безопасность организации это комплекс различных мероприятий, направленных прекращение несанкционированного доступа к базе данных компании, завладение конфиденциальной информации и изменения самой базы данных. Зная важность информации как ресурса в современном мире, утечка информации может привести к огромным ущербам [1].

Утечка информации может оказать различные эффекты на организацию и её невозможно спрогнозировать заранее. Результаты утечки может быть незначителен, а может привести организацию к неспособности заниматься хозяйственными делами [2, 3].

Коммерческая и конфиденциальная информация существовала и раньше, но с появлением и развитием электронных средств повышается вероятность утечки или кражи данных. В сравнение: если раньше для получения какой-либо информации необходимо было физическое воздействие, то с появлением ЭВМ такая необходимость попросту не нужна, сейчас необходимо получить доступ к базе данных, через взлом или какого-либо иного способа обхода безопасности [1, 4].

Основными видами данными для кражи являются:

- Данные работников организации
- Различные разработки научно-технических отделов
- Финансовое состояние организации
- Данные для доступа в более защищённые сервера

Также не стоит забывать, что украденные данные могут оказать на организацию эффект не сразу, а по прошествии какого-то промежутка времени. Именно поэтому данные не делятся на виды, а размещается в IT-инфраструктуре компании и храниться в архивах при этом данные не должны выходить за её пределы.

Существует множество угроз ИБ организации [4, 5].

Одной из причин утечки информации являются сами сотрудники.

Их можно разделить на несколько категорий:

- Нарушители. Это сотрудники что не обращают на протоколы безопасности и часто без ведомого вышестоящих запускают сторонние программы на рабочих ЭВМ. Такие действия часто приводят к появлению вредоносных программ, которые не только могут повредить базу данных, но и к утечке информации к злоумышленникам.

- Правонарушители. Это сотрудники, имеющие доступ к засекреченным данным организации и целенаправленно передают данные для вознаграждения или по другим причинам.

- Шпионы. Это сотрудники, которые нанимаются в организацию, с целью кражи данных. Чаще всего являются специалистами, способными обойти часть защиты и убрать признаки присутствия в системе постороннего, что усложняет попытку обнаружения нарушителя.

- Уволенные сотрудники. Это сотрудники, которые были уволены из организации по инициативе работодателя и смогли унести с собой часть информации, после чего распространяют или продают конкурентам для отмщения за причиненный ущерб [4, 6, 7].

Также причиной утечки может послужить халатное отношение сотрудников к защите, например, хранение конфиденциальной информации на сменных накопителях, использования обычной электронной почты для передачи данных и переход по неподтверждённым ссылкам что к приводит к заражению всей корпоративной сети.

Использование нелицензионных программ из-за экономии руководства средств на ПО. Такие программы внедряют в сеть вирус или же ухудшают защиту организации, что приводит к облегчению работы для злоумышленников [2, 5, 7].

Distributed-Denial-of-Service или же DDoS-атака так один из способов нанесения ущерба компании. DDoS-атака это массовое отправка запросов от

пользователей зараженных специальной программы, такая атака может привести к падению сервера организации что сильно ударит по лояльности её клиентов. Зачастую DDoS-атака использует не только для нанесения вреда имиджу компании, а скорее, как для отвлечения, пока сотрудники отвлечены на DDoS-атака, конкуренты занимаются кражей средств или важных данных, также DDoS-атака используется как способ шантажа [6].

Действия правоохранительных органов. При расследовании уголовных дел, сотрудники правоохранительных органов часто изымают технику и документы организации, что может привести к остановке или же полностью прекратить деятельность организации [4].

Средства и методы защиты конфиденциальных данных от кражи или изменения существует множество. Основными из них являются:

Физическая защита данных при помощи, которой в организации появляются ограничения на доступ лишь конкретных доверенных лиц к местам где храниться информация. Используется удаленное управление СКУД (Система контроля и управления доступом).

Общие средства защиты. Сотрудники должны пользоваться определенными утилитами и приложениями во время работы в сети. К ним можно отнести фильтры сообщений почты, антивирусные программы, а также система логинов и паролей с периодической сменной во избегание утечки.

Для защиты от DDoS-атак часто используют утилиты блокирующие сторонний трафик и сохраняет доступ для легальных пользователей.

Резервные копии информации при помощи удаленных носителей или «облачного» хранилища.

Восстановление работы после вмешательства, а точнее заранее продуманный план по ликвидации последствий, оказанных на сеть организации.

Передача зашифрованных данных при помощи утилит позволит также безопасно предать информацию без возможности её утечки даже при перехвате данных.

Меры по обеспечению информационной безопасности на предприятии должны разрабатываться и реализовываться постоянно, независимо от роли IT-инфраструктуры в производственных процессах.

К решению этого вопроса необходимо подходить комплексно и с привлечением сторонних специалистов. Только такой подход позволит предотвратить утечку данных, а не бороться с ее последствиями [3].

Список литературы:

1. Информационная безопасность предприятий [Электронный ресурс] режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-predpriyatij/
2. О проблеме изъятия электронных носителей информации в рамках следственных действий Электронный ресурс] режим доступа: https://www.advgazeta.ru/mneniya/o-probleme-izyatiya-elektronnykh-nositeley-informatsii-v-ramkakh-sledstvennykh-deystviy/
3. DDoS-атаки: нападение и защита Электронный ресурс] режим доступа: https://habr.com/ru/company/ruvds/blog/321992/
4. Сравнительный анализ существующих подходов к оценке травмоопасности / С.Ю. Щербаков, И.П. Криволапов, С.А. Петрушенко, А.П. Коробельников // Наука и Образование. – 2019. – Т. 2. – № 4. – С. 252.
5. Щербаков, С.Ю. Исследование опасных факторов производственной среды и факторов риска травмирования / С.Ю. Щербаков, А.А. Фокин, А.А. Заборских // Наука и Образование. – 2020. – Т. 3. – № 2. – С. 58.
6. Щербаков, С.Ю. Основные принципы математического моделирования в техносферной безопасности / С.Ю. Щербаков, А.А. Фокин, А.А. Заборских // Наука и Образование. – 2020. – Т. 3. – № 2. – С. 59.
7. Утечка конфиденциальной информации Электронный ресурс] режим доступа: https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/prichiny-

utechki-informatsii/istochniki-utechki-informacii/utechka-konfidencialnoj-informacii/

UDC 378.147:614.841.41

INFORMATION SECURITY IN THE ORGANIZATION.

Popov Roman Sergeevich
student
Krivolapov Ivan Pavlovich
Candidate of Technical Sciences, Associate Professor
ivan0068@bk.ru
Chechevitsyn Ivan Dmitrievich
student
Shcherbakov Sergey Yurievich
Candidate of Technical Sciences, Associate Professor
scherbakov78@yandex.ru
Michurinsk State Agrarian University
Michurinsk, Russia

Annotation. The article lists the causes of information leakage and its consequences.

Key words: Information security, information security, is, information leakage.