
В современном мире развитие всех организаций все больше зависит от информационных систем. Однако несмотря на это многие обеспокоены сохранением своей информации в информационных системах, особенно личными данными. Этому есть причина: угроза со стороны хакеров (киберприступников), совершающих кражи личных данных с последующей их продажей. В настоящее время количество хакеров постоянно растет во всем мире. Причиной роста является огромная финансовая составляющая. Несмотря на то, что информация – не материальная вещь, она является самым ценным и высокооплачиваемым активом. Из-за этого многие организации идентифицируют свою информацию как одну из важнейших операций, которую нужно защитить любым образом. Обычно любое предприятие проводит организационные и индивидуальные записи, например, в ИТ-системах организация может хранить конфиденциальную информацию о своих сотрудниках, зарплату, финансовую отчетность, а также бизнес-планы на последующие года. Кроме того, организация также держит коммерческие тайны, исследования и другую информацию которая дает конкурентное превосходство для их компании. Большая часть информации собирается, обрабатывается и хранится на компьютерах, а также передается по сети от одного компьютера к другому. Попадая в чужие руки, данная информация может привести к потере бизнеса, судебным искам, краже личных данных.

Очень часто в заголовках новостей появляются статьи об украденных или недостающих данных. А так как многие организации все чаще полагаются на хранение данных в электронном виде - это становится действительно важной проблемой. Необходимость беспокоиться об информационной безопасности, заключается в том, что большая часть стоимости бизнеса сосредоточена на ценности его информации. Чтобы полностью осознать серьезность проблемы, все должны понимать, в чём заключается смысл информационной безопасности и каким образом она обеспечивается.

С точки зрения карьерного направления, появляется все больше областей, где необходимы профессионалы по обеспечению информационной безопасности. Так как направление новое, то знающих людей в этой области не много, что приводит к дефициту кадров, а, следовательно, к высоким зарплатам.

**Кибертерроризм**

Акты кибертерроризма могут осуществляться через частные компьютерные серверы, против устройств и сетей, видимых через публичный интернет, а также против защищенных государственных сетей или других ограниченных сетей. Хакеры, которые взламывают компьютерные системы, могут внедрять вирусы в уязвимые сети, портить веб-сайты и/или создавать террористические угрозы в электронном виде.

Примеры деятельности хакеров:

- Разрушение крупных веб-сайты для создания общественных неприятностей / неудобств или для остановки трафика, которые публикуют контент, с которым не согласны хакеры.
- Получение удаленного доступа к данным пользователей, отключение или перекрытие каналов связи для перехвата информации.
- Существуют направления, направленные против критически важных инфраструктурных систем (например, отключение систем электропитания, перехват стратегически важной информации города или страны). Такой вид кибератаки может нарушить работу крупных городов, вызвать кризис в любой из социальных областей, поставить под угрозу общественную безопасность миллионов людей, а также вызвать массовую панику и гибель людей. Однако надо понимать, что это совершенно иной уровень, предполагающие большой опыт, множество связей злоумышленников.

В качестве инструментов хакерами могут использоваться:

- Вирусы, компьютерные черви и вредоносные программы, нацеленные на системы контроля компьютеров и ИТ-систем.
- DoS-атаки, когда злоумышленники принимают меры для предотвращения доступа законных пользователей к целевым компьютерным системам, устройствам или другим сетевым ресурсам.
- Программа-вымогатель, которая держит компьютерные системы в заложниках, пока жертвы не выплатят требуемую сумму.
- Фишинговые атаки - направлены на сбор информации пользователей по электронной почте, которую они затем могут использовать для доступа к пользовательским системам и устройствам.

Ключом к борьбе с кибертерроризмом является предотвращение. Следовательно, лучшим способом предотвратить взлом - это установка надежных мер, такие как антивирусное программное обеспечение и их регулярное обновление. Это

предлагает базовую систему защиты от кибертеррористов. Также рекомендуется периодически выполнять полные и своевременные резервные копии своих систем.

## Заключение

В качестве заключения, информационная безопасность имеет важное значение для развития различных предприятий любой области. Развитие современных организаций зависит от доступности, конфиденциальности и целостности обеспечения информационной безопасности. Помимо этого, широкое использование информационных технологий повышает эффективность бизнеса, но подвергает организацию дополнительным рискам и вызовам, таким как непонимание информационной безопасности, проблем незащищенных беспроводных каналов, нехватка персонала по информационной безопасности и атак на информационную безопасность. Внедрение информационной безопасности-это процесс, который является гораздо более сложным, чем реализация других процессов из-за большого количества вероятностных факторов, которые могут повлиять на его эффективность. Для обеспечения информационной безопасности организация должна понимать, что информационная безопасность-это не только технологический вопрос. При разработке информационной безопасности организации следует также учитывать нетехнический аспект информационной безопасности. Кроме того, следует отметить, что реализация информационной безопасности в организации имеет возможность снизить риск возникновения кризиса в организации.

## Список литературы


1. Фридланд А.Я. Информатика и компьютерные технологии: Основные термины: Толков. Слов.: Более 1000 базовых понятий и терминов. – 3-е изд. испр. и доп./ А.Я. Фридланд, Л.С. Ханамирова, И.А. Фридланд. – М.: ООО «Издательство Астрель», 2003. – 272 с.
2. Доронин Андрей Михайлович Уголовная ответственность за неправомерный доступ к компьютерной информации : дис. ... канд. юрид. наук: 12.00.08. Москва, 2003.
3. Ястребов Дмитрий Андреевич Неправомерный доступ к компьютерной информации: уголовно-правовые и криминологические аспекты : дис. ... канд. юрид. наук: 12.00.08. Москва, 2005.

4. В. А. Копылов «Информационное право», издание второе, Москва 2004.
5. Лэнс, Дж. Фишинг: Техника компьютерных преступлений; НТ Пресс, 2008. — 320 с.