Чопанова Б.,

студент 2 курса

Ивановский государственный университет,
bossan.chopanova93@mail.ru

Информационная безопасность

Аннотация. В статье представлен обзор информационной безопасности, защищённость информации и поддерживающая информационную безопасность от любых случайных или злонамеренных воздействий.

Ключевые слова: информационная безопасность, информационные технологии, ущерб самой информации,угрозы информационной безопасноти.

Chopanova B.,
student,
The Ivanovo State University,
bossan.chopanova93@mail.ru

Information security

Annotation. The article provides an overview of information security, information security and supporting information security from any accidental or malicious influences.

Keywords:information security, damage to information itself, threats to information security.

Информационные технологии используются повсеместно, и многие уже не могут представить свою жизнь без них: социальные сети, мессенджеры, интернет-магазины,онлайн-банкинг — все эти средства связи и коммуникаций мы используем, и все эти точки доступа потенциально уязвимы. Именно поэтому информационная безопасность играет крайне важную роль в нашей жизни. С развитием технологий все сложнее становится защита личных данных.

Информационная безопасность — это всесторонняя защищённость информации и поддерживающей её инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий. Проблема защиты информации становится все более актуальной. В подавляющем большинстве современных компаний документооборот существует в электронном виде. Накоплен массив статистической, финансовой, маркетинговой

информации, сформирована клиентская база. Все эти данные находятся под угрозой взлома. Попробуем непредвзято разобраться в проблеме защиты конфиденциальной информации и в таком явлении, как хакерство. Что можно считать конфиденциальной информацией? В первую очередь, это данные, составляющие коммерческую тайну компании, затем личные дела сотрудников, и в третью очередь — сведения партнеров, подрядчиков, поставщиков, клиентов и т. п. Разглашение таких сведений может нанести серьезный ущерб интересам и репутации фирмы. В большинстве крупных и успешных запорожских компаний есть квалифицированные системные администраторы.

В современной капиталистической экономике существует конкуренция, а значит, и спрос на секретную информацию конкурентов — это реальность. Способов добычи такого рода информации существует великое множество, и хакерские атаки, пожалуй, выглядят почти невинными в сравнении с некоторыми другими.Слово «хакер», если коротко, именует особенный тип компьютерных специалистов, досконально знающих принципы работы компьютерных систем. Хакеры — это целая субкультура, со своим языком, этикой, эстетикой. Подавляющее большинство в этой среде исповедует радикально левые или анархические идеи и не признают право собственности на информацию, как и на воздух, землю и т. п. Правда, такие убеждения не мешают совершать атаки по заказу и похищать коммерческие сведения. Сфера информационных технологий, интернет в частности, — всего лишь отражение общества. Туда постепенно перекочевывают все социальные проблемы и болезни. Пусть не все хакеры воры, но и далеко не каждый Робин Гуд. Это явление имеет все признаки как минимум хулиганства, часто злого и досадного, и всегда анонимного.

Хакерские атаки, выполненные на заказ, чаще всего имеют целью похищение коммерческих секретов компании или информации о клиентах. Особенно неприятная форма атаки — это изменение информации, например исправление бухгалтерской отчетности, удаление и замена файлов баз данных. Часто целью вредительства по заказу является дезорганизация работы корпоративной сети. В результате компания может быть выбита из рабочего графика на весьма длительное время. И самая зловредная неприятность — это действие от лица компании. Например, отправка электронной почты клиентам от имени сотрудников фирмы, внесение изменений в тексты корпоративного сайта и прочее. Репутации компании в результате такой деятельности может быть нанесен тяжелейший урон.

В современной компании вопросами корпоративной информационной безопасности должен заниматься компетентный IT-специалист или даже целый отдел, который, в свою очередь, должен обучать основам этой безопасности сотрудников. Неграмотность и

небрежность могут обойтись очень дорого. Необходимо разработать политику и процедуры безопасности и следить за неукоснительным их исполнением, а также своевременно информировать и обучать сотрудников.Очень важным, если не ключевым, правилом безопасности является использование антивирусной программы, причем здесь нельзя экономить. Если для домашнего компьютера вполне подойдет бесплатный антивирус (такой как Антивирус Каспер-ского, NOD32, DrWeb, McAffe Antivirus, Norton Antivirus), то корпоративную информационную безопасность им доверять нельзя. Хорошая, регулярно обновляемая антивирусная программа защищает компьютер от вирусов, троянов и червей процентов на 95, а это уже немало.

В рамках одной статьи невозможно даже перечислить все факторы, угрожающие информационной безопасности. Технический, экономический, юридический аспекты заслуживают отдельных статей, мы обязательно вернемся к этой теме. Главный вывод один: нужно довериться профессионалам, если вы по каким-то причинам этого еще не сделали. Компетентность и профессионализм IT-специалистов — лучший залог информационной безопасности. Помимо этого, необходимо усиление ответственности за правонарушения в информационной сфере. Например, в Евросоюзе нелегальное проникновение в компьютерные сети и серверы, а также разработка вредоносных программ, в том числе вирусов, троянов и разнообразных червей, карается по закону. Если преступный умысел программиста будет доказан в судебном порядке, то ему светит наказание в виде лишения свободы сроком от одного до пяти лет. И в заключение старая истина: стоимость защиты от угрозы взлома должна быть меньше, чем стоимость восстановления, если угроза действительно срабатывает, хотя потерю репутации и доверия клиентов и партнеров трудно оценить в деньгах.

Список использованной литературы:

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016.
2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017.
3. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016.
4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016.

5. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017.

6. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018.

7. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016.

8. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016.