Прочие проблемы безопасности ЛВС включают:

1) неадекватную политику управления и безопасности ЛВС,
2) отсутствие обучения особенностям использования ЛВС и защиты,
3) неадекватные механизмы защиты для рабочих станций,
4) неадекватную защиту в ходе передачи информации.

Слабая политика безопасности также увеличивает риск, связанный с ЛВС. Должна иметься формальная политика безопасности, которая определяла правила использования ЛВС, для демонстрации позиции управления организацией по отношению к важности защиты имеющихся в ней ценностей. Политика безопасности является сжатой формулировкой позиции высшего руководства по вопросам информационных ценностей, ответственности по их защите и организационным обязательствам. Должна иметься сильная политика безопасности ЛВС для обеспечения руководства и поддержки со стороны верхнего звена управления организацией. Политика должна определять роль, которую имеет каждый служащий при обеспечении того, что ЛВС и передаваемая в ней информация адекватно защищены.

Использование ПК в среде ЛВС также приносит риск в ЛВС. В общем, в ПК практически отсутствует меры защиты в отношении аутентификации пользователей, управления доступом, контроля деятельности пользователей и т.д.

Отсутствие осведомленности пользователей в отношении безопасности ЛВС также увеличивает риск. Пользователи, не знакомые с механизмами защиты, мерами защиты и т.п. могут использовать их неправильно и, возможно, менее безопасно. Ответственность за внедрение механизмов и мер защиты, а также за следование правилам использования ПК в среде ЛВС обычно ложится на пользователей ПК. Пользователям должны быть даны соответствующие инструкции и рекомендации, необходимые, чтобы поддерживать приемлемый уровень защиты в среде ЛВС.

## БУДУЩЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Ирина РОТАРЬ,***
*Школа им. М. Коцюбинского (Кишинев, Республика Молдова)*

Для того чтобы полностью раскрыть тему, давайте разберёмся в терминологии.

**Безопасность** – это такое состояние сложной системы, когда действие внешних и внутренних факторов не приводит к ухудшению системы или к невозможности её функционирования и развития (Заплатинский В. М. «Терминология науки о безопасности».)

**Информация** - (от лат. *informatio* — осведомление, разъяснение, изложение, от лат. *informare* — придавать форму) — в широком смысле абстрактное понятие, имеющее множество значений, в зависимости от контекста. В узком смысле этого

слова — сведения (сообщения, данные) независимо от формы их представления. Сведения об объектах живой или неживой природы, их свойств и взаимном влиянии друг на друга.В настоящее время не существует единого определения термина *информация*. С точки зрения различных областей знания, данное понятие описывается своим специфическим набором признаков.

Соединив два термина понятно, что **безопасность информации** (данных) - состояние защищенности информации (данных), при котором обеспечены её (их) конфиденциальность, доступность и целостность.

**Информационная безопасность** же это - защита конфиденциальности, целостности и доступности информации.

**Информационная безопасность** может быть как и организации, так и всего государства, где в организации это- состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие, а в государстве - состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере.

То есть - это своего рода программа, защищающая какой либо объект как независимую территорию от каких либо захватов, через угрозу раскрытия и использования информации, а так же людей, как граждан, которые по закону имеют право на личную жизнь.

Система информационной безопасности включает в себя несколько составляющих.

1. Законодательная, нормативно-правовая и научная база.
2. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
3. Организационно-технические и режимные меры и методы (Политика информационной безопасности).
4. Программно-технические способы и средства обеспечения информационной безопасности.

Где следует учитывать уязвимость информации:

- хищение носителя информации или отображенной в нем информации (кража);
- потеря носителя информации (утеря);
- несанкционированное уничтожение носителя информации или отображенной в нём информации (разрушение);
- искажение информации (несанкционированное изменение, несанкционированная модификация, подделка, фальсификация);
- блокирование информации;
- разглашение информации (несанкционированное распространение, раскрытие)

На мой взгляд будущего у информационной безопасности нет… Как утверждает прочитанная мною литература виной этому является интернет, а точнее вирусы распространяемые в интернете которые способны разрушить все.

Но по видимому высшие органы власти ни одной из стран это особо не волнует, хотя может кто- то и беспокоится по этому поводу, но судя по всему не очень сильно по тому, что как мне удалось выяснить эта проблема появилась еще в 70-х годах XX века. Мало того, что она не решена в принципе, так еще и различные технологии прогрессируют, а информации все сложнее находиться в безопасности… Ярким примером этого является публикация более 400 тысяч секретных документов по Ираку. Ну и усилят сейчас меры безопасности, ну и что это даст? Предположим, что какое-то время все будет хорошо, но ведь прогресс не стоит на месте, взломают снова… почему? Потому, что постоянно программы перерабатывать, переделывать и усовершенствовать никто не будет потому, что стоит это больших затрат, а властям все равно, они не вечны, через определенный промежуток времени они меняются и каждый думает, что это проблема следующего.

Есть еще один вариант экономии бюджета на сохранении целостности данных, примером этого является Россия. Я вполне допускаю мысль о том, что я ошибаюсь и даже возможно ошибаюсь сильно, но все же не исключаю вероятности того, что всеобщий допуск к секретным советским архивам был открыт именно по этой причине, под предлогом того, что современная Российская Федерация, как суверенное, демократическое, правовое государство, не может быть преемником политики коммунистического режима. Ведь все- таки, наверное, проще самому раскрыть государственные тайны и убедить народ, что это правильно, чем получить сюрприз от WikiLeaks, который грозится в ближайшем будущем разоблачением России и Китая. Это же на самом деле проще, чем создать достойную охрану информации и плевать, что большая часть общества просто не готова к таким откровениям, плевать, что многие живут еще по тем правилам и идеалам… зато бюджет сэкономили…

Как я уже упоминала ранее, я нашла довольно много статей о том, какую серьезную угрозу информационной безопасности представляют компьютерные вирусы, которые попросту уничтожают все данные. А в наш компьютеризированный век это одна из самых страшных проблем, ведь вся информация храниться именно в компьютерах, будь то попросту семейные фотографии или секретные государственные документы. И как я уже тоже упоминала эта проблема, наверное, не закончится, как бы это пессимистично не звучало, но государственные власти никогда не договорятся со своими гражданами. Причем тут власти и граждане? Объясняю, власти экономят бюджет, а для граждан - это не плохой заработок, причем как для тех, кто создает вирусы, так и для антивирусных компаний.

Вывод из этого всего у меня получился не утешительный даже для самой себя, так как осознавать, что в государстве, в котором я живу, могут произойти серьезные проблемы или, что любой кому не лень может считать мою личную информацию с моего же компьютера, не доставляет мне радости. Но серьезней всего над этим стоит задуматься именно властям, ведь от информационной безопасности зависит, наверное, и будущее государства. Хотя может это и слишком сильно, и громко сказано… но в любом случае, думать об этом необходимо уже сейчас пока не стало слишком поздно!