

УДК 004.056.52

*А. В. Гурков,  
курсант факультета милиции  
Могилевского института МВД  
Научный руководитель: А. Э. Белько,  
старший преподаватель  
кафедры оперативно-розыскной деятельности  
факультета милиции  
Могилевского института МВД*

## **СОВРЕМЕННЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ**

В настоящее время происходит интенсификация общества, в процессе которой все ее социальные структуры преобразуются в такой вид, при котором они наиболее эффективно развиваются, а также позволяют полностью использовать имеющиеся ресурсы. Следует отметить, что привычные традиционные материальные ресурсы со временем теряют свою значимость, так как к ним на замену приходят информационные.

При информатизации общества в целом важную роль играют именно люди, которые являются носителями знаний, передают технологическую информацию, а также передовой опыт. Для обеспечения коммуникации в информационных процессах создается инфраструктура средств телекоммуникации и компьютерной техники, которая изменяет процесс и характер трудовой деятельности людей, а также их жизнедеятельность.

Благодаря глобальной компьютерной сети Интернет перемещается огромное количество цифровой информации, происходит доступ большого количества пользователей к ней. Это обуславливает необходимость развития современных компьютерных систем хранения и переработки информации, которые бы повысили уровень ее защиты. В указанных условиях защита такой информации становится обязательной: издаются соответствующие нормативные правовые акты различных уровней.

В соответствии с пунктом 8 Концепции информационной безопасности Республики Беларусь (далее — Концепция) под информационной безопасностью понимается состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Защита информации в современных информационных системах заключается в ее изолировании от посторонних пользователей, которые пытаются ее получить путем несанкционированного доступа.

В Республике Беларусь охрана информации осуществляется посредством правовых норм, содержащихся в уголовном и административном законодательствах. В Уголовном кодексе Республики Беларусь содержится глава 31, в которой закреплены 7 составов преступления против информационной безопасности. В Кодексе об административных правонарушениях Республики Беларусь (далее — КоАП) содержатся составы административных правонарушений, предусмотренные статьями 22.6–22.9 КоАП. При этом защита конфиденциальной информации как от вредоносного программного обеспечения, так и от лиц, осуществляющих свою противоправную деятельность в сфере информационных технологий (хакеров), заключается в том, чтобы усложнить эти информационные системы, а также предупредить заранее граждан об установлении специального программного обеспечения с целью предупреждения совершения преступлений.

При этом хакеры затрачивают минимальное количество усилий при получении интересующей их информации. Так, согласно данным, которые были предоставлены аналитическим центром Info Watch, в 2018 году было зарегистрировано 1039 случаев утечки конфиденциальной информации. Это на 12 % больше, чем за аналогичный период 2017 года (925 утечек).

Совокупный объем скомпрометированных личных данных физических и юридических лиц составил 2,39 млрд записей, в том числе номера социального страхования, реквизиты пластиковых карт, иная критически важная информация. За аналогичный период 2017 года скомпрометировано 7,78 млрд записей. Атаки из внешней среды составили 35,5 % от общего числа атак и 64,5 % со стороны внутренних нарушителей системы.

Статистика, описанная выше, объясняет почему в настоящее время вопрос обеспечения информационной безопасности один из наиболее актуальных проблем, стоящих перед обществом и государством в целом.

Следует отметить, что утечки информации, исходящие из внутренней сети, связаны с несоизмеримо большим риском в плане наступления негативных последствий для обладателей информации, чем утечки из-за внешнего злоумышленника. Со стороны хакера из внешней среды компрометируется набор однородных данных, к примеру, сведения о пользователях интернет-сервиса, данные граждан, которые размещаются как в глобальной компьютерной сети Интернет, так и на стационарных компьютерах.

В связи с этим следует отметить, что принятие Республикой Беларусь Концепции призвано способствовать комплексному урегулированию данной

сферы общественных отношений и отразить государственную политику в сфере обеспечения информационной безопасности. В Концепции указаны меры по защите информации, определены виды и источники угроз в сфере информационной безопасности, а также определены первоочередные мероприятия по обеспечению информационной безопасности.

Таким образом, сфера информационной безопасности Республики Беларусь нуждается в регулярном анализе защищенности, своевременном реагировании и адекватном принятии мер по устранению обнаруженных внешних и внутренних угроз безопасности, прогнозированию последствий, а также мер по предотвращению возможности негативного влияния на информационную сферу.