Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

протоколов для различных способов передачи данных. Теоретические и практические знания по данным вопросам, на наш взгляд, однозначно пригодятся ИБ-специалистам в их последующей работе.

В текущем году Фирма «АНКАД» выпускает сборник лабораторных работ под названием «Практические методы обеспечения безопасности информационных ресурсов с использованием средств защиты информации серии «КРИПТОН». Он посвящен, в основном, средствам защиты информации от несанкционированного доступа и ряду смежных направлений. Сборник включает в себя следующие лабораторные работы:

1. Обеспечение санкционированного доступа на сервер корпоративной сети с использованием программного комплекса «Crypton Lock 3.5».
2. Разграничение и контроль доступа пользователей к техническим средствам вычислительной сети с использованием аппаратно-программного модуля доверенной загрузки «КРИПТОН-ЗАМОК».
3. Двухфакторная аутентификация в службе каталогов Active Directory с использованием USB-идентификатора «РУТОКЕН».
4. Исследование средств защиты информации, хранящейся на жёстких дисках, на примере комплекса «Crypton Disk».
5. Исследование средств защиты информации с использованием электронной цифровой подписи.
6. Исследование криптографических средств защиты информации при сетевом взаимодействии на примере программного комплекса «Crypton IPMobile».
7. Исследование возможностей по управлению USB-идентификатором «РУТОКЕН» с помощью APDU-команд.

Во всех этих лабораторных работах, помимо изучения на практике основных вопросов, вынесенных в заглавия работ, от студентов требуется изучение и последующее выполнение ряда действий по настройке компьютерного оборудования и программного обеспечения, поскольку это требуется для функционирования изучаемых СЗИ. Такая настройка включает в себя:

установку и настройку программного обеспечения, в т. ч. драйверов устройств;

работу в гостевых виртуальных машинах и их настройку, включая «проброс» функций аппаратного обеспечения в гостевые операционные системы;

настройку локальных сетей и др.

Подобные лабораторные работы позволят ИБ-специалистам получить некоторые из перечисленных выше требуемых знаний. На наш взгляд, специалисты по информационной безопасности обязательно должны обладать знаниями того аппаратного и программного окружения, в котором будут работать разрабатываемые или эксплуатируемые ими средства защиты, а также опытом работы с применяемым аппаратным и программным обеспечением.

ЗАЩИТА ИНФОРМАЦИИ В УГОЛОВНОМ ПРОЦЕССЕ

Т.В. РАДЫНО

ООО «Минский электротехнический завод имени В.И. Козлова»

Задачами уголовно-процессуального закона являются закрепление надлежащей правовой процедуры осуществления уголовного процесса, обеспечение законных прав и интересов физических и юридических лиц, которым преступлением причинен физи-

ческий, имущественный или моральный вред, а также уголовное преследование и защита лиц, которые подозреваются, обвиняются в совершении предусмотренных уголовным законом общественно опасных деяний. Уголовно-процессуальный кодекс Республики Беларусь (далее - УПК) [1], основываясь на Конституции Республики Беларусь, устанавливает порядок деятельности органов, ведущих уголовный процесс, а также права и обязанности участников уголовного процесса. Установленный УПК порядок производства по материалам и уголовному делу является единым и обязательным для всех органов и должностных лиц, ведущих уголовный процесс, а также для иных участников уголовного процесса.

В целях защиты информации в уголовном процессе предусмотрен ряд организационно-правовых мер по отношению ко всем участникам уголовного процесса. Защита информации в уголовном процессе носит комплексный характер: информация защищается от несанкционированного доступа, от разглашения третьим лицам, следует отметить также меры, направленные на защиту информации от искажения, на точную ее передачу – что особенно важно при установлении признаков преступления в целях его правильной квалификации. Среди охраняемой информации как непосредственно материалы следствия (документы), сведения, полученные оперативно-розыскным путем (деятельность оперативных сотрудников), информация, которой владеют участники уголовного процесса, - так и информация, к которой имеют доступ должностные лица в связи с проведением следственных действий.

Среди основных методов защиты информации, относящейся непосредственно к расследованию уголовного дела, меры, обеспечивающие ее защиту от разглашения третьим лицам - установление запрета на разглашение сведений, ставших известными в связи с участием в процессе таких участников, как защитник, свидетель, специалист, переводчик, понятой, потерпевший, гражданский истец, законный представитель: подозреваемого, обвиняемого, лица, совершившего общественно опасное деяние, потерпевшего или гражданского истца, или гражданского ответчика. За разглашение данных предварительного расследования или закрытого судебного заседания без разрешения органа, ведущего уголовный процесс, такие лица несут установленную уголовным законодательством ответственность (ст. 407 УК).

Еще одна мера защиты особо охраняемой информации – установление ограничительных мер согласно Конституции: государственные органы, должностные и иные лица, которым доверено исполнение государственных функций, обязаны в пределах своей компетенции принимать необходимые меры для осуществления и защиты прав и свобод личности: так, прокуратура осуществляет надзор за исполнением законов при расследовании преступлений; в случаях, предусмотренных законом, поддерживает государственное обвинение в судах. В соответствии с данными конституционными положениями уточняются полномочия прокурора в уголовном процессе на досудебной стадии и при осуществлении производства по уголовным делам в суде: требования органа уголовного преследования о предоставлении в том числе информации, содержащей государственные секреты или иную охраняемую законом тайну, санкционируются прокурором. Требования о предоставлении указанной информации связаны с ограничением конституционного права на информацию, имеют целью усиление гарантий соблюдения законности, предотвращения причинения ущерба интересам национальной безопасности, защиты конституционных прав и свобод граждан и соблюдение требования соразмерности их ограничений.

Законом установлена возможность применения современных информационно-коммуникационных технологий в уголовном процессе. Так, применяется для обеспечения полноты протокола судебного заседания стенографирование, звуко- или видеоза-

пись, система видеоконференцсвязи в уголовном процессе в определяемых уголовно-процессуальном законом случаях для проведения допроса, очной ставки, предъявления для опознания лиц и (или) объектов при проведении следственных действий и в ходе судебного разбирательства, а также при исследовании доказательств судом апелляционной инстанции. Применение информационно-коммуникационных технологий, в том числе систем видеоконференцсвязи, возможно только в случаях и порядке, определяемых уголовно-процессуальным законом – в том числе и с соблюдением мер защиты информации, передаваемой по оптово-волоконным сетям. Защита информации с точки зрения защиты ее в процессе такой передачи – это установление уголовной ответственности за несанкционированный доступ к такой информации. Сегодня законодатель исходит из того, что в настоящее время несовершеннолетние обладают широкими познаниями в области компьютерных технологий, являются уверенными пользователями компьютеров, что не исключает возможности использования ими знаний в данной области для совершения противоправных деяний, в том числе хищений, а уровень их физического и психического развития позволяет осознавать фактический характер и степень общественной опасности таких деяний, устанавливая уголовную ответственность лица, совершившего хищение путем использования компьютерной техники, с 14-летнего возраста [2].

Что касается организационно-правовых мер, устанавливающих порядок защиты информации, носителями которой являются такие участники уголовного процесса, как потерпевшие; свидетели; частные обвинители; подозреваемые, обвиняемые, их защитники; законные представители, представители потерпевших, гражданских истцов, гражданских ответчиков и частных обвинителей; эксперты, специалисты, переводчики, понятые; гражданские истцы, гражданские ответчики; секретари судебного заседания, секретари судебного заседания - помощники судьи. Порядок применения мер по обеспечению безопасности в отношении защищаемых лиц с учетом особенностей их применения устанавливается отдельным нормативным правовым актом [3].

К охраняемым конфиденциальным сведениям об осуществлении мер безопасности и социальной защиты относятся:

сведения о защищаемом лице, содержащиеся в базах данных (учетах), информационных системах, а также образующиеся в них в результате применения мер безопасности;

информация о временном наложении запрета на выдачу сведений о персональных данных, месте жительства или месте пребывания, имуществе защищаемого лица, о персональных данных его близких, об изменении их абонентских номеров и (или) уникальных кодов идентификации абонента (пользователя услуг электросвязи), а также регистрационных знаков используемых ими транспортных средств, содержащаяся в соответствующем постановлении или предписании органа, обеспечивающего безопасность;

сведения о применении мер безопасности;

сведения о реализации мер социальной защиты.

Должностное лицо органа, обеспечивающего безопасность, другого государственного органа, иной организации, уполномоченных на реализацию мер социальной защиты, обязано предупредить должностных лиц и других граждан, которым конфиденциальные сведения были доверены или стали известны в связи с применением соответствующей меры безопасности в отношении защищаемого лица или реализацией мер социальной защиты, об их неразглашении, а также об ответственности, предусмотренной законодательством за разглашение этих сведений, путем представления под роспись предупреждения о неразглашении сведений о защищаемом лице.

Письменные запросы, связанные с применением мер безопасности или реализацией мер социальной защиты, а также ответы на них передаются нарочным или на-

правляются специальными либо курьерскими почтовыми отправлениями (в исключительных случаях, если государственный орган или иная организация не являются пользователями услуг специальной связи или курьерских услуг, - заказными почтовыми отправлениями) с соблюдением требований по защите государственных секретов.

Порядок учета, хранения, использования и уничтожения информационных ресурсов, содержащих конфиденциальные сведения, а также порядок выдачи из таких информационных ресурсов указанных сведений определяются соответственно Министерством внутренних дел, Комитетом государственной безопасности, Государственным пограничным комитетом, Службой безопасности Президента Республики Беларусь, Оперативно-аналитическим центром при Президенте Республики Беларусь, Комитетом государственного контроля, Государственным таможенным комитетом и Министерством обороны.

Конфиденциальные сведения государственным органам, иным организациям и гражданам не предоставляются.

Если основанием для применения мер безопасности является постановление о применении мер безопасности, вынесенное должностным лицом органа, осуществляющего оперативно-розыскную деятельность, или процессуальное постановление органа, ведущего уголовный процесс, о результатах проверки информации об истребовании сведений о защищаемом лице в связи с производством по уголовному делу, орган, обеспечивающий безопасность, уведомляет принявший решение о применении мер безопасности орган, осуществляющий оперативно-розыскную деятельность, или орган, ведущий уголовный процесс, для решения вопроса о предоставлении запрашиваемых сведений или об отказе в их предоставлении.

Сводные данные о применении мер безопасности и реализации мер социальной защиты не должны содержать сведений, позволяющих определить принадлежность персональных данных защищаемому лицу.

Список литературы

1. Кодекс Республики Беларусь от 16.07.1999 № 295-З (ред. от 20.04.2016) "Уголовно-процессуальный кодекс Республики Беларусь".

2. Кодекс Республики Беларусь от 09.07.1999 № 275-З (ред. от 19.07.2016) "Уголовный кодекс Республики Беларусь".

3. Постановление Совета Министров Республики Беларусь от 21.01.2016 № 44 (ред. от 02.12.2016) "Об утверждении Положения о порядке применения мер безопасности в отношении защищаемых лиц".

4. Решение Конституционного Суда Республики Беларусь от 29.12.2015 № Р-1024/2015 "О соответствии Конституции Республики Беларусь Закона Республики Беларусь "О внесении изменений и дополнений в некоторые кодексы Республики Беларусь".

ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

В.Б. СОКОЛОВ

Белорусский государственный университет информатики и радиоэлектроники

Человечество жило в век пещер и мамонтов, в каменном, бронзовом и железном веке. Теперь же человечество живет в веке информации. Информация того или иного рода является неотъемлемой частью нашей жизни. Именно информация является доми-