насилия, как при грабеже, так и при разбое следует учитывать не только последствия физического насилия, но и другие обстоятельства по делу, в частности способ действия виновного при применении этого насилия, имеющий важное значение для квалификации содеянного[10].

Необходимо также учитывать, что разбой считается оконченным уже с момента осуществления нападения на личность независимо от того, была ли достигнута цель завладения чужим имуществом или нет. Пленум Верховного Суда РФ в постановлении от 27.12.2002 г. №29 «О судебной практике по делам о краже, грабеже и разбое»[5] пояснил, что грабеж как и кража признается оконченным с момента завладения чужим имуществом и получения реальной возможности распоряжаться этим имуществом как своим собственным. Различные моменты окончания этих преступлений объясняются тем, что при разбое преступник дополнительно посягает на такие блага личности, как жизнь или здоровье, в то время как при грабеже посягательство направлено на значительно менее ценные блага - телесную неприкосновенность и свободу личности. Различие между разбоем и грабежом следует проводить также по моменту окончания этих преступлений. Если разбой считается оконченным с момента нападения, независимо от завладения имуществом, то для оконченного грабежа необходимо, чтобы виновный завладел чужим имуществом. Грабеж и разбой влекут уголовное наказание независимо от размера похищаемого имущества, так как опасность этих преступлений заключается не только в причинении имущественного ущерба потерпевшему, но и в насильственном способе завладения или попытке завладения чужим имуществом.

Таким образом, основное различие рассматриваемых преступлений заключается в следующем:

1. Объектом посягательства кражи является собственность субъекта права, а объектом грабежа и разбоя, кроме собственности, является личность потерпевшего (при грабеже с насилием - телесная неприкосновенность и личная свобода, а при разбое - жизнь и здоровье).

2. Кража во всех случаях исключает насилие над личностью, тогда как грабеж возможен и с применением насилия, не опасного для жизни или здоровья. Разбой же во всех случаях совершается только с насилием

Список литературы:

[1] Конституция Российской Федерации от 12 декабря 1993 г.// (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ)
[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (ред. от 19.02.2018)
[3]"Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 19.02.2018)
[4] Гражданский кодекс Российской Федерации от 21 октября 1994 года(ред. от 04.03.2018)
[5] Постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29
«О судебной практике по делам о краже, грабеже и разбое».
[6] Владимиров В.А. Квалификация преступлений против личной собственности. – М.: Просвещение, 1968. – 325 с.
[7] Кадников Н.Г. Уголовное право. Общая и Особенная части: учебное пособие. – М.: Норма, 2009. – 395 с.
[8]Рарог А.И. Уголовное право России. Части Общая и Особенная: курс лекций. – М.: ТК Велби, 2009. – 987 с..
[9]Рарог А.И. Уголовное право России. Общая часть: учебник. – М.: ТК Велби, 2009. – 496с.
[10] Рарог А.И. Уголовное право России. Части Общая и Особенная: курс лекций. – М.: Юристъ, 2005. – 480с.
[11] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Под ред. А.А. Чекалина, В.Т. Томина, В.В. Сверчкова. – 4-е издание, переработанное и дополненное. – М.: Юрайт-Издат, 2007. – С. 346.

THE PROBLEMS OF DISTINGUISHING BETWEEN THEFT, ROBBERY AND PLUNDER.

Zakharova A.

Key words: theft, robbery, plunder, objective side, subjective side.

The article examines the differences in the concepts of theft, robbery and plunder. The objective and subjective aspects of theft, robbery and plunder are considered.

УДК 343.985:004.056

***Е. А. Илюшечкин**, магистрант 1-го курса магистратуры, группы Ю(м)-17-5304*
ФГБОУ ВО Волжский государственный университет водного транспорта 603950, г. Нижний Новгород, ул. Нестерова, д.5

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ОПЕРАТИВНО-РОЗЫСКНЫЕ МЕРОПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ УСТРОЙСТВ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ.

Ключевые слова: Информационная безопасность; доступность; целостность; конфиденциальность; угроза; оперативно-розыскные мероприятия; оперативная техника.

В 1988 году американская Ассоциация компьютерного оборудования объявила 30 ноября Международным днем защиты информации. Именно 1988 год не случайно стал родоначальником праздника, именно в этот год была зафиксирована первая массовая эпидемия «червя», получившего название по имени своего создателя - Морриса. Именно тогда специалисты задумались о необходимости комплексного подхода к обеспечению информационной безопасности.

Информационная безопасностью называется информации от любых воздействий, в результате которых информация может быть изменена или утеряна, а владельцу или пользователю информации нанесён недопустимый ущерб.

Защита информации - деятельность по предотвращению утечки защищаемой информации несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информационная безопасность имеет большую значимость не только в компьютерной сфере, и зависит не только от компьютеров, но и является поддержкой инфраструктуры, к которой можно этапом отнести системы конечному электро- , водо- и теплоснабжения, конечному кондиционеры, представлено средства коммуникаций воздействие и конечно, связаны обслуживающий персонал [2, с. 53].

К объектам информационной безопасности подлежащих к защите, относятся:

- информационные ресурсы с ограниченным доступом, составляющие коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, а также акустическая (речевая) информация;
- сведения, ставшие известными сотрудникам банка в процессе исполнения ими своих должностных обязанностей;
- средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телефонной, факсимильной, радиосвязи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);
- служебные помещения, в которых хранится и обрабатывается информация ограниченного доступа;
- технические средства и системы защиты информационных ресурсов.

К субъектам можно отнести:

- государство (в целом или отдельные его органы и организации);
- общественные или коммерческие организации (объединения) и предприятия (юридических лиц);
- отдельных граждан (физических лиц) [8, с. 32].

В процессе своей деятельности субъекты могут находиться друг с другом разного рода отношениях, в том числе, касающихся вопросов получения, хранения, обработки, распространения и использования определенной информации. Такие отношения между субъектами будем называть информационными отношениями, а самих участвующих в них субъектов - субъектами информационных отношений. Различные субъекты по отношению к определенной информации могут выступать в качестве источников поставщиков информации, потребителей информации, собственников, владельцев, распорядителей информации, физических и юридических лиц, о которых собирается информация, владельцев систем обработки информации, участников процессов обработки и передачи информации [5, с. 95].

Основные составляющие информационной безопасности это:

1. Доступность - возможность за приемлемое время получить требуемую информационную услугу [4, с. 98].

Если по тем либо иным причинам получение деятельности этих услуг становится невозможным, это также наносит ущерб всем субъектам внутренних информационных отношений.

Необходимую защиту в этой области обеспечивают такие ФЗ: Федеральный закон №99 «О лицензировании отдельных видов деятельности». ФЗ регулирует отношения между органами исполнительной власти и определяет методы лицензирования отдельных видов деятельности [13] и

Федеральный закон №184 «О техническом регулировании». ФЗ регулирует отношения, которые возникают при производстве различных товаров. Описание технических товаров должно соответствовать их реальным характеристикам согласно положении об информационной безопасности[14].

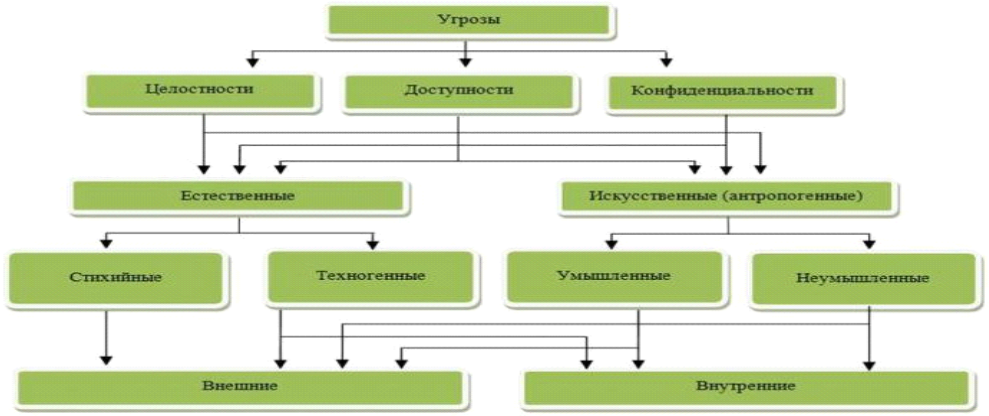
2. Целостность - актуальность и непротиворечивость информации, ее защищённость от разрушения и несанкционированного изменения. Целостность можно подразделить на статическую (понимаемую целом как неизменность информационных объектов) и динамическую (относящуюся к обеспечивающие корректному выполнению разделение действий (транзакций). Например: покупка товаров, оказание услуг и т.д. В этом случае на помощь приходит Федеральный закон №63 «Об электронной цифровой подписи». ФЗ перечисляет области деятельности, в которых используется электронная цифровая подпись в целях обеспечения информационной безопасности[15].

3. Конфиденциальность - защита несанкционированного ознакомления. На страже конфиденциальности стоят законы, нормативные акты, многолетний опыт соответствующих служб. Аппаратно-программные продукты позволяют закрыть все потенциальные каналы утечки информации [3, с.120]. Урегулирование происходит с помощью Федерального закона №152 «О персональных данных». ФЗ регулирует отношения между органами государственной власти во время поиска важных сведений и обеспечивает информационную безопасность персональных данных[16].

«Неприемлемый ущерб» в информационной безопасности, очевидно, говорит о том, что застраховаться от всех видов ущерба конечно невозможно.

Знание угроз необходимо знать для того, чтобы соблюдать обеспечения безопасности [12, с.73].

Рассмотрим основные угрозы безопасности в краткой схеме:



Стоит отметить, что некоторые угрозы нельзя считать следствием чьих-либо ошибок или этапом просчетов. Например, из-за угрозы отключения местного электричества или в случае если что-то вышло из строя, поэтому в данной ситуации в Информационной безопасности следует обозначить важность электропитания. Само понятие «угроза» трактуется по-разному. Например, для открытой организации угроз конфиденциальности может просто не существовать, поскольку вся информация считается доступной [8, с. 134].

Существуют методы обеспечения безопасности информации в ИС:

1. Препятствие – физическое преграждение пути злоумышленнику к защищаемой информации (например, коммерчески важная информация хранится на сервере внутри здания компании, доступ в которое имеют только те сотрудники).

2. Управление доступом – регулирование, использование информации и доступа к ней за счет системы идентификации пользователей, их распознавания, проверки полномочий и т.д. (например, когда доступ в отдел или на этаж с компьютерами, на которых хранится секретная информация, возможен только по специальной карточке-пропуску или когда каждому сотруднику выдается персональный логин и пароль для доступа к базе данных предприятия с разными уровнями привилегий).

3. Криптография – шифрование информации с помощью специальных алгоритмов (например, шифрование данных при их пересылке по Интернету; или использование электронной цифровой подписи).

4. Противодействие атакам вредоносных программ (англ. «malware») – предполагает использование внешних накопителей информации только от проверенных источников, антивирусных программ, брандмауэров, регулярное выполнение резервного копирования важных

данных и т.д. (вредоносных программ очень много и они делятся на ряд классов: вирусы, эксплойты, логические бомбы, трояны, сетевые черви и т.п.).

5. Регламентация - создание условий по обработке, передаче и хранению информации, в наибольшей степени обеспечивающих ее защиту (специальные нормы и стандарты для персонала по работе с информацией, например, предписывающие в определенные числа делать резервную копию электронной документации, запрещающие использование собственных флеш-накопителей и т.д.).

6. Принуждение - установление правил по работе с информацией, нарушение которых карается материальной, административной или даже уголовной ответственностью (штрафы, закон «О коммерческой тайне» и т.п.).

7. Побуждение - призыв к персоналу не нарушать установленные порядки по работе с информацией, т.к. это противоречит сложившимся моральным и этическим нормам (например, Кодекс профессионального поведения членов «Ассоциации пользователей ЭВМ США»).

Тесно связаны с информационной безопасностью оперативно-розыскные мероприятия, в ходе проведения которых используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерб жизни и здоровью людей и не причиняющие вред окружающей среде. [10, с. 138].

Подводя итог, нельзя не упомянуть, что для решения масштабных задач ИБ оперативно-розыскные органы испытывают острую потребность как в задействовании значительного числа квалифицированных специалистов, получивших серьезную подготовку в области информационных технологий (оперативные сотрудники, следователи, аналитики, эксперты, программисты и др.), так и в разработке и внедрении комплексного программного обеспечения, приобретении сложного дорогостоящего оборудования, создании мощных дата-центров для хранения и обработки цифровых данных, совершенствовании системы сбора, хранения и обработки всей оперативно значимой информации. Это возможно лишь при условии объединения усилий и четкой координации деятельности всех субъектов реализации Доктрины информационной безопасности Российской Федерации.

Список литературы

[1] Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право. М.: ЮНИТИ-ДАНА, Закон и право, 2004.
[2] Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации 3-е изд. Учеб. Пособие для студ. высш. учеб. заведений/В. П. Мельников, С. А. Клейменов, А. М. Петраков.- М.:2008.
[3] Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002.
[4] Галатенко В. А. Стандарты информационной безопасности. — М.: ИНТУИТ, 2006.
[5] Интернет-университет информационных технологий, 2006.
[6] Галицкий А. В., Рябко С. Д., Шаньгин *В. Ф.* Защита информации в сети — анализ технологий и синтез решений. М.: ДМК Пресс, 2004.
[7] Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008.
[8] Лопатин В. *Н.* Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000.
[9] Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008.
[10] Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006.
[11] Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004.
[12] Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.
[13] Федеральный закон "О лицензировании отдельных видов деятельности" от 01.01.2018 N 99-ФЗ
[14] Федеральный закон "О техническом регулировании" от 29.07.2017 N 184-ФЗ
[15] Федеральный закон "Об электронной подписи" от 31.12.2017 N 63-ФЗ
[16] Федеральный закон "О персональных данных" от 29.07.2017 N 152-ФЗ

INFORMATION SECURITY. INVESTIGATION ACTIVITIES WITH THE USAGE OF NATIONAL SECURITY TECHNICAL DEVICES.

Key words: Information security; availability; integrity; confidentiality; threat; investigation activities; operational technology.

The article describes the problem of information security provision. The forms and the types of information security provision in Russia, its threats, as well as the methods for information protection are considered. Investigation measures with the usage of national security technical devices to ensure information security bare studied.