ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

Факультет безопасности информационных технологий

Дисциплина:
«Организационное и правовое обеспечение информационной безопасности»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1

Государственная политика информационной безопасности и ее реализация в законодательстве Российской Федерации

Выполнил:
Студент ОИП 1.1 гр. №N3253
Пастухова А.А.

Проверил:
Королёва А.А._____
Дата _____ отметка _____

Санкт-Петербург
2022 г.

1. **Классификация угроз информационной безопасности РФ, изложенных в главе III Доктрины информационной безопасности, по различным признакам.**

По расположению источника:
Зарубежные страны; внутри России.

По видам взаимодействия:
Публикация недостоверных материалов в средствах массовой информации; информационное воздействие на население, в первую очередь на молодежь; компьютерная преступность, прежде всего в кредитно-финансовой сфере; разведывательная деятельность иностранных государств в отношении РФ

По направленности:
Воздействие на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников; подрыв суверенитета и нарушение территориальной целостности других государств; нарушением конституционных прав и свобод человека и гражданина

По цели воздействия:
Геополитические, военно-политические, террористические, экстремистские, криминальные и иные противоправные цели. Информационная инфраструктура в военных целях, техническая разведка в отношении государственных органов, научных организаций и предприятий оборонно-промышленного комплекса; оборона страны, территориальная целостность, политическая и социальная стабильность РФ

2. **Перечень реестров, которые создаются и ведутся уполномоченными органами государственной исполнительной власти, в соответствии с федеральным законом 149-ФЗ**

Статья 2. В реестр включаются:
1) доменные имена и (или) указатели страниц сайтов в сети "Интернет", содержащих информацию, распространение которой в Российской Федерации запрещено;
2) сетевые адреса, позволяющие идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено.

Статья 5. Основаниями для включения в реестр сведений, указанных в части 2 настоящей статьи, являются:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети "Интернет":

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года N 244-ФЗ "О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации" и Федерального закона от 11 ноября 2003 года N 138-ФЗ "О лотереях" о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети "Интернет" и иных средств связи, а также информации, обеспечивающей возможность совершения действий по переводу денежных средств через иностранных поставщиков платежных услуг, включенных в перечни, предусмотренные частями 16 и 32 статьи 5.1 Федерального закона от 29 декабря 2006 года N 244-ФЗ "О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации", частями 11 и 26 статьи 6.2 Федерального закона от 11 ноября 2003 года N 138-ФЗ "О лотереях";

е) информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции;

ж) информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц;

з) информации, содержащей предложение о розничной торговле лекарственными препаратами, в том числе дистанционным способом, розничная торговля которыми ограничена или запрещена в соответствии с законодательством об обращении лекарственных средств, и (или) информации, содержащей предложение о розничной торговле лекарственными препаратами, в том числе дистанционным способом, лицами, не имеющими

лицензии и разрешения на осуществление такой деятельности, если получение лицензии и разрешения предусмотрено законодательством об обращении лекарственных средств;

и) информации, содержащей сведения о лицах, в отношении которых в соответствии с Федеральным законом от 20 апреля 1995 года N 45-ФЗ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов" и Федеральным законом от 20 августа 2004 года N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" обеспечивается конфиденциальность;

2) решение суда о признании информации, распространяемой посредством сети "Интернет", информацией, распространение которой в Российской Федерации запрещено;

3) постановление судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети "Интернет", порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица.

3. Определить перечень органов исполнительной власти, регулирующих правоотношения в сфере действия федерального закона 149-ФЗ.

Название ОГВ в законе	Название ОГВ актуальное
Федеральные органы исполнительной власти	ФСБ, МВД, МИД, Министерство обороны
Правительство РФ	Правительство РФ
Совет Федерации Федерального Собрания РФ	Совет Федерации (Верхняя палат Федерального собрания)
Государственная Дума Федерального Собрания РФ	Государственная дума России I созыва
Совет Безопасности РФ	Совбез, СБ РФ
Органы местного самоуправления	Представительный орган муниципального образования, глава муниципального образования, местная администрация

Эссе на тему «Личная информационная безопасность»

Прежде всего, скажу, что в век технологических инноваций никак не обойтись без защиты собственных данных. Зачастую мы даже не задумывается о том, как часто в течение дня мы используем информацию, которая подлежит надёжному сокрытию.

И даже если вам кажется, что в аккаунте компьютерной игры нет никакой важной и ценной информации, вы точно ошибаетесь. Умелый хакер сможет вычислить не только номер вашего телефона, банковской карты, ссылки на другие соцсети, но и пароли к ним или прочитать личные переписки.

Видно, что проблема хищения личной информации (ваши имя и фамилия), паспортных данных (номер, серия, копия паспорта), паролей для доступа к различным сервисам и электронным кошелькам является на сегодняшний день актуальной в современном мире, так как ее касается почти каждый человек.

С правовой точки зрения, согласно федеральному закону РФ о персональных данных от 2006 года, личная информация не может распространяться, использоваться в личных целях или передаваться третьим лицам без разрешения владельца. Также с персональной информацией нельзя совершать действий, которые могут нарушать права человека, зафиксированные в международных законах.

Далее я напишу несколько основных советов, как обезопасить себя и свои личные данные от злоумышленников и нежелательных лиц.

Во-первых, все личные технические устройства следует заблокировать, причем советуют использовать разные способы в том числе биометрический и обыкновенный пароль/ПИН-код на случай, если один из них вы забудете. Пароль для регистрации на сторонних интернет-ресурсах должен быть достаточно сложным, но легко запоминающимся для пользователя. Например, можно использовать метод ассоциаций или составлять 1 большое слово из нескольких маленьких, связанных последовательно, и заменить некоторые буквы на цифры и символы. При этом рекомендуют устанавливать на разных ресурсах различные пароли и менять их через каждый полгода-год.

Безусловно, запомнить все пароли наизусть невозможно, особенно, если на каждом ресурсе они разные, а таких полсотни. Тогда крайне удобно воспользоваться, так называемым, менеджером паролей. Специальное облачное пространство, которое надежно шифрует все пароли и логины, что даже владельцу нужно подтвердить свои данные, прежде чем он сможет их увидеть.

Из плюсов: пароли всегда «под рукой», из минусов: доступ к облаку также может быть взломан.

Во-вторых, обязательно используйте двухфакторную аутентификацию в соцсетях, мессенджерах и учетных записях. Она обеспечит мощную защиту, потребовав ввести не только придуманный пароль, но и номер телефона или отпечаток пальца. По началу, это покажется неудобным и будет занимать много времени, но в случае массового взлома страничек вы определенно поблагодарите себя. Ведь, в большинстве случаев, к вашему аккаунту злоумышленник не сможет получить доступ.

В-третьих, отслеживайте что и кому вы говорите относительно своей личной жизни или близких людей, как и когда вы публикуете записи в соцсетях, как часто вы удаляете устаревшие данные из интернета. Все это очень важно, поскольку "всё, что попало в сеть, остается там навсегда" и есть риск столкнуться с серьёзными неприятностями.

В дополнение, следует периодически проверять свой персональный компьютер с использованием антивируса, который поможет выявить вредоносные файлы и программы. Немаловажно читать клиентское соглашение, когда заполняем какие-то документы или онлайн опросы, там может скрываться скрытая информация, позволяющая распространять ваши личные данные.

Вышеперечисленные пункты я применяю в повседневной жизни и предлагаю вам. Таким образом можно создать относительно безопасное информационное пространство, внутри которого вы будете чувствовать себя менее уязвимым и жить в удовольствие.

Подводя итог, скажу, что проблема личной информационной безопасности остается открытой и по сей день. Возможным ее решением может являться, по моему мнению, комплекс действий со стороны государства (правовые и технические меры) и со стороны конкретного человека (ответственное хранение и передача данных).

Будьте бдительны всегда и соблюдайте правила личной безопасности!