УДК 004

Ваулин В.И.[1], кандидат педагогических наук, доцент;
Карсунцев В.А.[1], **Плохотнюк А.А.**[1], **Ваулин С.В.**[2]
[1] *Филиал ФГБОУ ВО «Самарский государственный технический университет», г. Сызрань, Российская Федерация*
[2] *ОАО «ТЯЖМАШ», г. Сызрань, Российская Федерация*

КИБЕРПРАВА ЧЕЛОВЕКА В УСЛОВИЯХ ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ

Аннотация: в статье рассматриваются результаты реализации цели исследования анализа информационной безопасности жизни и деятельности общества в современных условиях. Утверждается, что теоретическую значимость исследования определили выводы анализа информационной безопасности, которые констатируют факт проблем, связанных с возможной порчей, потерей или несанкционированных взломом важной информации. Практическую значимость определяют выводы, которые включают: методы преступников; классификация средств и методов защиты информации; методы и способы защиты информации. Главным направление противодействия киберпреступлениям является система законодательных и нормативно-правовых актов. Предлагаются рекомендации по защите информации.

Abstract: the article examines the results of the realization of the purpose of the research analysis of information security of life and activities of society in modern conditions. It is argued that the theoretical significance of the study was determined by the conclusions of the information security analysis, which state the fact of problems related to possible damage, loss or unauthorized hacking of important information. The practical significance is determined by the conclusions, which include: methods of criminals; classification of means and methods of information protection; methods and methods of information protection. The main area of countering cybercrime is the system of legislative and regulatory legal acts. Recommendations on information protection are proposed.

Ключевые слова: информационная безопасность, проблемы информационной безопасности, методы киберпреступлений, методы и средства защиты информации, система законодательных и нормативно-правовых актов

Keywords: information security, problems of information security, methods of cybercrime, methods and means of information protection, system of legislative and regulatory legal acts.

В век компьютерных информационных технологий сложно представить существование сфер деятельности, как научные исследования, образование, промышленность, транспорт, коммерческая, финансовая и др. направлений. Использование информационных технологий в деятельности организаций существенно облегчают работу, но и создают проблемы возможной порчи, потери, взломов информации и

т.д., что определяет актуальность темы исследования. Возможно выделить уровни проявления киберпреступлений: – **микроуровень** (уровень отдельных домохозяйств и предприятий); – **макроуровень** (уровень отдельных отраслей); – **мезоуровень** (уровень отдельных стран или их объединений). Источники возникновения операционных киберрисков систематизировали. В условиях цифровизации выделяются следующие виды рисков и угроз в деятельности организации: стратегические, технологические, операционные, сторонние, нормативные, кибернетические, риски устойчивости, утечки данных, конфиденциальности и т.д.Информационная безопасность государства – состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере. В социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т.п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Информационная безопасность (ИБ) характеризует сохранение свойств конфиденциальности, целостности и доступности информации (КЦД) [3], свойства подлинности, подотчетности, неотказуемости, надежности, свойство доверия (trustworthiness), свойства контролируемости владельцем (possession) и полезности, «обеспечение ИБ» [7].

Киберпреступники используют программы с популярными паролями для перебора комбинаций букв, цифр и символов. Для реализации угроз используется канальный и прикладной уровень эталонной модели. Такие атаки получили название «фишинг» (англ. fishing - «рыбалка»), который может быть двух видов: как бы законный фишинг (когда в результате невнимательности пользователя его запрос переадресуется с необходимого объекта на ложный объект); незаконный (когда идет подстановка (замена) маршрута). К типовым угрозам относятся: подмена доверенного объекта; создание в сети ложного маршрута; ложного объекта с использованием недостатков алгоритмов удаленного поиска; угрозы типа «отказ в обслуживании», основанные на IP-дефрагментации, формировании некорректных ICMP-запросов (например, атака «Ping of Death» и «Smurf») и некорректных TCP-запросов (атака «Land»), на создании «шторма» пакетов с запросами на соединение (атаки «PING flood» и «SYN flood») и др. К типовым угрозам, реализуемым на прикладном уровне, относятся: направленные на несанкционированный запуск приложений; угрозы, реализация которых связана с внедрением программных закладок (типа «троянский конь»); выявления паролей доступа к ресурсам ИС и т.д. [8]. Преступники присылают: фишинговые письма, от банков, компаний, органов власти; письмо с выгодным

предложением, поддельные приложения, подделывают мобильные банки и др., чтобы получить логинам и паролям, номерам карт, банковским счетам. Придумайте пароль для каждого критичного аккаунта: интернет-банка, соцсетей и Госуслуг.

Основными способами защиты информации являются [2]: препятствие (физическая защита информационных систем); маскировка (преобразование на основе определенного принципа информации в зашифрованную форму; регламентация (создание и следование инструкциям по манипуляции с информацией); управление (системный подход к управлению защитой информационных систем); принуждение (комплекс управленческих мер, заставляющий работников следовать определенным правилам в компании); побуждение (выполнений инструкций по моральным и личностным соображениям). Способы информационной защиты обеспечиваются различными средствами: законодательными, организационными, физическими, психологическими, техническими (программные и аппаратные) [3]. Физические средства защиты информации заключаются в ограничении физического доступа к информации. К ним относятся: установка замков, решеток, прочных ворот, дверей, сигнализации. Организационные средства защиты информации основаны на правильной организации системы работы персонала и используют методы: управление, регламентация и принуждение [2].

К законодательным средствам относят систему нормативно-правовую систему, регулирующую работу сотрудников компании с уголовной или административной ответственностью за ее утерю, порчу. Психологическими средствами защиты информации называют систему мотивирующих факторов, предполагающих личную заинтересованность каждого в защите информации.

Обеспечение информационной безопасности объектов в России основывается на системе нормативно-правовых актов, которые регулируют порядок защиты и контроля за соблюдением безопасности.

Система нормативных актов дает основы обеспечения информационной безопасности. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». Текст Указа опубликован на «Официальном интернет-портале правовой информации» (www.pravo. gov.ru) 3 июля 2021 г. № 0001202107030001, в Собрании законодательства Российской Федерации от 5 июля 2021 г. № 27 (часть II) ст. 5351. и др.

Данный подход позволяет предложить модель процесса обеспечения кибербезопасности.

На основе анализа нормативно-правовой документации по защите персональных данных в организации основных требований регулирующих органов, предъявляемых к аппаратным, программным и

административным средствам по защите персональных данных, выявить необходимый и достаточный уровень защищенности персональных данных в медицинских информационных системах и основные концепции его реализации.

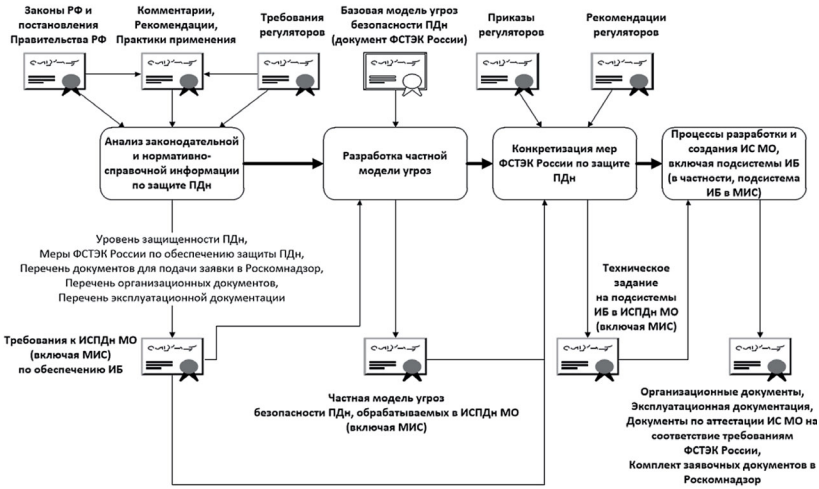

Рисунок – Процессы обеспечения ИБ [1].

Согласно постановлению выделяют три типа актуальных угроз:

• угрозы 1-го типа – угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в ИС;

• угрозы 2-го типа – угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в ИС;

• угрозы 3-го типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИС.

Для защиты сведений в организациях и на предприятиях применяются методы:

- юридические;
- организационно-управленческие;
- технические (программное обеспечение) [6].

Заключение. Таким образом, в ходе выполнения исследования была реализована цель анализа информационной безопасности жизни и деятельности общества в современных условиях. Теоретическую значимость определили выводы анализа информационной безопасности,

которые констатируют факт проблем, связанных с возможной порчей, потерей или несанкционированных взломом важной информации. При этом информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической безопасностью. Практическую значимость определяют выводы: преступники используют методы: взлом пароля электронного устройства, фишинг, письмо с выгодным предложением, поддельные приложения, блокировать попытки программного взлома устройств (хакерские и т.п. атаки); классификация средств защиты информации включает: организационные средства защиты информации, физические средства защиты информации, психологические средства защиты информации; методы и способы защиты информации: препятствие, маскировка, регламентация, управление, принуждение, побуждение; физические средства защиты информации; средствами информационной защиты являются: законодательные, организационные, физические, психологические, технические (программные и аппаратные) мероприятия. Рекомендации: быть внимательным, быть аккуратным и бережно относиться к данным, скачивать только проверенные приложения, не давать приложениям лишних разрешений, обновлять систему защиты.

Повсеместная интеграция цифровых технологий и создание децентрализованных экосистем способны открыть новые горизонты и устранить ряд текущих проблем. Ключевая роль нейронных сетей в этом процессе заставляет уделять особое внимание каждой потенциальной угрозе. Особого внимания заслуживает вопрос возникновения цифровой защиты и использование доверенного искусственного интеллекта.

Список цитируемой литературы

1. Бердникова Л.Ф., Вокина Е.Б. Функции и виды рисков, влияющих на экономическую безопасность организации в условиях цифровизации бизнеса // Вестник СамГУПС. – 2019. – № 4(46). – С. 72–77.

2. Газизова Е.В. Современные технологии защиты информации//Современные научные исследования и инновации. 2016. № 11 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2016/11/73532 (дата обращения: 25.02.2025).

3. ГОСТ Р ИСО/МЭК 27000 - 2012 НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Информационная... docs.cntd.ru›document/1200102762 (дата обращения: 25.04.2025).

4. ГОСТ Р ИСО/МЭК 15408-1(2,3) - 2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1-3.

5. Доброва К.Б. Проблемы обеспечения информационной безопасности инновационной деятельности в интегрированных промышленных структурах // Вопросы инновационной экономики. – 2017. № 4. – С. 349–360. – doi: 10.18334/vinec.7.4.38559 .

6. Иванов А. А. Ключевые понятия системного подхода к адаптивному мониторингу информационной безопасности киберфизических систем // Цифровая трансформация общества и информационная безопасность: материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.). Екатеринбург, 2022. – С 17-20.

7. Марков А.С. КИБЕРБЕЗОПАСНОСТЬ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК БИФУРКАЦИЯ НОМЕНКЛАТУРЫ НАУЧНЫХ СПЕЦИАЛЬНОСТЕЙ//Журнал Вопросы кибербезопасности. – Москва: 2022. №1(47). С.2.-10.

8. Муханова А.А., Ревнивых А.В., Федотов А.М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах//Вестник НГУ. Серия: Информационные технологии. 2013. Том 11, выпуск 2. С.55–72.

Summary. The purpose of the research is to analyze the information security of society's life and activities in modern conditions. **Materials and methods.** Methods of systematic and structural analysis of scientific sources and statistical data. **Result.** Criminals use the following methods: hacking the password of an electronic device, phishing, a letter with a favorable offer, fake applications, blocking attempts at software hacking of devices; methods and methods of information protection: obstruction, disguise, regulation, management, coercion, inducement; physical means of information protection; means of information protection are: legislative, organizational, physical, psychological, technical (software and hardware) measures. Recommendations: be careful, be careful and take care of the data, download only verified applications, do not give unnecessary permissions to applications, update the protection system.

УДК 331.45

Мартынова Л.Г.[1], заместитель начальника отдела охраны труда и пожарной безопасности,
Белохвостов Г.И.[2], кандидат технических наук, доцент
[1] ОАО «Агентство охраны труда, г. Гродно, Республика Беларусь
[2] Учреждение образования «Белорусский государственный аграрный технический университет», г. Минск, Республика Беларусь

ШУМОВОЕ ВОЗДЕЙСТВИЕ НА РАБОТНИКОВ И ЕГО ОЦЕНКА

Аннотация. Рассмотрено воздействие шума на органы и системы организма работника, а также процедура оценки шумового воздействия.

Abstract. The impact of noise on the organs and systems of the worker's body, as well as the procedure for assessing noise exposure, are considered.

Ключевые слова. Шум, октавные звуковые полосы, измерение, лабораторный контроль.

Keywords. Noise, octave bands, measurement, laboratory control.

Производственный шум остается одним из ведущих вредных факторов на предприятиях машиностроения, горнодобывающей, легкой промышленности, агропромышленного комплекса. Производственный