Карнаухова Юлия Александровна,
курсант учебной группы 19о7г
факультета подготовки специалистов ГИБДД
ОрЮИ МВД России им. В.В. Лукьянова, г. Орёл

Научный руководитель: **Флоря Денис Федорович,**
кандидат юридических наук, доцент, начальник кафедры ОРД ОВД
ОрЮИ МВД России им. В.В. Лукьянова, г. Орёл

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РФ В СОВРЕМЕННЫХ УСЛОВИЯХ
INFORMATION SECURITY OF THE RUSSIAN FEDERATION IN MODERN CONDITIONS

Аннотация: В данной статье рассматриваются основные аспекты, связанные с обеспечением информационной безопасности в РФ, обозначаются и анализируются проблемы регулирования и защиты информации на современном этапе развития государства. Перечислены наиболее распространенные уязвимости в системах защиты информационных данных, проанализирована динамика инвестиций в информационную безопасность в РФ.

Abstract: This article discusses the main aspects related to ensuring information security in the Russian Federation, identifies and analyzes the problems of regulation and protection of information at the current stage of state development. The most common vulnerabilities in information data protection systems are listed, the dynamics of investments in information security in the Russian Federation is analyzed.

Ключевые слова: информационная безопасность, киберугрозы, инфраструктура безопасности, цифровая экономика, цифровизация.

Keywords: information security, cyber threats, security infrastructure, digital economy, digitalization.

Глобализация стала особенно сильно проявляться в начале XXI века. Этому способствовало бурное развитие информационных технологий. Современное общество обеспокоено вопросом информационной безопасности используемых технических систем.

Развитие и распространение информационных технологий определяет информационную безопасность как значимую составляющую стабильного функционирования любой организации. Распространение удаленного формата работы, вызванное нестабильной эпидемиологической обстановкой, формирует необходимость внедрения систем, обеспечивающих связь и совместную работу сотрудников в дистанционном режиме. В отдельных случаях обеспечение непрерывности бизнес-процессов в сложившихся условиях может быть связано с ослаблением или отказом от отдельных элементов информационной безопасности, что создает новые уровни уязвимости в организации.

В нынешнее время мы можем говорить о том, что сложилась определенная система управления национальной безопасностью в РФ. Однако функционирование такой системы нельзя назвать совершенным. Так, если взять аспект, связанный с внедрением цифровизации во все сферы общественных отношений, то сможем заметить определенную проблематику, связанную с обеспечением национальной безопасности в РФ в условиях цифровой трансформации [3].

Ускорившиеся темпы цифровизации порождают, в том числе, и новые угрозы, что, в совокупности с перечисленными обстоятельствами, повышает запрос на создание надежной инфраструктуры безопасности и системы управления рисками. Создание надежной инфраструктуры безопасности предполагает внедрение набора стратегий, поддерживающих целостность и конфиденциальность информации, блокируя несанкционированный доступ к информационным ресурсам организации. Достижение данной цели связано с применением комплекса организационных и технических мер, которые обеспечивают защиту информационных данных и поддерживают инфраструктуру от случайного или преднамеренного вмешательства.

Информационная сфера представляет собой системообразующий фактор развития страны и проникает во все сферы жизни государства, общества, личности, влияя на них независимо от социальной, политической, экономической, культурной либо же военной направленности. В сложившихся реалиях развития современного мира можно с уверенностью утверждать тот факт, что национальная безопасность РФ напрямую зависит от способности государства обеспечить состояние защищенности информации как одного из главенствующих и «стратегических» ресурсов XXI века, и эта зависимость, несомненно, будет возрастать с дальнейшим совершенствованием научного и технического прогресса.

В настоящее время существует достаточно большое количество определений понятия «информационная безопасность», но, на наш взгляд, для более глубокого и полного понимания следует обратиться к Указу Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [1], согласно которому информационная безопасность Российской Федерации понимается как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. Положения «Доктрины информационной безопасности Российской Федерации» более детально раскрываются в отдельных приказах и распоряжениях министерств и ведомств, одним из них является Приказ Минкомсвязи России № 486 от 20.09.2018 г. «Об утверждении методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения» [2].

Таким образом, для того, чтобы создать необходимые условия для обеспечения защиты всего информационного поля, складывающегося в различных направлениях и сферах жизни, государству приходится постоянно противостоять и бороться с различными внутренними и внешними угрозами, которые могут пошатнуть баланс регулирования потоков безопасной информации на территории нашей страны. Но несмотря на все предпринимаемые меры для защиты информации на данный момент в нашем государстве существует ряд проблем, требующих масштабного и эффективного решения, поскольку не устранение таких проблем может привести к серьезным вредоносным последствиям, которые, в конечном счете, могут коснуться каждой структуры обеспечения жизнедеятельности и каждого человека в стране. Важнейшей проблемой в области обеспечения информационной безопасности до сих пор является защита самой информации [4].

Угрозы информационной безопасности можно классифицировать по следующим видам:

Естественные. Угрозы, связанные со стихийными бедствиями, в результате которых происходят сбои в функционировании системы безопасности организации; искусственные. Подразделяются на угрозы, возникающие в результате преднамеренных внутренних или внешних атак с целью вывода из строя систем безопасности, и угрозы, возникающие из-за неосторожных действий, которые привели к нарушению целостности информационной безопасности организации;

Внутренние. Угрозы, источники, возникновения которых находятся внутри системы;

Внешние. Угрозы, источники, появления которых расположены за пределами системы.

Перечисленные угрозы могут по-разному воздействовать на систему безопасности организации.

Цифровая трансформация экономических процессов и распространение электронных транзакций формируют возможности для совершенствования искусственных угроз, которые обладают наибольшей разрушительной силой. Это, в свою очередь, способствует развитию индустрии кибербезопасности и определяет основные тенденции в области информационной безопасности. Формирование большинства тенденций в данной сфере является ответной реакцией на периодически расширяющуюся поверхность кибератак, чему способствует рост числа устройств с выходом в Интернет, а также распространенность программ, требующих постоянного доступа к сети. Увеличение количества точек доступа в Интернет является плацдармом для покушений на систему безопасности и предполагает рост потенциальных возможностей получения несанкционированного доступа обманным путем с использованием фишинговых схем.

Ситуация усугубляется возрастающей сложностью и изощренностью совершаемых атак, направленных на повреждение систем защиты. Наличие одной уязвимости в перспективе представляет угрозу для деятельности всей организации, таким образом, к тяжелым последствиям могут привести кибератаки, носящие точечный характер. К числу тенденций киберугроз, предполагающих непосредственное взаимодействие с сотрудниками организаций, относится применение мошеннических схем, основанных на актуальных повестках в информационном пространстве.

Таким образом, новые вызовы информационной безопасности вынуждают государственный и частный сектор инвестировать больше средств в систему защиты собственных данных. Необходимость предупреждения несанкционированного доступа в корпоративные сети и компрометации данных требует постоянного совершенствования систем защиты и адаптации их к появляющимся киберугрозам. Выстраивание подобных систем, обладающих достаточной устойчивостью к попыткам нарушения информационной безопасности, предполагает внедрение комплексной системы безопасности,

включающей процессы управления и мониторинга рисков. Перечисленные обстоятельства в совокупности с реализацией проектов в рамках «Цифровой экономики» обуславливают динамику роста инвестиций на российском рынке информационной безопасности.

Список литературы:

1. Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

2. Приказ Минкомсвязи России «Об утверждении методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения» от 20.09.2018 г. № 486 (ред. от 10.09.2021) [Электронный ресурс] Режим доступа: https://base.garant.ru/ (Дата обращения: 08.12.2022)

3. Бирулёв И.М. Система управления национальной безопасностью в РФ // В сборнике: Школа молодых новаторов. Сборник научных статей 3-й Международной научной конференции перспективных разработок молодых ученых. В 3-х томах. Курск, 2022. С. 140-143.

4. Шуршалова Е.С. Искусственный интеллект в информационной безопасности // В сборнике: Цифровая экономика: перспективы развития и совершенствования. Сборник научных статей 3-й Международной научно-практической конференции. Курск, 2022. С. 464-467.