Качалов Вадим Юрьевич
канд. социол. наук, доцент
Кулакова Татьяна Олеговна
судентка
Казанский кооперативный институт (филиал)
АНОО ВО ЦС РФ «Российский университет кооперации»
г. Казань, Республика Татарстан

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: РИСКИ УГРОЗ И ИХ ВИДЫ

Аннотация*: в статье анализируется понятийный аппарат по информационной безопасности, раскрываются основные виды угроз в современности, а также высказаны некоторые предложения по попытке защите информации.*

Ключевые слова*: информационные угрозы, обеспечение безопасности, негативные последствия.*

Информационная безопасность играет важную роль в сохранности и повышении скорости передачи информации в сетях. В настоящее время снижение скорости и угроза потери данных является одной из основных проблем в современном мире, так как информационные сети развиваются быстро и идут шаг в шаг со временем.

Рассмотрим определение информационной безопасности и возьмем в пример Российскую Федерацию. Согласно статьи Доктрине РФ: «Информационная безопасность России – «состояние защищенности личности, общества и государства от внутренних и внешних угроз в информационной сфере» [3]. Информационная безопасность и виды угроз информационной безопасности тесно взаимосвязаны. Если пренебрегать безопасностью и подвергать ее к постоянному риску, которые с каждым днем растут, могут возникнуть проблемы в различных отраслях деятельности государства таких как:

– экономическая отрасль государства;
– социальная сфера деятельности;
– хозяйственных сфера деятельности;
– правоохранительная сфера деятельности.

Постоянная угроза информационной безопасности может лишь ухудшить жизнь населения любого государства, именно поэтому нужно грамотно планировать и защищать информационную система от угроз.

Что же представляет из себя информационная угроза? Информационная угроза – это совокупность последовательных действий, которые приводят к нарушению сохранности информационной безопасности и информационных сетей, нарушая конфиденциальность данных обеспечивая утечку информации в массовые сети.

Какие же группы информационных угроз существуют на данный момент? Они делятся на две группы:

1) естественные угрозы – это угрозы, которые появляются в следствии наступления различных стихийных бедствий и не зависят от человека (потоп, метеорит и так далее);

2) искусственные угрозы – это угрозы, на которые влияет сам человек, зачастую специально для получения скрытой информации, но существуют и непреднамеренные оплошности из-за неопытности рабочих.

Исходя из этих групп выделяют множество видов угроз информационной безопасности, выделим из них самые наиболее опасные:

1) информационный саботажем считают недобросовестное и небрежное неисполнение рабочих обязанностей, которое возникает из-за злого умысла и для нанесения крупного ущерба предприятию;

2) неправомерным доступом к информации считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя) [1];

3) утечка информации – это незаконная и специальная передача информации из скрытых, безопасных источников, которая распространяется за пределы информационной безопасности;

4) киберпреступность – это незаконный вид деятельности во многих странах, киберпреступники осуществляющие данный вид деятельности вторгаются в информационную сеть или в персональный компьютер для пользования ими;

5) спам – это рассылка бесполезной информации, различные рекламы, послания, встречающиеся на просторах всемирной паутины. В основном этим занимаются хакеры, они чем-то схожи с киберпреступниками, но их задача внедрить в сеть вредоносное программное обеспечение, которое будет все рассылать. Со спамом в сетях мы встречаемся каждый день и воспринимаем уже как должное;

6) кибервойны (CyberWarfare) – это военные события, которые разворачиваются в виртуальном пространстве. Кибервойны применяются на политическом уровне и направленны на жителей стран через заранее готовую иногда ложную, а иногда и правдивую информацию;

7) кибертерроризм – незаконный вид деятельности, в ходе которой террористы получают доступ к конфиденциальной информации о сооружениях, технологических картах различных объектов, схемах подземных туннелей, захват информационных ресурсов с целью дальнейшего нанесения вреда жителям и нарушению внутреннего баланса государства. Террористических организаций становится все больше, они начинают порабощать виртуальный мир;

8) майнинг – новый вид информационной угрозы, к которой подвержен даже простой пользователь персонального компьютера, но зачастую это происходит с какой-либо организацией. Где майнер внедряется через локальную сеть в персональные компьютеры этой организации, устанавливая вредоносное программное обеспечения. Входе, которого вычислительные мощности компьютеров незаметно начинают работать на майнера и используются для выработки криптовалюты, то есть получение дохода;

9) одной из угроз ИБ является «фрод» – это информационное мошенничество с банковскими картами, оплатами и платежами, внедрение в систему онлайн банков.

Все эти виды угроз несут вредоносные последствия, если не принимать меры по обеспечению безопасности и защиты от них. Ведь эти угрозы напрямую зависят на жизнь населения и стабильности в экономике государства.

Хакеры выбирают себе жертву исходя из выгоды для себя, исследуя значимость отрасли, экономическое положение компании на рынке государства или в мире. Какие же отрасли чаще всего выбирают хакеры? В основном они атакуют самые важные отрасли для жизнедеятельности любого государства. Значимую часть урона получают медицинские учреждения (17%), госучреждения (16%) и промышленность (16%) [2].

В случае медицинских учреждений хакеры получают доступ к инновационным технологиям, от которых зависят жизни людей. Атакуют оборудование, используют личные данные для покупки препаратов третьим лицам или вносят изменения в протоколы лечения заболевшего человека. Людям которая нужна срочная неотложная помощь из-за сбоев в системе, попросту могут не принять. Пользуясь этим, мошенники вымогают денежные средства за возвращение полного доступа и возвращение всех данных в реестр. Медучреждения легко атакуются, так как устаревшие IT-системы редко обновляются.

Угроз информационной безопасности трудно избежать даже госучреждениям. А также списание денежные средств с расчетных счетов госучреждений, вывод технического оборудования из строя, что сильно бьет по бюджету для государства. Целью хакеров является получение информации, после достижения своей цели. Они обменивают информацию на крупные денежные средства.

Чтобы избегать данные виды угроз нужно бережно и тщательно относиться к системе безопасности:

– своевременно обновлять систему защиты;

– включать защиту от ддос аттак, спама и вирусов;

– шифровать данные;

– создавать резервное копирование данных в отдаленной точке доступа;

– использовать виртуальные частные сети VPN, которые создают безопасность подключенных к сети приложений;

– установка DLP (Data Loss Prevention software) технологий – обеспечивает безопасность информационной системе, а именно отвечает за целостность файлов и устранению утечки этих файлов.

Угрозы информационной безопасности оказывают большое влияние на различные сферы жизнедеятельности, поэтому важно обеспечить безопасность этих сфер, так как от защиты информационной сети зависит благополучие населения.

Различные угрозы информационной безопасности в жизни любого государства характеризуется негативными последствиями для жизни населения. Как результат, эти угрозы могут принести большие убытки и затраты как для государственных учреждений, так и для обычного пользователя интернет сети. Исходя из этого, всегда требуется защита сети, поэтому чтобы сохранить безопасность нужно ответственно и разумно относиться к угрозам информационной безопасности, потому что угрозы никогда не пропадут.

Список литературы

1. Уголовный кодекс Российской Федерации: Федеральный закон от 13.07.1996 №63-ФЗ (ред. от 01.07.2021) // СПС «КонсультантПлюс». [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/

2. Наскидашвили К.А. Информационная безопасность. виды угроз информационной безопасности // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет». – 2020. – №12. – С. 187–189.

3. Доктрина Информационной безопасности [Электронный ресурс]. – Режим доступа: https: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf