Секция «Информационное общество, цифровая экономика и информационная безопасность»

Риски кибербезопасности 21 века

Научный руководитель – Нургазина Гульмира Есимбаевна

Шакирова Антонина Альбертовна
Студент (бакалавр)
Российская государственная академия интеллектуальной собственности, Москва, Россия
E-mail: tonys132435@gmail.com

Мир XXI активно подвергается внедрению компьютеризированных технологий. Совсем недавно было невозможно представить работу учебу без библиотеки, врача без ручки и работу без офиса. Благодаря новым технологиям активно развивается удаленная работа, дистанционное обучение и электронные хранилища информации. Всю необходимую информацию: фотографии, документы - каждый может хранить в своем телефоне или компьютере.

Теперь благодаря онлайн-сервисам удаленная работа и мобильность - мировой тренд, благодаря которому к 2025 году 75% работников будут трудиться вне офисов. В то же время рост количества сотрудников и обучающихся на интернет-платформах ставит перед ИТ-отделами трудные задачи по обеспечению необходимого уровня безопасности данных. Затраты на развитие данной сферы колоссальны, но гораздо дороже обходится ликвидация последствий кибер-атак.

Рынок ИТ-безопасности - один из самых быстроразвивающихся и инвестируемых рынков, но до сих пор недостаточно зрелый.
Ниже приведена таблица, демонстрирующая затраты на ликвидацию пробелов в сфере защиты данных и затраты на ее развитие до 2022 года.

Существующие риски и угрозы довольно обширны и разнообразны. В связи с этим полный переход на удаленную работу или дистанционное обучение не представляется возможным. Ведь новые технологии, помимо пользы и удобства, могут создавать опасность и угрозу для сохранения конфиденциальности данных.

Прежде чем начать рассматривать главные риски в сфере кибербезопасности стоит разобраться в терминах, которые необходимы для понятия данной темы.

На международном уровне единого определения кибербезопасности нет. Во всех странах определение данного термина может значительно различаться. Как следствие, существуют и разные подходы к составлению стратегий кибербезопасности

Кибербезопасность - это воплощение всех мер защиты сетей, приложений и устройств. Это решение направлено на безопасность конфиденциальных данных, на защиту их целостности, а также на сохранение корректной работы той или иной организации.

Несмотря на сложность правовых процедур, в большинстве стран законодательство гибко подстроилось под современные тенденции. Таким образом, законодательства развитых стран содержат правовую основу для деятельности, связанной с обеспечением кибербезопасности. Например, в России на законодательном уровне дано следующее определение. Кибербезопасность - совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. Так же необходимо понимать, что представляет собой киберпространство. Киберпространство - сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функцио-

нирование, и любых форм осуществляемой посредством их использования человеческой активности.

На данной диаграмме показаны сферы, в которых потребителям больше всего необходима кибербезопасность для сохранения их данных.

Таким образом, видна потребность в защите различных видов информации (личной, корпоративной. Облачного хранилища).

Одна из самых значительных и частых проблем - ransomware. Это вредоносное ПО, после установки которого на электронном носителе появляется вирус, который способен уничтожить и взломать все важные файлы.

Эксперты провели исследование, и было выявлено, что каждые 14 секунд в мире появляется новый ransomware.

Следующий риск - кибер-атаки на государстве государственные структуры. Для стран с развитой информационной и инновационной инфраструктурой эта проблема является наиболее актуальной. Средств из бюджета выделяется совсем мало, недостаточно для того, чтобы обеспечить достойный уровень зашиты государственной информации, баз данных и государственных реестров. Ликвидация последствий кибер-атаки, совершенной на государственные информационные каналы, может стоит около $1.6 млн.

Для минимизации риска кибер-атак государству необходимо выделять большее количество средств из бюджета для найма высококвалифицированных кибербезопасников. В качестве примера можно привести Россию, где для информационной безопасности выделено 18 млн рублей на 5 лет.

Следующий риск, представляющий собой опасность для пользователей - кибер-атаки на облачные сервисы. Облачные сервисы представляют собой средство хранения данных и информации в информационном пространстве. Благодаря данным сервисам клиенты имеют возможность получить доступ к своим данным с любого устройство, где бы они ни были. В то же время чрезмерное доверие своих данных этим сервисам является угрозой для их сохранности и конфиденциальности.

Самые известные облачные хранилища предоставляются такими компаниями как AppleInc., Microsoft, Google, Yandex, DropBox. Сами представители компаний соглашаются с тем, что не могут обеспечить достаточный уровень охраны личных данных в связи с тем, что кибер-атаки с каждым разом все мощнее, опаснее и более непредсказуемы.

Чтобы максимально обезопасить пользователя от вскрытия его облачного хранилища, разработчики предлагают следующие способы:

-Двухфакторная аутентификация;

-Вход в облачный сервис через проверенное устройство;

- Не предоставлять свои данные третьим лицам;

Два вышеуказанных риска представляют собой большую угрозу для конфиденциальной и значимой информации пользователей.

«Вредоносные программы-вымогатели являются постоянно растущей и развивающейся угрозой, которая может нанести вред организациям всех размеров, но в особенности — малому и среднему бизнесу. Чтобы избежать ransomware-атаки, предприятия должны обеспечить безопасность всех устройств и облачных сервисов, а также убедиться, что они используют «правило 321» для регулярного резервного копирования данных и продолжают применять традиционные правила безопасности: устанавливают надежные пароли, ограничивают ненадежные устройства, задействуют учетные записи администратора только там, где этого нельзя избежать, и внедряют многофакторную аутентификацию», — так считает Торстен Курпьюн, директор по развитию бизнеса Zyxel.

Таким образом, безопасность информации и данных зависит в большей степени от бдительности и внимательности самих пользователей, от бюджета компаний или государства,

выделяемого на кибербезопасность, на уровень специалистов («кибербезопасников»), задействованных в структуре организации. Так же особую роль играет предикативный анализ. Суть которого заключается в том, чтобы заранее позаботиться о кибербезопасности, создать необходимые условия для максимального предотвращения совершения кибер-атаки.

Источники и литература

1) Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ
2) Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ
3) Федеральный бюджет. Краткая информация об исполнении федерального бюджета [Электронный ресурс] 2020 URL: https://www.minfin.ru/ru/statistics/fedbud/execute/?id_65=80041-yezhegodnaya_informatsiya_ob_ispolnenii_federalnogo_byudzhetadannye_s_1_yanvarya_2006_g.
4) Диогенес. Cybersecurity – Attack and Defense Strategies 2020
5) Кибербезопасность и угрозы 2020 года [Электронный ресурс] 2019 URL: habr.com