Заключительная лекция

С.А. Краснов

Заключение

# Заключение

Заключительная лекция.

Тема лекции: Заключение.

**Учебные вопросы:**

1. Краткий обзор дисциплины.
2. Проблемы обеспечения ИБ современных информационных систем. Перспективы и тенденции развития.

**В.1.**

В рамках данной дисциплины мы с Вами изучили три основных темы, материал которых нацелен на обеспечение информационной безопасности в компьютерных системах с помощью программно-аппаратных средств защиты информации.

Тема 1: Основные понятия и задачи программно-аппаратной защиты информации, принципы её построения.

Тема 2: Методы и средства защиты информации от НСД.

Тема 3: Методы и средства и антивирусной защиты.

В рамках изучения данных тем Вы освоили материал, который позволит Вам в Вашей профессиональной деятельности решать вопросы по обеспечению безопасности при проведении различных работ при разработке и эксплуатации различных информационных, автоматизированных, интеллектуальных и других систем. Вы изучили методы и способы в области защиты информации, которые применяют разработчики различных защитных механизмов включенных в состав средств защиты информации. Кроме того, Вы на практике приобрели навыки по настройке различных средств защиты информации в соответствии с требованиями руководящих документов РФ.

Все это позволит Вам качественно выполнять должностные обязанности в данной предметной области.

**В.2.**

Задачи в сфере информационной безопасности в России являются только частью общемировых задач и проблем. Общее соотношение угроз в мире показывает, что Россия находится на втором месте по количеству кибертеррористических актов и хакерских атак. Однако если в США совершается 41% всех хакерских атак в мире, в России – не более 10%. Сложившаяся ситуация дает возможность воспользоваться относительно комфортным режимом и направить силы на повышение уровня защиты от предполагаемых угроз.

**Роль информационной безопасности в современном мире**

Под информационной безопасностью понимается комплекс организационных и технических мер, которые принимаются для обеспечения защиты, целостности, доступности и управляемости массивов информации. В рамках общей концепции безопасности государства информационная безопасность обеспечивает связанное взаимодействие всех элементов системы.

**Структурные элементы информационной безопасности на международном и внутригосударственном уровне включают:**

* защиту сведений, содержащих государственную или коммерческую тайну;
* защиту серверов государственных учреждений и систем жизнеобеспечения;
* защиту безопасности данных как набор аппаратных и программных средств, которые обеспечивают сохранность информации от неавторизированного доступа, затруднения доступа, разрушения и перепрограммирования;
* информационно-психологический блок, который подразумевает реализацию системы мер, направленных на защиту от целенаправленного информационного воздействия на субъект нападения, его психологическое состояние или имидж на международной арене.

Защита всех составляющих требует разработки методического аппарата и создания собственной инфраструктуры. Задачи обеспечения информационной безопасности осложняются тем, что информационное пространство не имеет границ. Особенности работы сети Интернет и возможности беспроводной связи создают предпосылки для бесконтрольного и беспрепятственного переноса через границы государств огромных массивов данных, часто содержащих сведения, оборот которых в мире или в отдельных странах запрещен или ограничен.

Атакующие технологии развиваются быстрее защитных, поэтому даже государственные базы данных находятся в зоне риска. Для защиты государственной тайны применяются самые совершенные технологии. Но государственная тайна попадает в зону риска, как только выходит из наиболее охраняемого периметра и становится объектом взаимодействия государственных учреждений с коммерческими организациями или общественными институтами, степень защиты которых существенно ниже.

Однако и государственные защитные меры несовершенны, о чем говорят участившиеся взломы правительственных серверов в разных странах мира. Для сравнения: в течение 2016 года в России на государственные и частные ресурсы было совершено уже 70 млн кибернападений, что говорит о скорости возрастания и серьезности угрозы.

Проблема осложняется тем, что взломщики чаще всего не попадают под юрисдикцию государства, подвергшегося кибернападению. Преступники являются либо иностранцами, либо лицами без гражданства – «гражданами мира». Все это вынуждает искать общемировой консенсус в борьбе с угрозами и создавать общую систему информационной безопасности. Ведутся предварительные переговоры о возможности не только признавать кибератаки преступлениями, но и приравнивать их к вооруженным нападениям, когда целью являются государственные институты.

Редким примером систематизации норм в сфере защиты информационной безопасности служит правительственное соглашение между Россией и США, заключенное в 2013 году о сотрудничестве в научных исследованиях и разработках в ядерной и энергетической сферах. В документе в том числе перечислялись меры доверия и способы противодействия кибервойне, а также декларировалось создание общей системы информационной безопасности. Однако в 2016 году действие соглашения приостановили.

Дополнительным аргументом, который подтверждает необходимость создать международную нормативно-правовую базу по борьбе с киберугрозами, служит риск ущерба репутации государства. Использование информационных технологий в политической конкуренции стало привычным делом, и ущерб от «кибервыпадов» в адрес конкурирующего государства выражается не только в репутационных, но и в финансовых потерях. Информационная безопасность и защита репутации государства должны стать одним из инструментов в геополитическом противоборстве.

Информационная безопасность в России

В России все аспекты борьбы с ИБ-угрозами национального масштаба рассматриваются на уровне Доктрины информационной безопасности, которая служит основой для принятия нормативных актов. Среди фундаментальных вопросов доктрины – необходимость самостоятельного информационного присутствия России в международном сообществе и выбор каналов поставки достоверных данных и новостей, что позволит снизить ущерб от дезинформационных атак.

Применительно к качеству государственного или корпоративного управления уровень информационной безопасности определяется способностью государства или компании:

* обеспечить функционирование информационных ресурсов и потоков, достаточное для нормальной жизнедеятельности и развития;
* защитить в полном объеме коммерческую или государственную тайну от незаконных посягательств;
* противостоять техническим и психологическим угрозам, оградить систему и пользователей от негативного воздействия с использованием информационных технологий;
* поддерживать эффективность работы, возможность «саморазвития» и адекватные реакции системы на возрастающие вызовы;
* использовать такие методы и средства защиты информационного суверенитета государства или корпоративных ценностей, которые не посягали бы на целостность прав и свобод других государств и граждан.

Информационная безопасность государства складывается из множества факторов. Массивы информации являются основным ресурсом, который поддерживает жизнеспособность государства в политической, социальной, экономической и военной сферах. Основным приоритетом государственной политики становится выделение роли и повышение значимости информационной безопасности в качестве системообразующего элемента управления.

За информационную безопасность России на современном этапе отвечают различные государственные учреждения, в том числе Федеральная служба по техническому и экспортному контролю (ФСТЭК), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), специализированные подразделения министерств и ведомств, а также межведомственная комиссия при Совете Безопасности. Однако участники процесса борьбы с кибератаками считают, что на современном этапе необходимо объединить функции и передать отдельному регулятору уровня федеральной службы с самостоятельными ресурсами и значительными полномочиями.

Пока российская система переживает стадию роста и отвечает не всем требованиям, позволяющим обеспечить ИБ в полном объеме. Причин несколько.

Независимость

Независимость, или степень локализации систем, жизненно важных для функционирования государства, обеспечивается за счет:

* собственного программного обеспечения – операционных систем, систем защиты информации, SIEM-систем и других ИБ-продуктов российских разработчиков;
* собственных каналов связи, чтобы поддержать «автономию» от мировой сети Интернет наиболее важных ресурсов;
* квалифицированных кадров (по подсчетам Минкомсвязи, к 2020 году в России появится до 350 тысяч квалифицированных специалистов в области информационной безопасности).

Важный аспект обеспечения независимости – создание четко выстроенной системы межведомственного взаимодействия и самостоятельной структуры для управления рисками с опорой на нормативно-правовую базу, что обеспечит полномочия и возможности для работы. Существенной проблемой становится и отсутствие собственной аппаратной части, что ставит систему ИБ России в положение зависимости от иностранных поставщиков.

Несовершенство ИБ в социальной сфере

Важной задачей становится обеспечение на должном уровне информационной безопасности в социальной и образовательной сферах. Ярким проявлением отсутствия должных мер защиты является вовлечение несовершеннолетних в опасные сетевые сообщества террористической или суицидальной направленности. Основная причина кроется в недостаточной локализации популярных интернет-ресурсов и невозможность полного контроля с российской стороны над глобальными социальными сетями. В первом случае проблема заключается в том, что принцип давления на крупнейшие ресурсы с требованиями о предоставлении персональных данных пользователей срабатывает не всегда, как в случае с «Твиттером» и «Фейсбуком. Во втором случае требуется координация различных служб, так как справиться с проблемой только силами МВД и Роскомнадзора невозможно. За 2016 год Роскомнадзор заблокировал 17 тыс. доменных имен и пользователей, но они появляются вновь – под другими именами, но с тем же кругом последователей.

Проблемы и угрозы ИБ на международном уровне

Угрозы информационной в России и мире преимущественно экономического «происхождения». Кибертерроризм с целью подорвать политическую стабильность менее распространен, а мнимый масштаб ему придает широкое освещение в СМИ. Кроме того, громкие взломы чаще всего носят «рекламный» характер и служат своеобразной презентацией услуг той или иной хакерской группировки, которая планирует поставить навыки и умения на коммерческий «конвейер». Акты, носящие публичный характер, как, например, атака вируса WannaCry, выполняют еще и функции разведки, хакеры таким образом определяют степень защищенности мировых информационных ресурсов и готовятся к новым, более серьезным и масштабным операции.

По оценке американского Центра стратегических и международных исследований, ежегодный ущерб от преступлений, связанных с хищением компьютерной информации, по всему миру превышает 440 миллиардов долларов.

Информации корпораций, банков и правительственных организаций угрожают не только хакеры. Среди угроз безопасности:

* системные сбои, возникающие по различным причинам, в том числе из-за случайных ошибок или внедрения неверного кода в программное обеспечение;
* технические неисправности аппаратных средств, вызванные сбоями в системе электроснабжения, в том числе намеренными диверсиями, конструктивными проблемами или действиями пользователей;
* вирусы, которые постоянно совершенствуются и модифицируются, в частности, в начале 2017 года от вирусов-шифровальщиков NotPetya и WannaCry пострадали крупных международные компании и государственные учреждения, число жертв только WannaCry превысило 200 тысяч в 150 странах;
* деятельность сотрудников, направленная на разрушение систем безопасности, намеренный саботаж;
* внедрение в сеть неавторизованных пользователей, которые могут перепрограммировать компьютеры или похитить важные сведения;
* хищение данных любыми способами, включая кражу физических носителей информации, с различными целями.

На государственном уровне разрабатывается не только стратегия борьбы с угрозами, но и «наступательные» кибероперации, когда государственные структуры совершают акты кибершпионажа или повреждают сети государств-«конкурентов» с целью похить или повредить критическую информацию. Уже к 2014 году в США, например, власти взяли под контроль почти весь объем производства spyware (программы для кражи и перенаправления данных с компьютера пользователя) и adware (программы распространения «вирусной» рекламы).

Другие инструменты совершения атак на государственные, корпоративные и личные устройства включают:

**Ransomware**, или программы-вымогатели. При запуске программы компьютер или мобильное устройство теряют работоспособность по различным причинам. Для возвращения работоспособности необходимо заплатить хакерской группировке. Особенность атак с помощью программ-вымогателей «новой волны» в том, что злоумышленники требуют выкуп в криптовалюте, оборот которой находится в теневой зоне, и отследить получателя которой крайне затруднительно.

**Лжеантивирусы**. Версия программ-троянов. Пользователь добровольно устанавливает вредоносное ПО на компьютер, которое в дальнейшем или блокируют работу ПК и требуют заплатить деньги, или помогают проникнуть в систему другим вирусам.

**Madware-программы**. Нацелены на повреждение ПО мобильных устройств.

**Кибербуллинг**, или использование информационных атак для воздействия на психологию жертв.

Под постоянной угрозой находятся и компьютеры частных пользователей, которые бессистемно относятся к защите персональных данных, и тщательно охраняемые базы данных международных корпораций. Компании в США и Евросоюзе готовы платить за хакерскую атаку и похищение данных у конкурентов от 3 до 12 млн долларов. Притом, если атака производится на военный или промышленный объект, цена увеличивается в пять раз.

В России объем киберпреступлений частного характера существенно меньше, но это обстоятельство одновременно является и основанием неподготовленности систем безопасности большинства российских компаний, что отмечают на уровне МВД.

Спасибо за внимание!!!